Caveats for Cisco IOS Release 12.2(33)SRC through 12.2(33)SRC6

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)SRC6

Cisco IOS Release 12.2(33)SRC6 is a rebuild release for Cisco IOS Release 12.2(33)SRC. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRC6 but may be open in previous Cisco IOS releases.

- 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.

- CSCsz72591

  Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.

  Conditions: The router must be configured to act as a DHCP client.

  Workaround: There is no workaround.

- CSCta79704

  Symptoms: Router crashes with a breakpoint exception

  Conditions: Router is configured with either of the following features:

  – IP Transfer Point (ITP), Cisco IOS Release

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122mb/122mb2/itp20/index.htm

  – PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

    http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ft_0546.html

  – Reliable Export with SCTP, Cisco IOS Release

    http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/nfhtsctp.html

  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.

- CSCtc68037

  Symptoms: A Cisco IOS device may experience an unexpected reload as a result of mtrace packet processing.

  Conditions: This symptom is seen as a result of mtrace packet processing.

  Workaround: There is no workaround other than avoiding the use of mtrace functionality.

- 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.

- 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

Resolved Caveats—Cisco IOS Release 12.2(33)SRC5

Cisco IOS Release 12.2(33)SRC5 is a rebuild release for Cisco IOS Release 12.2(33)SRC. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRC5 but may be open in previous Cisco IOS releases.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsk35688

  Symptoms: Aggregate routes are not processed if all aggregated child routes are deleted prematurely.

  Conditions: The symptom is observed when all aggregated child routes are marked for deletion and the periodic function which processes the routes to be deleted deletes the route before the aggregate processing function gets a chance to process them and the aggregate route to which they belong.

  Workaround: Configuring “bgp aggregate-timer” to 0 or the lowest value would considerably reduce the chances of hitting this problem. In case this problem does occur, in order to delete the stale aggregate route, configure a temporary local BGP route (say, redistribute a static route or network a loopback) with its address being a subnet of the stale aggregate address and then remove the aggregate address and the added route. This should delete the route from table and send withdraws to the other routes also.

  Further Problem Description: The periodic function is by default called at 60 second intervals. The aggregate processing is normally done based on the CPU load. If there is no CPU load, then the aggregate processing function would be triggered within one second. As the CPU load increases, this function call will be triggered at higher intervals and if the CPU load is very high it could go as high as the maximum aggregate timer value configured via command. By default this maximum value is 30 seconds and is configurable with a range of 6-60 seconds and in some trains 0. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- 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.

- 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/noshut or Hw-module reset was issued.

  Conditions: Applies to Cisco IOS Release 12.2SX and related releases.

Workaround: There is no workaround.

- CSCsl56660

  Symptoms: After increasing the interface bandwidth, interface output rate does not exceed the previously configured interface bandwidth.

  Conditions: Symptom observed when all following conditions are met: - Cisco 7600 running Cisco IOS Release 12.2(33)SRC or a rebuild of 12.2(33)SRC. - Interface in question is on a Cisco 7600-SIP-400 line card. - **interface bandwidth** command is configured. - QoS service policy attached to the interface.

  This bug does not affect Cisco IOS Release 12.2(33)SRB.

  Workaround: There are two workarounds:

  1. Reload line card after each **interface bandwidth** change.
  2. Remove the **interface bandwidth** command. Remember to reload the 7600-SIP-400 to make change effective. Note that if QoS service policies with **bandwidth percent** commands are applied to this interface, percentages will have to be adjusted. Removing the interface **bandwidth** command may affect the dynamic routing protocol metric on this interface.

- CSCsm96243

  Symptoms: On executing **show tcam interface acl in ip det | include** command with traffic coming into the interface, the switch crashes.

  Conditions: This has been observed on an interface where there are no features configured.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsq15577

  Symptoms: On a Virtual Private LAN Services (VPLS) setup, when the core-facing link is flapped, some VCs are disposed off SIP-600, or the ESM20 stops disposing traffic.

  Conditions: Core interface flap can cause this condition.

  Workaround: Enter the **clear mpls ldp neighbor** command or perform a **shut/no shut** on the VLAN interface.

- CSCsq39084

  Symptoms: Memory leak occurs on ESM20 and X40G line cards.

  Conditions: Occurs when member links of port-channel are added/deleted and there are EVCs configured under the port-channel.

  Workaround: There is no workaround.

- CSCsq63209

  Symptoms: Standby Router reloads.

  Conditions: Occurs when “vbr-nrt” or “cbr” is configured in “pvc-in-range mode.” After **shut/no shut** on a sub-interface, the router crashes.

  Workaround: There is no workaround.

- CSCsq68600

  Symptoms: An RP crashes upon executing the **clear interface virtual-access** command with high traffic.

  Conditions: The symptom is observed with dLFIoATM/PPPoATM on a Cisco 7600 series router upon executing the **clear interface virtual-access** command.

  Workaround: There is no workaround.

Further Problem Description: The **clear interface virtual-access** command is not typically used for configuration or debugging.

- CSCsq82041

  Symptoms: Memory leak occurs when remote provider edge (PE) devices have more xconnects configured than the unit under test.

  Conditions: Occurs when you set session limit under vpdn-group and over subscribe sessions.

  Workaround: There is no workaround.

- CSCsr53059

  Symptoms: A PPPoA session fails to come up after modifying the PVC.

  Conditions: The symptom was seen while testing the feature PPP over ATM with Subscriber Service Switch.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsu22952

  Symptoms: Cisco 7600 RP crashes when the traffic crosses ATM dLFI interfaces.

  Conditions: This could happen when all the following met:

  1) MLP over ATM is configured.

  2) QoS queuing policy applied on the MLP bundle.

  3) The MLP link goes down.

  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.

- 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 aaa account system guarantee-first” configuration.

- 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.

- 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.

- 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.

- CSCsu74279

  Symptoms: If pseudowire is configured under the ATM interface then it may lead to crashing the RP.

  Conditions: Occurs during normal operation.

  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.

- 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.

- CSCsv05057

  Symptoms: There is a corner case where BGP peers may become stuck in Idle or Active state forever and session establishment does not progress.

  Conditions: The symptoms are observed with a BGP VPNv4 session and when the router is reloaded.

  Workaround: Disable and re-enable the individual BGP peer, i.e.: **neighbor X shut neighbor X no shut**

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsv76105

  Symptoms: Standby supervisor crashes during bootup.

  Conditions: Occurs in Cisco IOS Release 12.2(46)SG, and possibly 12.(44)SG and 12.2(40)SG.

  The crash occurs if the following commands are configured:

  snmp mib notification-log globalsize 10000

  snmp mib notification-log globalageout 120

  snmp mib notification-log default

  Workaround: Remove the above commands from the configuration.

- CSCsv94437

  Symptoms: After an online insertion and removal (OIR) is performed on a line card, QoS does not work for PPPoE sessions.

  Conditions: Problem seen only if QoS is configured for PPPoE sessions.

  Workaround: There is no workaround.

- CSCsw16157

  Symptom: 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.

- CSCsw43211

  Symptoms: Following errors are seen:

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

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

  Workaround: There is no workaround.

- CSCsw63003

  Symptoms: Memory increase occurs in “BGP Router” process due to BGP path attributes. Memory used by this process increase every day and so do the BGP path attributes 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, 12.2(33)SB, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, 12.4, 12.4T. Problem is seen with continuous churn in the network such that BGP never manages to converge and when the paths churning are not reusing existing path attributes. That will cause those paths to allocate new paths attributes.

Workaround: Reload the router if low memory conditions are reached or identify the root cause of the churn and attempt to fix that is possible.

- 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.

- 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.

- 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.

- CSCsx10028

  Symptom: A core dump may fail to write or write very slowly (less than 10KB/s).

  Conditions: This is seen when the cause of the crash is Processor memory corruption. When this happens, the corrupted memory pool cannot be used to write the core dump, so it will likely fail. I/O memory corruption crashes should not have this problem.

  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).

- 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.

- 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.

- 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.

  c

- 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

- 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 web page.

  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

- CSCsy26883

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

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

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

- CSCsy27500

  $$PREFCS

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

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

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

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

- CSCsy29534

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

  Conditions: It was observed in the following context:

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

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

- 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.

- 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.

- 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.

- CSCsy70184

  Symptoms: Traceback occur on SPA inside SIP-400.

  Conditions: Occurs during online insertion and removal (OIR) of SPA.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsy98369

  Symptoms: Prune flag is not set after host leaves the group.

  Conditions: Occurs during normal operation.

  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”.

- 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.

- CSCsz11784

  Symptoms: DS3 interface on choc3/STM1 stops passing traffic.

  Conditions: Occurs when a DS3 is oversubscribed.

  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.

- 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.

- 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 release 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

- CSCsz25686

  Symptoms: Command can not be removed from CLI view once it has been added. As a result this command will not be visible in other view. As an example, if the following commands are entered:

  * **commands exec include-exclusive show snmp user**

  * **no commands exec include-exclusive show snmp user**

  The **show snmp user** portion will be missing from other view.

  Conditions: Occurs on Cisco IOS Release 12.2(33)SRC3.

  Workaround: There is no workaround.

- CSCsz29991

  Symptom The error message "%OSPF-4-NULL_PREV_LINKAGE" is displayed with a traceback upon executing **clear ip ospf process**. This spikes the CPU to 100% forever ultimately leading to a Sup/RSP crash. The crash could happen immediately or even after several hours.

  Conditions: A "clear ip ospf process" especially in an environment having multiple OSPF process and learning the same prefix via different processes could end up with the above issue due to a race/timing condition. In this case it was due to the fact that one process was having a "default-information originate always" CLI causing an implicit redistribution and the other process also learning a default route as E2. Clearing the IP OSPF process i.e. both the process the hard way could lead to the above issue.

  Workaround: To Avoid the issue, enter **clear ip ospf process** on a process-by-process basis a few minutes apart. Perform a **shut/no-shut** of the OSPF process instead of a hard reset or clear.

- 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.

- 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.

- 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.

- 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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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: Policy-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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCtb64636

  Symptoms: SPA_CHOC_DSX-3-HDLC_CTRL_ERR messages are seen continuously with any channelized SPA with full channelization with MLP bundles with C7600-sip-400 linecard. There is some traffic outage due to this.

  Conditions: Occurs when the following conditions are: present:

  1. SPA should be fully channelized.

  2. There should be some MLP bundles, and the traffic should be at the near to the line rate of the SPA.

  3. Member links are flapping continuously for approximately 2 hours.

  Workaround: Perform a **shut/no shut** on the bundle from which the member links are flapping.

Resolved Caveats—Cisco IOS Release 12.2(33)SRC4

Cisco IOS Release 12.2(33)SRC4 is a rebuild release for Cisco IOS Release 12.2(33)SRC. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRC4 but may be open in previous Cisco IOS releases.

- CSCee19691

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

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

  Workaround: There is no workaround.

- CSCee72833

  Symptoms: Cisco 7200/NPE-G1 router running Cisco IOS Release 12.3(5c) hangs during reload.

  Conditions: Occurs if AUX port is connected to console port of Catalyst 3550.

  Workaround: Disconnect cable from AUX port

- CSCeg35237

  Symptoms: Watchdog timeout crash when using the **show crypto session** command.

  Conditions: Occurs on a Cisco 7200 NPE-G1 running Cisco IOS Release 12.3(7)T2 and Cisco IOS Release 12.3(8)T1.

  Workaround: There is no workaround.

- CSCeh04362

  Symptoms: RBE does not function in an IPv6 environment

  Conditions: This problem is seen with the 12.2(27)SB images. Traffic does not pass through with RBE configured for IPv6.

  Workaround: There is no workaround.

- CSCei59800

  Symptoms: The **commands configure include all policy-map** command does not include the policy-map mode commands as part of the view.

  Conditions: Occurs on a Cisco router running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- 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.

- CSCsb06920

  Symptoms: The following error messages are seen in the router log with SAA configured:

  %SYS-3-MGDTIMER: Running timer, init, timer

  -Process= "SAA Event Processor", ipl= 0,

  or

  %SYS-2-LINKED: Bad enqueue of 68BA76C4 in queue 63629FD0

  -Process= "SAA Event Processor", ipl= 0, pid= 126

  Workaround: Remove the SAA configuration from the router.

- CSCsb77148

  Symptoms: The output of the **show ip mpacket a.b.c.d quality** command is misleading after the circular buffer wraps around.

  Conditions: The problem is seen with the following configuration,

  ip multicast cache-headers rtp 16

  and is not seen with the following,

  ip multicast cache-headers rtp

  Workaround: Enable the multicast cache buffer, but don't configure the size of the buffer.

- CSCsc32706

  Symptoms: In IPv6 egress rep mode, the interfaces remain in the DFC TCAM on shut.

  Conditions: One box test, local RP. One traffic flow. Three outgoing interfaces. Two of them are shut down, but DFC still has all three installed, despite the DFC MFIB, which is correct.

  Workaround: There is no workaround.

- 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.

- CSCsc80427

  Symptoms: The **errdisable flap-setting cause link-flap max-flaps** command is saved as **errdisable flap-setting cause link-flap flap-count**. The command is then ignored during bootup.

  Conditions: Unknown at this time.

  Workaround: Manually reconfigure the command after system reload.

- 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.

- CSCse45978

  Symptoms: If the next-hop IP address of a redistributed BGP prefix in the RIP database changes to take an alternate path in the RIB, the route is removed from the RIP database.

  Conditions: This has been seen when the BGP peers are configured for multihop, and redundant paths to the peer exist. When the primary path fails, the alternate path is then installed in the routing table and the BGP session remains up.

  Workaround: Use one of the following options:

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

  Use another IGP, other than RIP, such as EIGRP.

  Perform a **shut/no shut**.

- 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.

- CSCsg07531

  Symptoms: The parse chain for the 'logging event spanning-tree ...' is incorrect.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsg12887

  Symptoms: A Cisco 7600 might crash continuously due to Address Error (load or instruction fetch) exception, CPU signal 10.

  Conditions: Occurs when multicast traffic is sent over GRE tunnel and a tunnel key is configured. This affects both Cisco IOS Release 12.2(33)SRC1 and Cisco IOS Release 12.2(33)SRC2.

  Workaround: Remove the tunnel keys from all GRE tunnels where PIM is configured.

- 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.

Further Problem Description: This happens every time, but there is no major negative impact to operation.

- 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.

- 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.

- CSCsi63649

  Symptoms: All the routers synced to one router are showing every 10 seconds the following error messages:

  Apr 23 13:33:41.929: %SYS-3-TIMERNEG: Cannot start timer (0x7543D68) with negative offset (-996736100). -Process= "TTY Background", ipl= 0, pid= 42

  Conditions: This issue is being observed on some Cisco GSRs running 12.0(28)S, 12.0(31)S, 12.0(32)S and 12.0(32)SY releases. The issue happens when a telnet session is initiated on the router, and then a new telnet session to a different device is initiated from the telnet session.

  When a user logs in via telnet session into the router and then we issue a telnet somewhere else, the exec-timeout will not disconnect the session even if no keystrokes are issued. At the exact moment the timeout expires, the error message will be displayed every 10 seconds.

  Workaround: Use the **show users** command to determine which users are logged via telnet. Then use **clear line X** to clear the line, disconnect the users and stop the error messages.

- CSCsj34128

  Symptoms: A newly created ATM sub-interface will have the **no snmp trap link-status** command enabled by default, even if the **snmp-server enable traps atm subif** command is configured under the global configuration mode.

  Conditions: This problem is observed in Cisco IOS Release 12.4(5) and after.

  Workaround: You can manually configure the **snmp trap link-status** command under the sub-interface configuration mode.

- CSCsk63780

  Symptoms: After switchover in RPR+ mode, some line cards may get stuck in STRTIOS state.

Conditions: This problem is seen on a Cisco 12000 router booted with the c12kprp-p-mz.120-32.S6q image. The router is fully loaded with E5, E4+, and E3 line cards; and configured with 113 mVRFs.

Workaround: There are no workaround.

- CSCsk80250

  Symptoms: The command **show ip bgp neighbors** *x.x.x.x* **paths ^([^7][^0][^1][^8]|.|..|...|.....) +_7018_** may cause the router to reload.

  Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.2SRC1.

  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.

- CSCsk97295

  Symptoms: SIP400 crashes due to memory corruption sometimes just after loading a new image on the router as the line card is coming up

  Conditions: SIP400 is loaded with 4xCT3, 1xCHSTM1/OC3, 8xCHT1E1 and 4xT3E3 SPA. Around 50 multilinks are configured on the line card and traffic is going through them. Crash occurs after saving the configuration and reloading the router.

  Workaround: There is no workaround. Impact on functionality after the crash is minimal. The line card resumes operating as expected. This problem is seen very rarely and only on router reload.

- CSCsl28371

  Symptoms: When SPA-IPsec-2G or VPNSM in Cisco 6500 or Cisco 7600 is configured in VRF mode, a spanning-tree L2 loop and a broadcast storm may occur over it.

  In this case SPA interface counters show that module is sending/receiving excessive traffic (up to 1 Gbps) even if the crypto configuration is not present at all. Power cycling SPA module helps temporarily, but later the loop and the storm may occur again.

  High CPU may be also seen when the broadcast storm is present.

  SPA card crypto statistics show most of the traffic going through the module as broadcast/multicast and clear text (not encrypted).

  Conditions: - L2 loop actually occurs over VLAN1 which is added (allowed) on both SPA trunk ports by default during module auto-configuration (this occurs when module is first inserted to the chassis, when crypto mode is switched to vrf, etc).

  - Loop occurs in VRF mode only. In crypto connect mode, the loop does not occur.

  - Vlan 1 should be present somewhere else in the system to trigger this issue. At least a single broadcast packet should be injected into Vlan 1 to initiate a broadcast storm over the loop.

- Theoretically, the loop may occur over VLANs 1001-1005 as well (these VLANs are also added to SPA trunks by default) but the probability of this situation is very low because these VLANs do not carry user traffic.

  Workaround: Disable VLAN 1 manually on both SPA trunk ports (remove it from list of allowed VLANs). This configuration will be preserved after 6500/7600 reboot.

  VLANs 1001-1005 may be disabled as well.

  Keep in mind that VLAN 1 may be auto-generated on SPA ports again if:

  - if the module is removed from the chassis and inserted back

  - if the crypto mode is switched to crypto connect and then back to vrf mode again

  - if the startup configuration is erased and the whole chassis is rebooted

- 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.

- CSCsl42113

  Symptoms: Multicast egress replication is broken for IPv4 and IPv6:

  - mroute entries are correct.

  - IGMP groups are correct.

  - Receivers on the egress line card are not able to receive the multicast.

  - Interfaces counters show that the switch is receiving the multicast stream.

  Conditions: Applies to Egress multicast replication.

  Workaround: Change the multicast replication mode to "ingress"

- CSCsl68327

  Symptoms: Packets may be lost during rekey.

  Conditions: Occurs because IPSec transit packets may trigger invalid SPI.

  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.

- CSCsm00459

  Symptoms: Failed to create ima-group.

  Conditions: Issue is seen upon trying for 4 to 5 times of provision and unprovision 42 IMA groups.

  Workaround: There is no workaround.

- CSCsm39308

  Symptoms: There may be a system crash while trying to configure **router isis** or **router iso-igrp**.

  Conditions: The symptom is observed when **router isis** or **router iso-igrp** is already configured without a tag.

  Workaround: Use a tag in **router isis** and **router iso-igrp** configurations.

- 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.

- 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.

- CSCsm66896

  Symptoms: Memory leak in SNMP ENGINE process.

  Conditions: This is has been seen on Cisco routers running Cisco IOS Release 12.4 and configured as an IP SLA probe router.

  Workaround: There is no workaround.

- CSCsm74948

  Symptoms: In a multicast VPN environment, RP does not send join to directed connected PE. When RP gets a register message from PE or the periodic join timer expires, it never sends out a join.

  Conditions: The RP and PE are PPP direct connected with default setting "peer neighbor-route".

  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.

- CSCsm89052

  Symptoms: 30 second offered rate under **show policy-map interface** command is incorrect.

  Conditions: Occurs when policer uses "policed-dscp-transmit" for exceed action.

  Workaround: There is no workaround.

- CSCso04657

Symptoms: SSL VPN service stops accepting any new connections.

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

Workaround: There is no workaround.

- CSCso09801

  Symptoms: The **send log** command does not include date and time in syslog.

  Conditions: Upon executing the **send log***severity console message*, the date and time should be included in the syslog entry. It is not.

  Workaround: There is no workaround.

- CSCso30480

  Symptoms: The cempMemPoolTable is currently indexed by module index. This is wrong for LAN cards. It should be indexed by CPU.

  Conditions: Occurs when a line card that has a CPU is installed.

  Workaround: There is no workaround.

- CSCso49064

  Symptoms: The SIP600/ES20 line cards crash when a EoMPLS packet with destination MAC address is zero (all zero except the last nibble).

  Conditions: The line card crashes as soon as it receives a packet in the disposition side. The crash is seen only when the size of the packet is less than 68.

  Workaround: There is no workaround.

- 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.

- 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*.

- CSCso57602

  Symptoms: Diagnostic failure seen on Cisco 7600-SIP-200 after online insertion and removal (OIR). OIR of SIP-200 with a Supervisor 32 results on major diagnostic failure. OIR of SIP-200 with a Supervisor 720 results in a minor error.

Conditions: Minor Error occurs on Supervisor 720 when module OIR occurs with no cables attached.

Workaround: Reset the SIP-200 module with an active connection.

- CSCso68580

  Symptoms: After online insertion and removal (OIR) of member link module, the switchport configurations will be doubled in a Cisco 7600 router.

  Conditions: Occurs when BCP and MLP is configured and OIR is performed.

  Workaround: There is no workaround.

- CSCso71955

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

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

  Workaround: Disable netflow if possible.

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

- 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.

- CSCso85193

  Symptoms: After running for some time, the Cisco 7609 generates a general error when setting a value on any SNMP object. The **show users** command indicates a ghost entry:

  #show users

  Line User Host(s) Idle Location

  1 vty 0 Virtual Exec 00:00:00

  Conditions: Occurs on routers running Cisco IOS Release 12.2(33)SRB2.

  Workaround: Enter the **clear config lock** command.

- CSCso85789

  Symptoms: ciscoFlashFileStatus shows deleted for all files. ciscoFlashFileType shows unknown for all files

  Conditions: Observed on a Cisco 7600 running Cisco IOS Release 12.2SR. Occurs when polling ciscoFlashFileTable using SNMP.

  Workaround: There is no workaround.

- CSCso87916

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

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

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCso93296

  Symptoms: IPv6 rate limiters do not drop multicast packets

  Conditions: Occurs when multicast is not enabled.

  Workaround: Enable multicast routing.

- 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.

- CSCso97927

  Symptoms: OIR insertion takes a long time on a Cisco 7200 router compared to OIR removal. Excessive CPU usage then impacts router functionality.

  Conditions: Occurs when executing a graceful or manual OIR of any of the PA's in a Cisco 7200 router. OIR insertion operation takes approximately 25 seconds. OIR removal is completed in approximately 4 seconds.

  Workaround: There is no workaround.

- CSCsq00728

  Symptoms: All packets are classified under one QoS group.

  Conditions: This happens on a Cisco 7200 router loaded with Cisco IOS Release 12.4(19.16)T1 image.

  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.

- CSCsq08625

  Symptoms: Traffic does not flow after stateful switchover (SSO) because of Incorrect PBR TCAM redirect adjacency programming.

  Conditions: If a router with PBR route map configured is reloaded and then SSO is performed, the TCAM redirect adjacency programming is not correct.

  Workaround: Unconfigure and reconfigure route-map or reload the router.

- CSCsq13111

  Symptoms: The output rate value shown by **show interface vlan** is much lower than the actual line rate.

  Conditons: Unknown at this time. There is no functional impact. Display issue only.

Workaround: There is no workaround.

- CSCsq14311

  Symptoms: Router crashed while clearing NAT translations.

  Conditions: Occurred on a Cisco 7200.

  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.

- 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 desination - 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.

- CSCsq45161

  Symptoms: RP on Sup720-3BXL reaches 100% CPU on Virtual-Exec after renewal of DHCP snooping database located on remote TFTP server. Renewal is performed via VTY session, which as a result of bug hangs and can not be cleared. Router is still accessible via another VTY session, so it is seen that DHCP snooping agent remains active.

  Conditions: Occurs when DHCP snooping is configured to store bindings database on remote TFTP server.

  Workaround: While issue is observed, access impacted router via console connection. It releases the hung VTY session and RP CPU goes down to normal level. You can also reload the router.

- 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.

- 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.

- CSCsq66506

  Symptoms: Layer 3 ports take the wrong MAC address sometimes on bootup of line cards.

  Conditions: During bootup or sometimes after OIR, Layer 3 ports take the MAC address from the line card pool instead of the router MAC address

  Workaround: Perform a **shut/no shut** on interfaces with incorrect mac-address.

- CSCsq74185

  Symptoms: The command **verify disk2:c7200-spservicesk9-mz.122-33.SRC** does not complete the verify operation and yields the following error messages:

  Router#verify disk2:c7200-spservicesk9-mz.122-33.SRC Verifying file integrity of disk2:c7200-spservicesk9-mz.122-33.SRC Embedded hash not found in file disk2:c7200-spservicesk9-mz.122-33.SRC. Router# *Jun 11 18:18:09.301: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file disk2:c7200-spservicesk9-mz.122-33.SRC. *Jun 11 18:18:09.301: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file disk2:c7200-spservicesk9-mz.122-33.SRC. Router#

  Conditions: Occurs when the verify operation is performed on a Cisco 7200 router running Cisco IOS Release 12.2(33)SRC or 12.2(33)SRC1. Does not affect other platforms running these releases.

  Workaround: Perform the image verification using the MD5 checksum from the Software Center using the **verify /md5 disk2:c7200-spservicesk9-mz.122-33.SRC**.

- CSCsq78538

  Symptoms: When "issu runversion" or "issu commitversion" specifies "sup-bootdisk:/slavesup-bootdisk:", the command fails and the following message is given....

  by-7606S#issu runversion 6 slavesup-bootdisk:s72033-adventerprisek9_dbg-mz.v2 % The Standby image name specified [sup-bootdisk:s72033-adventerprisek9_dbg-mz.v2] does not match the previously specified image name [bootdisk:s72033-adventerprisek9_dbg-mz.v2]

  Conditions: Only seen when sup-bootdisk is the file system containing the image. Using disk0: does not show the same problems.

  Workaround: - Use "issu runversion slot" form of the command or specify bootdisk instead.

  - If using ATS scripts with HA package, use disk0: or disk1: instead.

- CSCsq81365

  Symptoms: Broadcast UDP traffic forwarded using the IP helper-address in a VRF may be leaked into the global table. The router is process-switching the broadcast packet and when generating the new packet it is not applying the required labels to keep the packet in the VPN.

  Conditions: Seen only for UDP traffic in an MPLS VPN.

  Workaround: There is no workaround. If forwarding of UDP traffic (such as Netbios) is not required, this can be turned off with the **no ip forward-protocol <protocol>** command.

- CSCsq84670

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

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

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

- CSCsq85044

  Symptoms: The Cisco Express Forwarding consistency checker may report that the prefix 224.0.0.0/4 is missing from the forwarding tables of line cards.

  %COMMON_FIB-4-LCPREFIXINCONST2: Slot 5/0 (5) prefix entry for 224.0.0.0/4 in FIB table IPv4:Default [scan-rp-lc] reason: missing

  Conditions: The problem will be seen if flow exporting version 5 or 9 is configured, and a routing table is then cleared with **clear ip route ***.

  Workaround: There is no workaround.

- CSCsq92440

  Symptoms: A router may crash when continuously executing the **sh ip mroute count | incl groups** command with large number of mroutes.

  Conditions: The symptom is observed only when unconfiguring a large number of static joins at a time or unconfiguring the class-map having large number of groups and executing the **sh ip mroute count | incl groups** command multiple times continuously. (Unconfiguration/configuration of a large number of static joins can be done only by using a class-map.)

  Workaround: Do not check **sh ip mroute count | incl groups** continuously when unconfiguring or configuring a large number of mroutes.

- CSCsq96843

  Symptoms: SIP crashes upon inserting SPA.

  Conditions: Observed on a SIP-400 when a SPA-2XT3/E3 SPA is inserted.

  Workaround: There is no workaround.

- CSCsr05501

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

  "% NBAR Error: hwidb could not found"

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

  Workaround: There is no workaround.

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

- CSCsr06707

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

  Conditions: Occurs when duplicated BGP router-id is received

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

- CSCsr07626

  Symptoms: Sub interface S9/3.161 reports output bandwidth utilization approx 25,000 times higher as it should be.

  Conditions: There has been a router replacement from 7609 to 7609s with new IOS (c7600s72033-advipservicesk9-mz.122-33.SRB2.bin) since May 9th, 2008.

Workaround: There is no workaround

- CSCsr18500

  Symptoms: Intermittent ping drops seen (one drop in every 10-11 packets) after reload of router, online insertion and removal (OIR) of line card, or stateful switchover (SSO).

  Conditions: Issue seen with basic back-to-back ping with IP address configured on interface.

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

- CSCsr20133

  Symptoms: Tracebacks seen while adding/looking up a prefix into the BGP table .

  Conditions: This happen if we are adding/lookingup a prefix which is a substring of an existing prefix in the BGP table.

  Workaround: There is no workaround

- CSCsr21670

  Symptoms: Sometimes see more routes than configured at "maximum-paths eibgp import" by "show ip route".

  Trigger: In a 2 RR setup, - Reloading RR1 and - shut/unshut on the RR2 - PE(ingress) interface on the RR2 side

  Condition: when we have multiple paths with same nexthop and are also candidates for multipaths (equal metrics). - when bestpath changes (router flap) from router with lower router id to higher one, multipath is also changing (which is correct) but does not remove the older multipath, which causes the problem.

  Workaround: - Restrict the no of configured multipaths to max real multipaths (unique next hops, in this case 2) - Problem solves itself after certain amount of time

- 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.

- CSCsr45961

  Symptoms: Following a PRE switchover, the VRF ARP table for a GE interface is not populated correctly which results in traffic drop. The problem will block MPLS forwarding after RPR+ switchover.

  Conditions: This is observed on PRE2 running 12.2(33)SB1 with RPR+ as redundancy mode.

  Workaround: The workaround is to ping the remote CE IP address from the PRE2.

  Further Problem Description: Problem is only seen on PRE2 after PRE switchover is performed. After switchover, PRE does not have the CE MAC entry in the ARP VRF table so the traffic which is sent towards the CE is dropped.

- CSCsr48563

  Symptoms: Taking care of some unnecessary error messages. The messages now appear under a debug flag ’debug pc debug’

  Conditions: The error messages are related to the FWSM module

  Workaround: There is no workaround.

- CSCsr48600

Symptom:

With WS-SUP32-GE-3B card, the physical structure of the device displayed in ANA is missing GigaEth port 1/9. The entPhysicalParentRelPos for Gi5/9 is coming as 9 which is clashing with Gi5/3.

Conditions: This is a problem specific to WS-SUP32-GE-3B

Workaround: There is no workaround

- 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**.

- CSCsr57636

  Symptoms: Symptoms: 7200 NPE-400 running 12.2SB ecountered bus error crash

  Workaround: There is no workaround

- CSCsr62529

  Conditions: Withdraws are not sent and updates are stuck when peers go down in large scale scenario. Has been seen when there is a neighbor configured as admin down (shutdown), or in idle state, from which the route was previously learned.

  Symptoms: bgp updates are not sent to peers, although most show commands signal that the route is getting sent. An example scenario is that **neighbor default-originate** does not send a default route if the 0.0.0.0/0 route is stuck in the **show ip bgp pending-prefix**, although it should ALWAYS send a default route, in theory, to the configured neighbor.

  Workarounds: Deleting "idle" neighbors has been shown to clear up some issues. Routes may clear from "pending" state by deleting neighbors that are in a shutdown state.

- CSCsr66286

  Symptoms: REP VLAN load-balancing is off set by 1 in **show interfaces trunk** output from configuration that is actually written in the edge port. This causes traffic on the boundary VLANs.

  Po1 : rep block port -2 vlan 6-10 "show int trunk" results as below.

  Port Vlans in spanning tree forwarding state and not pruned Po1 5-9 <--- off set by 1 Po2 1-10

  In the above case, configuring SVIs on each switch, VLAN 5 gets loop and vlan 10 is unreachable.

  Conditions: Occurs when VLAN load balancing is used with Resilient Ethernet Protocol (REP).

  Workaround: Disable boundary VLANs.

- CSCsr72301

  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.

- 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.

- CSCsr98999

  Symptoms: MUX-UNI + tag native : UDLD packets are sent on wrong vlan, this can lead to UDLD disabling the link .

  Conditions: MUX-UNI + tag native . In case of "vlan dot1q tag native" we notice this issue .UDLD packets are sent on wrong vlan packets are sent to vlan 1012 "PM vlan process (trunk tagging)" This has been reproduced in TAC lab in SRA, SRB, SRC

  Workaround: No Workaround exists

- CSCsu02975

  Symptoms: 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

- CSCsu05927

  Symptoms: IPV6 MTID not generated in LSP even when multi-topology is enabled. Conditions: If address family ipv6 related configuration is entered before multi-topology is enabled. Workaround: Enable ipv6 multi-topology before configure other address family ipv6 items.

- CSCsu06744

  Symptoms: Wrong BGP AS number is being returned when doing traceroute to any ipv6 prefix. Even if we traceroute to router's own ipv6 address we notice bgp as "2686" being returned while the router is running AS 7473.

  Conditions: This problem was noticed on SRB3 release and it looks like a cosmetic issue.

  Workaround: There is no workaround as this is a cosmetic issue.

- 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.

- CSCsu11161

  Symptoms: This bug will cover all the default-originate issues, specifically that have been found in 12.2 code

  Conditions: 1. Out-of-order generation of default-originate update (CSCek28763) 2. Default route adverised to neighbor with default-originate not configured. 3. After unconfiguring default-originate, default-route withdraw message not sent to the peer. (CSCsu05525) 4. After unconfiguring default-originate and issuing a hard reset , static default route not advertised to peer.

  Workaround: Please review each individual bugs above to see specific conditions and workarounds.

- CSCsu19056

  Symptoms: In Cisco SUP running image SRA & above, RLB may not install software shortcuts for user traffic. Because of this, SUP CPU might go higher than expected.

  Conditions: The issue occurs only if all of the following conditions are met:

  1) User traffic is configured to do SLB routing 2) Configure multiple static IP routes for the destination in the RLB vlan

  Workaround: Configure only one static IP route for the destination

  Further Problem Description

  Following is configuration snippets on which the problem can be seen, this is an illustration MWTCL06-SW1#sh run | inc ip route ip route vrf RLB 192.168.58.0 255.255.255.0 172.10.58.33 ip route vrf RLB 192.168.58.0 255.255.255.0 172.10.58.22

  for destination network 192.168.58.0, there are multiple static routes in RLB VLAN.

  To Work around, do the following. MWTCL06-SW1#conf t Enter configuration commands, one per line. End with CNTL/Z. MWTCL06-SW1(config)#no ip route vrf RLB 192.168.58.0 255.255.255.0 172.10.58.22

  MWTCL06-SW1#sh run | in ip route ip route vrf RLB 192.168.58.0 255.255.255.0 172.10.58.33

- CSCsu33006

  Symptoms: A VRF is setup with Multi-VRF Selection Using Policy-Based Routing (PBR). If we ping from a local PE1 (inside a specific VRF) to a specific destination, it works however, if we ping from PE2 (inside the same VRF), it fails.

  CE1---PE1---P---PE2---CE2

  The global static routes are not redistributed into IGP nor BGP global.

  Conditions: The issue occurs on a 7609 when the VRF is setup with Multi-VRF Selection Using Policy-Based Routing (PBR).

  When we put in ip vft fowarding or a route in the global table the traffic is forwarded with out problem. If these are not in place then the traffic fails

  CE---PE---P---P---PE <-----

  The issues occurs to be on the PE towards the CE.

  The issue was orignially seen on: Platform: 7609-S IOS: 12.2(33)SRB2 5 2 Route Switch Processor 720 (Hot) RSP720-3C-GE 6 2 Route Switch Processor 720 (Active) RSP720-3C-GE 7 20 ESM20G 7600-ES20-GE3C

  The issue was also seen with 12.2(33)SRB4.

  Workaround: If the IP VRF receive config on the int is removed, and "ip vrf forwarding vrf <name>" is placed under the int, the ping from remote PE works inside vrf <name>.

  Also if a global static route is added for the problem ip range on the PE with next-hop of CE, the ping from remote PE starts working again.

- 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.

- CSCsu49257

  Symptoms: fip timer timeout causes fip and cstn sticky to be deleted even though access-request is seen just before timeout and accounting after timeout. Causes access request and accounting start to head to different real.

  Conditions: Access request is seen just before fip timeout and accounting start after

  Workaround: Configure "delay sticky radiuf framed-ip 0"

- CSCsu59575

  Symptoms: When a 7200 NPEG1 is running 12.2(33)SRC1 and negotiation auto is configured on a RJ-45 Gigethernet interface the speed and duplex cannot be changed.

  Conditions: Workaround: The negotiation auto command has no effect on RJ-45 Gigethernet therefore leave it disabled which is the default.

- CSCsu73516

  Symptoms: Inventory doesnot distinguish b/w 1x and 10x ES-20 GE card.

  Conditions: SNMP query on entPhysicalDescr.

  Workaround: There is no workaround

- 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.

- CSCsu78906

  Symptoms: - %SYS-5-CONFIG_I Syslog massages are being generated on the device as if the configuration had been changed via SNMP: "%SYS-5-CONFIG_I: Configured from x.x.x.x by snmp" , even when those IP addresses are blocked via an SNMP ACL for the RW community string.

  Workaround: There is no workaround.

- CSCsu81838

  Symptoms: Memory leak occurs.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- 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.

- CSCsu84697

*OSPF adjacency fails to get established across vpls connected sites.

- CSCsu90010

  Symptoms: Cisco 7301 with PA-A3-OC3SMI and running Cisco IOS Release 12.2(33)SRC is unable to accept more then 4096 PVCs under **range pvc** command. Since the card is supporting maximum 4096 VCs, this could be considered expected behavior. However, there is inconsistency between different IOS versions and this bug is opened to address this issue.

  Conditions: Occurs when the **range pvc command** command is configured.

  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.

- 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.

- 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.

- 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.

- 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.

- CSCsv02214

  Symptoms: Customer is doing color aware policing ona 7200 vxr with NPE 400. Once the router is reloaded the conform-color config is removed from the startup config.

  Conditions: Issue is seen when the router is reloaded.

  Workaround: Include PIR (Peak Information Rate) command along with the CIR (Committed Information Rate)

- CSCsv04689

  Symptom: On a TACACS+ AAA client you may not see accounting for configuration changes that are done using a http client.

  Conditions: The problem has been observed in 12.2(44)SEE2 code and 12.2(25r)SEE1. The bug was reproduced with Firefox 3, IE7 and Cisco Network Assistant 5.3 seperately. Only one command is be logged to the TACACS+ server for a single http connection. Subsequent commands on that same connection are not logged till that connection times out.

  Workaround: configure the ip http timeout to change the max lifetime of a connection to the minimal (1 second). This is not a complete workaround any scripted commands that issue more than 1 configure command via http will not be logged. It would also mean that advantage of persistent http connection is lost

- 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.

- CSCsv05009

  Symptoms: %OSPF-4-FLOOD_WAR: error message may be seen for both type-5 and type-7 LSAs re-origination when the affected prefix is constantly flapping.

Conditions: This issue can be seen for a prefix constantly flapping that is being redistributed into OSPF on an ASBR connected to the backbone area via a NSSA. On the ASBR connected on the NSSA we can see the error message appearing for the re-origination of the type-7 LSA, while on the BB ABR/ASBR we see the same for the type-5 LSA that is originated.

Workaround: There is no workaround.

- CSCsv05263

  Symptoms: Supervisor 32 resetted after running internal command. test platform firmware get asic register r2d2 0 0 100 all

  Conditions: this command is available on earlier release. in latest, SRD or SXI, there is new format.

  Workaround: don’t run this commands. this command is for intenal debug purpose. test plat firm comp r2d2 acc reg print <instance> <offset> <count>

- 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.

- CSCsv06973

  Symptoms: Router crashes For Authentication RESPONSE with GETUSER and when getuser-header-flags is modified and sent.

  Conditions: TACACS single-connection is configured. When authorization is configured Telnet to router and removing authorization,telnet to router again

  Workaround: Do not use TACACS single-connection option.

- CSCsv07188

  Symptoms: Unable to configure PVC when **connect** command is configured.

  Conditions: Occurs Cisco 7200 routers.

  Workaround: There is no workaround.

- 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.

- CSCsv07858

  Symptoms: SNMP polling of ifIndex shows unknown, unconfigured VLAN.

  Workaround: There is no workaround.

- CSCsv10982

  Symptoms: BGP state is going in "IDLE" state in the output of "show ip bgp vpnv4 all sum" command while its in ACTIVE state.

Conditions: This symptom is observed while configuring password between the neighbors. When there is a password mismatch (one side is configured with MD5 password while other side is not) between two neighbors, BGP state is going in "IDLE" state in the output of "show ip bgp vpnv4 all sum" command while its in ACTIVE state.

Workaround: There is no workaround

- CSCsv13243

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

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

  Workaround: Configure subinterface in "non-native" mode.

- CSCsv14963

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

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

  Workaround: There is no workaround.

- CSCsv18034

  Symptoms: MAC limit does not work on the Hub in H-VPLS design.

  Conditions: HUB is c7600 with ES-20 or SIP-400 module.

  Workaround: There is no workaround

- CSCsv21403

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

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

  Workaround: There is no workaround.

- CSCsv22930

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

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Do not enable FRR between these routers.

- CSCsv24179

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

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

  Workaround: There is no workaround.

- CSCsv24908

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

Conditions: Occurs on a SIP-400 with SPA-2X1GE running BGP and GRE tunnels. Interface 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.

- CSCsv27480

  Symptoms: VRRP virtual MAC address is stored as a dynamic, instead of static, entry after a reload.

  Conditions: The symptom is observed when VRRP is configured on an SVI with xconnect pseudowire:

  interface Vlan X ip address 10.0.0.1 255.255.255.0 vrrp 2 ip 10.0.0.254 xconnect vfi VRRP_3201

  Workaround: Use the **shutdown** followed by the **no shutdown** commands on the SVI (VLAN interface).

- CSCsv27670

  Symptoms: Unable to bring up PPPoE sessions on 7600.

  Conditions: This issue only affects a CISCO 7600 router having a QinQ interface with multiple ranges for the inner vlan, e.g:

  interface GigabitEthernet 1/0/0.100 access encapsulation dot1q 100 second 50-100,125,150-300 pppoe enable group global

  Workaround: Two workarounds exists a] When the problem is seen, reconfiguring the interface will fix the issue. b] modify the config such that only 1 range is present per subinterface. This would mean that the above config will have to be replaced as

  interface gig 1/0/0.100 access encap dot1q 100 second 50-100 pppoe enable group global

  interface gig 1/0/0.101 access encap dot1q 100 second 125 pppoe enable group global

  interface gig 1/0/0.100 access encap dot1q 100 second 150-300 pppoe enable group global

- CSCsv31126

  Symptoms: SNMP walk of the mplsTunnelTable does not return all configured MPLS TE (Traffic Engineering) tunnels

  Conditions: N/A

  Workaround: Perform SNMP walk of mplsTunnelTable specifying the mplsTunnelIndex

  This index is correlates to the integer in tunnel interface name, which can be shown by the IOS CLI "show mpls interface" or snmpwalk of ifDescr

  Alternative workaround: Use the IOS CLI to obtain information about MPLS TE's via "show mpls traffic-eng tunnels"

- CSCsv32057

  Symptoms: In a 7600 with Sup RSP720-3CXL-GE and version 12.2(33)SRC2, a port channel is made of 2 interfaces TE (module WS-X6704-10GE). A "show interface port-ch X" will show: reliability 255/255, txload 0/255, rxload 0/255

whereas the "show interface ten A" will show: reliability 255/255, txload 125/255, rxload 62/255

and the "show interface ten B" will show: reliability 255/255, txload 125/255, rxload 188/255

Conditions: Normal working conditions.

Workaround: No known workaround.

- CSCsv33847

  Symptom:

  ifInDiscards counts up when ES20 recived CRC error packets.

  Conditions: 7600-ES20-GE3C 12.2(33)SRC1,12.2(33)SRC2 The problem does not affect 12.2(33)SRC.

  Workaround: Further Problem Description:

- 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.

- CSCsv34397

  Symptoms: Users(atm)--------7200--------dhcp_server

  We have the following scenario where the 7200 uses ATM subinterfaces between with the users in routed mode (encap RFC 1483Routed). The 7200 does the dhcp relaying between the 2.

  After an upgrade to 12.2(31)SB12 we cannot ping the clients from the 7200, even though they are getting an ip address from the DHCP server. There is also a /32route and an arp entry in the 7200 for the client.

  There is no connectivity across the ATM pvc when using DHCP

  Conditions: After an upgrade to 12.2(31)SB12.

  Workaround: There is no valid workaround at the moment. In 12.3 the issue was not seen.

- CSCsv34532

  Symptoms: The packet length field incorrectly indicates the length is "zero".

  Conditions: During any use of PPPoE, the length is not available. Thus the law enforcement device that catches the stream is not able to calculate correctly.

  Workaround: There is no workaround.

- 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.

- CSCsv36312

  Symptoms: parser config cache interface issue when using uRPF on 7600 PFC3

  Conditions: This symptom is observed on a 7600 series router with PFC3 and IOS 12.2(33)SRC2. You configure Unicast RPF check on a per-interface basis, but the PFC3 supports only one Unicast RPF method for all interfaces that have Unicast RPF check enabled. When you configure an interface to use a Unicast RPF method that is different from the currently configured method, all other interfaces in the system that have Unicast RPF check enabled should use the new method. However when parser config cache interface is enabled the interface is not changed. when disabling it all goes fine. This is cosmetic as "show mls cef rpf" shows the correct operational mode for the router.

  Workaround: There is no workaround.

- CSCsv36549

  Symptoms: The issue is seen when version is 12.2(33)SRBx and the feature set is ipservice. ex) c7600s72033-ipservicesk9-mz.122-33.SRB4

  VRF cannot be configured on GRE tunnel interface. When we try to configure "ip vrf forwarding" under interface tunnel, it indicates "mls mpls tunnel-recir" should be configured before configuring the VRF, but "mls mpls tunnel-recir" is not supported on the Feature set of ipservice.

  7600(config)#int tunnel 1 7600(config-if)# 7600(config-if)#ip vrf forwarding test The module in slot 2 requires that the global configuration command 'mls mpls tunnel-recir' be applied before VRF forwarding is enabled on a tunnel interface

  7600(config-if)# 7600(config-if)#mls mpls tunnel-recir ^ % Invalid input detected at '^' marker.

  Conditions: - 7600 installs ES20 - This is vrf-lite configuration without MPLS. - The issue does not occur on 12.2(33)SRC train with same feature set,ipservice. ex) c7600s72033-ipservicesk9-mz.122-33.SRC2

  - The issue does not occur on the other feature set, advipservice. ex) c7600s72033-advipservicesk9-mz.122-33.SRB4

  Workaround: It seems it might be workaroud.

When in advance the VRF is configured on GRE tunnel interface with the other feature set advipservice and then reloading the 7600 with the feature set of ipservice, the vrf is configured on GRE tunnel interface correctly.

- 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.

- CSCsv37543

  Symptom: GRE/IPsec tunnel on a VPN SPA module will not come up fully if source and destination addresses overlap with another tunnel interface. The problem persists even after fixing the configuration to use separate source or destination addresses and even removing/reapplying tunnel interface configurations.

  Conditions: Source and destination addresses both overlap on two or more tunnel interfaces for GRE/IPsec on a 6500/7600 device with the VPN SPA module. This is seen in 12.2.33.SXH code.

  Workaround: Adjust the configurations and reload the chassis. Alternatively, you can reload the VPN module by itself and then removing/reapplying the tunnel interface configurations as well.

- 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.

- CSCsv41067

  Symptom:

  7206VXR (NPE-G1) got bus error crash at invalid in normal mode.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsv51261

  Symptoms: In c7600 12.2(33)SRB2 to SRB4, PE doesn't install RIP default route from CE in its routing table (default with administrative distance 120) as PE is preferring default from MPBGP PE peer (administrative distance 200).

  Problem is easy to reproduce in lab (customer's lab as well as IOU) and exists in SRB2, SRB3, SRB4 however does NOT exist in SXF8, SRA1.

  Conditions: PE doesn't install RIP default route from CE in its routing table

  Workaround: injecting default route on PE under ipv4 RIP address-family via command "default-information originate route-map foo" where route-map foo is empty.

  "route-map foo permit 10"

- CSCsv54863

  Symptoms: If auto-enrollment is configured in IOS trustpoint, and some percentage is specified (like "auto-enrollment 50"), then automatic re-enrollment is started before certificate expiration date. If Certification Authority (CA) is in manual granting mode, these requests are not granted without human's attention. When this happens, router tries to make autoenrollment attempts for 1 day only (with default PKI timers). After last autoenrollment attempt, router prints this message:

  *Nov 5 04:45:17: %PKI-3-CERTPENDERR: Failed to receive pending certificate during enrollment

  After that, router stops making further enrollment requests and deletes the certificate.

  In other words, certificate is deleted in 1 day after starting auto-enrollment, even if it's not expired yet.

  Conditions: - Auto-enrollment is configured with some percentage <100% in IOS trustpoint:

  crypto pki trustpoint TEST auto-enroll 50

  - The CA is in "manual granting" mode. Issue occurs both with Microsoft CA and IOS CA.

  Further Problem Description

  This bug can bring VPN network down if VPN router is configured with certificate authentication for IPsec tunnels and auto-enrollment occurs on the weekend. If the CA is in manual granting mode and noone is available for 2 days to grant a certificate request manually on CA, the certificate is deleted on weekend.

  Workaround: 1. Disable autoenrollment ("no auto-enroll").

  or

  2. Change the CA mode from manual grant mode to auto grant mode

or

3. Increase the number of autoenrollment requests and the interval between them to maximum possible values:

crypto pki trustpoint ca enrollment retry count 100 enrollment retry period 60

This will allocate 4 days for auto enrollment attempts instead of 1 day by default. This is longer than typical 2-days weekends.

- CSCsv56160

  Problem Description: BGP session flapping due to : Oct 5 05:03:36.057 PDT: %BGP-5-ADJCHANGE: neighbor 192.168.44.185 Down BGP Notification sent Oct 5 05:03:36.057 PDT: %BGP-3-NOTIFICATION: sent to neighbor 192.168.44.185 1/2 (illegal header length) 2 bytes FFFF Oct 6 14:55:16.812 PDT: %BGP-3-NOTIFICATION: received from neighbor 192.168.44.185 1/1 (header synchronization problems) 0 bytes Oct 6 14:55:16.812 PDT: %BGP-5-ADJCHANGE: neighbor 192.168.44.185 Down BGP Notification received

  Condition: When "ip tcp selective-ack" enabled.

  Workaround: Remove "ip tcp selective-ack".

- CSCsv59980

  Symptoms: MTU is limited to 7673 for DS3 interfaces on OSM-1CHOC12/T1-SI.

  Conditions: No Conditions.

  Workaround: 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

- CSCsv65187

  Symptoms: Incorrent entPhysicalModelName listed in the MIB

  Workaround: There is no workaround.

- CSCsv65824

  Symptoms: From Cisco7600, unable to ping a directly connected device.

  Conditions: - This issue is seen in Cisco7600 running 12.2(33)SRCx releases. - When ping fails, interface status is up/up, with no errors on the interface. 100% ping loss. - Issue is reported for the device connected on FlexWAN modules, or SIP-400 modules. - "show ip cef switching statistics" report: 7600A#show ip cef switching statistics Reason Drop Punt Punt2Host RP LES Unknown input if 10 0 0 <<== - After sending 10 pings, and 100% failure: 7600A#show ip cef switching statistics Reason Drop Punt Punt2Host RP LES Unknown input if 20 0 0 <<==

  Workaround: Reload the Cisco7600 in issue.

Fix should be available in 12.2(33)SRC4, 12.2(33)SRD1 or later.

- 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.

- 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/no shut** under the service instance.

- 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.

- 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.

- CSCsv80456

  Symptoms: The following SACL statement will never match for any session packet.

  access-list 100 permit tcp any any established

  Conditions: Occurs when using Cisco Intelligent Services Gateway (ISG) downstream traffic to the subscriber.

  Workaround: There is no 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.

- CSCsv84808

  Symptoms: After SSO switchover, restarting node could not respond NACK to the incoming Srefresh and ignore it as epoch mismatch. It would result in refresh hold time expiration on neighbor node.

  Conditions: Symptom is observed under the following condition.

  - RSVP Graceful Restart is configured - RSVP Refresh Reduction is configured - Restarting node is Tail-end of TE tunnel and connecting to the IOS-XR Midpoint

  Workaround: disable refresh reduction, use normal refresh scheme(Path/Resv) instead

- CSCsv85052

  Symptoms: Crash observed when "ispf" is issued in vty with ip routing disabled in another terminal

  Conditions: Ip routing should be disabled (no ip routing).

  Workaround: No Work-around

- CSCsv85641

  Symptoms: IPv6 BGP neighb gets activated under IPv4 AF by changing neighbor description or by sh/no sh neighbor

  Conditions: When having 2 ebgp neighbors peering under ipv6 AF and with no neighbor <ipv6 neighbor address> activate configured under ipv4 AF, if we change the description of the neighbor or shut/no shut the neighbor it gets activated under ipv4 AF. show ip bgp ipv4 unicast summary shows the neighbor and we can see in the config that the "no" is removed from "no neighbor <IPv6 neighbor IP> activate" under ipv4 AF.

  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.

- CSCsv87091

  Symptoms: When 7600 router is conntected via PW with a XR, the mpls ping request is sent with no RA label, even though type2 is supported type. Conditions: This happens when the IOS device do not support CC type locally but is supported by the remote device. This causes IOS device to send MPLS OAM packet with wrong CC type. Workaround: On the remote device, disable the unsupported CC type so that only the IOS supported CC type is configured on PW.

- CSCsv87997

  Symptoms: DHCPv6 relay process crash on Actice RP.

  Conditions: Unknown at this time.

  Workaround: Unknown at this time.

- 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.

- 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.

- 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.

- CSCsv94560

  Symptoms: EoMPLS packet send over VC is reflecting on time when VC is coming up. Reflection will not happen always and just for a few first packet send over VC.

  Conditions: This problem happen when VC is coming up. RSP/VS720 in PFC3C mode are not affected.

  Workaround: Configure no route rate limiter to zero: mls rate-limit unicast ip icmp unreachable no-route 0

- 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.

- CSCsv98488

  Symptoms: when cef is enabled, dot1Q frames with HSRP virtual mac destination address are forwarded. it should be discarded on the router.

  Conditions: with dot1Q tag and cef is enabled.

  Workaround: disable cef.

- CSCsv99150

  Symptoms: Status LED of 2+4 port GE-WAN Module not showing proper status(EVEN THE LINK IS UP).

  Conditions: After reload/upgrading from 12.2(33) SRB2 to SRB-4.

  Workaround: The 'sh/no sh' of the affected WAN interface will resolve the issue locally in DE setup. But the Customer reported that the workaround hasn't helped in resolving the issue.

- CSCsv99443

  Symptom:

HSRP group will become Active on a reloaded router even if there are already Active routers in this group.

Using "standby delay reload" has no effect to delay the HSRP process from entering Active state at boot time.

Condition:

Routers which have long hardware initialisation times or have a lot of configuration exceed the maximum time which HSRP uses to determine if a reboot has happened recently. The reload delay is then ignored, and any interfaces which are not fully initialised will not accept incoming Hello messages from adjacent HSRP routers.

Workaround: Configure "standby delay minimum" instead.

- 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

- CSCsw20213

  Symptom: When a T1 is taken out of the MLP bundle it takes around 7 for the mlp bundle to declare it down and as a result of that packet going through the MLP bundle are lost

  Conditions

  Removing a T1 out of the MLP bundle

  Workaround no workaround is available.

- CSCsw20267

  Symptom

  When MLP members are across SPAs and protected by APS , after APS failure some of the MLP with the new member links are not part of the routing table

  Condition

  Failing APS on MLP

  Workaround no workaround

- CSCsw22436

  Symptom: When active and standby devices are simultaneously reloaded, SLB's load is not reported to GSS, because of which GSS considers SLB is down.

  Conditions: When running KAL-AP between GSS and IOS-SLB HSRP address, upon simultaneous reload of active and then standby device, the IOS-SLB cannot recognize the KAL-AP tags anymore. This is seen with 12.2 SRC1 and SRC2 supervisor images.

  Workaround: Unconfigure and reconfigure *peer* command in SLB under *ip slb capp udp*.

- 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.

- CSCsw24959

  Symptom:

  Router crashes when VT has lot of rate limit configuration.

  Conditions: Under VT configure lot of rate-limit configs.

  interface Virtual-Template3 description For_PPPoE_Unlim_subscribers rate-limit outputaccess-group 2070 128000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2072 128000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2073 64000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2074 64000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2077 64000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2079 64000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2081 64000 131072 131072 conform-action transmit exceed-action drop rate-limit outputaccess-group 2082 256000 262144 262144 conform-action transmit exceed-action drop

  Workaround: Configure the same under real interface. issue is not seen

- CSCsw26414

  Symptoms: Online diag fails to detect internal device locked up:

*Dec 2 19:16:00.315: %DIAG-SP-6-TEST_RUNNING: Module 6: Running TestSPRPInbandPing{ID=2} ...

*Dec 2 19:16:08.451: %DIAG-SP-6-TEST_OK: Module 6: TestSPRPInbandPing{ID=2} has completed successfully

Conditions: Device goes into BAD state for unknown reason.

Workaround: There is no workaround.

- CSCsw28023

  Symptoms: Host routes are not getting installed

  Conditions: This happens when vserver are moved from operational to non-operational state and then again back to operational state

  Workaround: Use only the "advertise" command under the vserver and not the "advertise active" command. The adverise will not remove the host routes even when the reals are down.

- 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 usualy happen 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.

- CSCsw34351

  Symptoms: Customer is unable to remove or modify some MLS rate limiters.

  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 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.

- CSCsw36793

  Symptoms: PRDI alarm is declared incorrectly on SPA-1XOC48POS

  Conditions: PAIS received by the interface.

  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.

- CSCsw37536

  Symptoms: Traffic received over TE Tunnel is not forwarded after power cycle.

  Conditions: The ingress linecard is a WS-X6704-10GE with a WS-F6700-DFC3B. The behavior has been seen on after power cycle when running 12.2(33)SRB3.

  Workaround: There is no known workaround.

- 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.

- CSCsw40048

  Symptoms: **vpdn logging** can't be deleted in recent 12.4T and 12.2 releases

  Conditions: Normal operation once **vpdn logging** or any associated command is issued.

  Workaround: Issue command **no vpdn logging cause normal** and then issue **no vpdn logging**

- CSCsw42724

  Symptoms: 2 x RSP720 running 12.2(33)SRC2 can't reach SSO terminal state but Terminal state reached for (RPR) instead

  Conditions: in case in router EIGRP context under address-family ipv4 vrf xxx trying to filter routing updates with the distribute-list

  here's an example:

  redundancy main-cpu auto-sync running-config mode sso

  interface GigabitEthernet1/8.5 encapsulation dot1Q 5 ip vrf forwarding INET ip address 10.174.194.169 255.255.255.252 ! interface GigabitEthernet1/8.6 encapsulation dot1Q 6 ip vrf forwarding INET ip address 10.174.194.141 255.255.255.252

  router eigrp 100 no auto-summary ! address-family ipv4 vrf INET autonomous-system 400 network 10.174.194.0 0.0.0.255 no auto-summary default-metric 10000 1 255 1 1500 == distribute-list NODEF in GigabitEthernet1/8.5 distribute-list ONLYDEF out GigabitEthernet1/8.5 == exit-address-family

  Workaround: And If I delete the following config strings == distribute-list NODEF in GigabitEthernet1/8.5 distribute-list ONLYDEF out GigabitEthernet1/8.5 ==

  RSPs reach SSO mode

  7606#conf t Enter configuration commands, one per line. End with CNTL/Z. 7606(config)#router eigrp 100 7606(config-router)#address-family ipv4 vrf INET 7606(config-router-af)#no distribute-list NODEF in GigabitEthernet1/8.5 7606(config-router-af)#no distribute-list ONLYDEF out GigabitEthernet1/8.5 7606(config-router)#^Z 7606#wr Building configuration... [OK] 7606#reload Proceed with reload? [confirm] Cisco IOS Software, c7600rsp72043_sp Software (c7600rsp72043_sp-ADVIPSERVICESK9-M), Version 12.2(33)SRC2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu 18-Sep-08 03:46 by prod_rel_team *Dec 11 09:53:40.167: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded *Dec 11 09:53:39.887: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode *Dec 11 09:53:41.047: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)

  7606#show redundancy Redundant System Information : ------------------------------ Available system uptime = 4 minutes Switchovers system experienced = 0 Standby failures = 0 Last switchover reason = none

  Hardware Mode = Duplex Configured Redundancy Mode = sso Operating Redundancy Mode = sso Maintenance Mode = Disabled Communications = Up

  Current Processor Information : ------------------------------ Active Location = slot 5 Current Software state = ACTIVE Uptime in current state = 4 minutes Image Version = Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 12.2(33)SRC2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu

18-Sep-08 03:16 by prod_rel_team BOOT = sup-bootdisk:c7600rsp72043-advipservicesk9-mz.122-33.SRC2,1; CONFIG_FILE = BOOTLDR = Configuration register = 0x2102

Peer Processor Information : ---------- Standby Location = slot 6 Current Software state = STANDBY HOT Uptime in current state = 1 minute Image Version = Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 12.2(33)SRC2, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Thu 18-Sep-08 03:16 by prod_rel_team BOOT = sup-bootdisk:c7600rsp72043-advipservicesk9-mz.122-33.SRC2,1; CONFIG_FILE = BOOTLDR = Configuration register = 0x2102 7606#

- 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.

- CSCsw51126

  Symptoms: High CPU utilization in virtual Exec process on TTY #, and vty session hang.

  Conditions: Connect via telnet(vty) to the router and execute setup command. After the vty idle timeout, this session would hang and you can’t clear vty but only recover using force switchover

  Workaround: Not allow that a session timeouts where executed the setup command.

- 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 configurationss with SIP400 and channelized SPAs.

  Workaround: There is no workaround.

- 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.

- CSCsw72640

  Symptoms: Dot1q routed subinterfaces for vlans less than 1005 are not accounted for in the output of the "show platform hardware capacity vlan" CLI command.

  Conditions: Configure a dot1q subinterface (confg subinterface and then encap command) with vlan number less than 1005, and issue the show command prior and after the configuration. See that the vlan used count is not decremented.

  Workaround: Use the "show vlan internal usage" command to see vlans used internally.

- CSCsw73391

  Symptoms: Multicast groups are denied when the limit for IGMP has been reached, because the limit never decrements.

  Conditions: The command "ip igmp limit" is used.

  Workaround: Use the command "clear ip igmp group".

- CSCsw73863

  Symptom:- ID’s allocated from DHCP are getting leaked and it leads to box getting reloaded.

Conditions:- Box is configured as ISG-DHCP with 24k sessions flapping every 10-12 minutes.

Workaround: There is no workaround.

- CSCsw74573

  Symptom: PPTP traffic does not get NAT'ed when Static NAT is configured on interfaces having PPTP sessions on it. NAT translations do not get created for the GRE.

  Conditions: Cisco 7600 series router running 12.2(33)SR based images.

  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 HotICE 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.

- CSCsw77313

  Symptoms: The command "login", executed at exec, allows us to change login username. Now if we have AAA enabled on the box for whatever combination of username/password show users will report always the new user.

  Conditions: Enable AAA authentication on the box.

Workaround: There is no workaround.

- CSCsw78369

  Symptoms: Serial interface remains inactive in the multilink bundle, though the serial interface is UP

  Conditions: The issue is seen when you do 'shut' and 'no shut' of the serial interface that is part of multilink interface

  Workaround: Reconfigure serial interface with mutilink configs

- 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.

- CSCsw83626

  Symptoms: When 7600 is connected to Juniper/other boxes, 7600 accepting the peer asking for imposition rewrite option when negotiating vc type 4.

  Conditions: MPLS AToM configuration with vc type 4 could create interoperability issues.

  Workaround: The workaround is not to use the peer with imposition rewrite option.

- 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.

- 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.

- CSCsw93094

  Symptoms: The policy-map on ATM in SIP200 displays 20Bytes overhead for each matched packet whereas in SIP400 the detected overhead is 16Bytes.

  Conditions: SIP200. 12.2(33)SRD

  Workaround: There is no workaround

- 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.

- CSCsw96606

  Symptoms: - C72k NPE-G2 and PA-GE module - 12.4(15)T7 and T8 - If service-policy with QoS config is attached to the PA-GE interface, the device crashes *after reload*.

  Conditions: - Service policy attached to PA-GE interface

  Workaround: - Do not apply service-policy to PA-GE interface

- CSCsw99768

  Symptoms: Malformed update in MDT environment with RR clients.

  Conditions: On configuring MDT on an RR client, the RR would add the source AS ecomm attribute when reflecting client routes. As such we would have duplicate attributes and the peer would detect this as a malformed attribute.

  Workaround: There is no workaround

- 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.

- CSCsx03219

  Symptoms: During functional test of "sessions per-vc limit" got unexpected results - router allows less sessions then configured. Router counts the session as active despite it has been dropped by PPPoE

  Conditions: PADR larger then supported (currently 544 octets).

  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.

- CSCsx06049

  Symptoms: When doing MPLS-to-IP with egress ACL applied, packets may be punted to RP and dropped when rate-limits are hit.

  Conditions: When IP egress path has loadbalance paths, shutting down and bringing the one of the paths back causes this issue.

  Workaround: 1. Remove and reapply the egress ACL 2. exclude prefix in LDP or use pure IP on ingress

- 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.

- 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.

- CSCsx16152

  Symptoms: Under unique circumstances erroneous routing prefixes may be added to the routing table.

  Conditions: When the DHCPv6 relay feature is enabled and a router receives a normal DHCPv6 relay reply packet, this may lead to an erroneous route being added to the routing table.

  Workaround: No workaround except turning off DHCPv6 relay.

- CSCsx17446

  Symptoms: Both tunnel and non tunnel interfaces are chosen as nexthop when tunnel metric is lower than isis interface metric. The correct way shall only chose tunnel interface with lower metric as nexthop. Conditions: This happens when there are equal cost paths exist and tunnel metric is lower than isis metric and incremental spf is enabled.

  Workaround: clear isis * or any other way to trigger a full spf will correct this problem

- 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.

- 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.

- CSCsx21886

  Symptoms: The following error may be seen:

  Jan 20 06:22:09.043: Config Sync: Starting lines from MCL file:

  -mls ip slb purge global

  Conditions: This is seen when two different images are running on redundant supervisors, and only one of which has the fix for CSCsr99933.

  Workaround: There is no workaround.

- 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.

- 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.

- 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**.

- CSCsx34506

  Symptoms: If a packet is received on an interface in the Olist with no active PIM neighbor and RPF check fails, a PIM hello is triggered.

  Conditions: Problem seen in environments where there are two routers sending different multicast streams to receivers on the same subnet. A PIM neighbor cannot be established in this scenario because both routers need to be a PIM DR.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsx44223

  Symptoms: "show version" shows wrong bandwidth for M1T-T3+ pa Documented is 90 BW but its defined in IOS as 100 BW

  Conditions: Execute "show version" CLI having the M1T-T3+ pa in router

  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

- 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.

- CSCsx52197

  Symptoms: Standby supervisor in a C7600 is reloading in a loop due to bulk-sync failure caused by PRC mismatch.

  Logs:

  Config Sync: Bulk-sync failure due to PRC mismatch. Please check the full list of PRC failures via: show redundancy config-sync failures prc

  Config Sync: Starting lines from PRC file: -ip sla reaction-trigger <x> <y>

Conditions: This is seen on a C7600 running 12.2(33)SRB5.

Workaround: Disable 'ip sla' configuration.

- CSCsx55265

  *OSPF adjacency fails to get established across vpls connected sites.

- 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.

- 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.

- 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.

- CSCsx61043

  Symptoms: c7600 don't counter increment on output of 'show interface counter etherchannel' command. The correct output is shown when exec 'show interface' command.

  Conditions: This issue were confirmed on Sup32/Sup720/RSP720 with 12.2(33)SRC3.

  Workaround: Use 'show interfaces counter' commnad instead 'etherchannel' option.

- 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.

- CSCsx69437

  Symptoms: Memory leak causes the I/O mem to be depleted.

  Conditions: Occurs for a certain multicast traffic where packets' length includes padding are being fast switched

Workaround: No Workaround

- CSCsx73770

  Symptoms: A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  Conditions: This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  Workaround: The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

- 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.

- 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.

- CSCsx79137

  Symptoms: - A T3 serial interface default bandwidth is 44210

  interface Serial1/0 no ip address shutdown dsu bandwidth 44210 framing c-bit cablelength 10 serial restart-delay 0

- However, when show int , it is showing a T1 BW as 34010

  Serial1/0 is administratively down, line protocol is down Hardware is M2T-T3 pa MTU 4470 bytes, BW 34010 Kbit, DLY 200 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation HDLC, crc 16, loopback not set Keepalive set (10 sec) Restart-Delay is 0 secs Last input never, output never, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max)

  - This will happen to both PA-T3 or PA-T3+

  Conditions: This problem happen under normal condition. It often happen when card first insert into the chassis.

  Workaround: Sometime reload will help clear the problem and show correct BW afterward. However, this is not guarantee.

- CSCsx82365

  Symptoms: After a reload and a new session of LDP comes up, LDP does not immediately send all of its IP addresses across the LDP session to its LDP peer. Under certain condition, this could cause up to one minute of traffic loss in an MPLS network.

  Conditions: LDP enable for the first time on a router and while LDP is initializing, new interfaces are coming up. The IP address of some of those interfaces may not get sent to the LDP peer. If those missing addresses are the next hop for some route on the LDP peer then MPLS traffic for those routes get dropped.

  Workaround: If LDP-IGP Sync feature is available, enable LDP-IGP sync under the routing protocol and configure "mpls ldp igp sync delay 60" on the interface(s). The issue also resolves by itself after one minute.

- 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.

- 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.

- CSCsx96115

  Symptoms: Memory Alignment error observed on Cisco 10000 router at customer site.

  Conditions: Causes packet drops and high CPU usage..

Workaround: There is no workaround.

- CSCsx97093

  Symptoms: When trying to parse a callback string attribute in an ACCESS-ACCEPT, which has no callback value, RADIUS/DECODE fails: *Feb 24 16:04:22.252: RADIUS: Received from id 1645/68 10.48.88.121:19645, Access-Accept, len 52 *Feb 24 16:04:22.252: RADIUS: authenticator 49 7C 52 33 F8 BF 21 49 - 6C EF EC 2C 6D 09 92 BD *Feb 24 16:04:22.252: RADIUS: Vendor, Cisco [26] 32 *Feb 24 16:04:22.252: RADIUS: Cisco AVpair [1] 26 "lcp:callback-dialstring=" *Feb 24 16:04:22.252: RADIUS(00000000): Received from id 1645/68 *Feb 24 16:04:22.252: RADIUS/DECODE: convert VSA string; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: cisco VSA type 1; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: VSA; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: decoder; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: attribute Vendor-Specific; FAIL *Feb 24 16:04:22.252: RADIUS/DECODE: parse response op decode; FAIL

  Conditions: Any of the following callbacks fail parsing when configured with NULL value: "arap:callback-dialstring=" "slip:callback-dialstring=" "shell:callback-dialstring=" "lcp:callback-dialstring="

  Workaround: NA

- CSCsx97605

  Symptoms: Although CISCO-RTTMON-MIB is listed as "active" in IOS 12.2(33)SRC3, it appears to not be completely implemented. Certain parts which are essential for UDP-Jitter measurements are missing:

  rttMonJitterStatsOWMinSDNew - 1.3.6.1.4.1.9.9.42.1.3.5.1.52 rttMonJitterStatsOWMaxSDNew - 1.3.6.1.4.1.9.9.42.1.3.5.1.53 rttMonJitterStatsOWMinDSNew - 1.3.6.1.4.1.9.9.42.1.3.5.1.54 rttMonJitterStatsOWMaxDSNew - 1.3.6.1.4.1.9.9.42.1.3.5.1.55

  Conditions: This was first seen on a Cisco 7200 NPE-G2 with 12.2.33SRC3 used for IP SLA UDP-Jitter measurements.

  Workaround: - ignore all the OW objects in rttMonJitterStatsEntry

  - use the rttMonLatestJitterOper instead

- CSCsy04562

  Symptoms: 'Show inventory' command does not provide any output

  Conditions: 7200 running 12.2(33)SRC and SRD with feature C7200-SPSERVICESK9-M.

  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.

- CSCsy05044

Symptoms: In an MVPN setup and on a decap PE, symptom of this problem is the incorrect appearance of an (S,G) entry in the context of a VRF as well as one in the global context. The (S,G) in the global table is the only one required in this case.

See CSCef08631 for a possible root cause on one platform.

Conditions: This problem affects 12.2(33)SRB3.

On a decap PE, the platform may incorrectly not remove the outer tunnel header on an incoming MVPN data packet. This results in the incorrect creation of an (S,G)

Correct behavior is for the platform code to decapsulate the tunnel header and do a second lookup on the appropriate VRF table for the VRF in question. It is possible that decapsulation has not been done before the second lookup. This results in a failure to find the entry in the VRF and hands the packet to multicast packet input software. This software gets a packet with VRF context mismatching that of its input interface. A second (S,G) entry is incorrectly created in the context of the VRF.

Conditions causing CSCef08631are described below:

Multicast global entries leak into the VRF table on cat6k when sending packet size is greater than 1480 bytes. This happens on Decap PE when Encap PE has the ethernet interface with default MDT MTU 1500 bytes. The problem is due to incorrectly handle the fragmentation since the receiving cat6k cannot reassemble the frames in hardware before the decapsulation.

Workaround: There is no workaround if conditions in CSCef08631 are not causing this problem and platform is different from that in CSCef08631. Otherwise, a possible workaround is to send packets of size less than 1480 bytes.

- 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.

- 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.

- CSCsy09168

  Symptoms: Due to known limitation of the sup720 GRE tunnels must have unique source interfaces to configure a GRE tunnel in hardware. If there are multiple GRE tunnels using the same source interface and configured to support multicast, multicast traffic is not forwarded. The packets should be processed in software and forwarded at the expense of the CPU.

  Please reference informational BUG CSCdy72539 regarding SUP-720 requirements for GRE tunnels in hardware.

  Conditions: 1. SUP 720 configured with muliple GRE tunnels using the same source interface. 2. PIM configured on the tunnels interfaces to support multicast-routing.

  Workaround: 1. Configure unique source interfaces for each GRE tunnel configured. 2. If unique source interfaces ar not possible disable IP mroute-cache and force multicast in software path.

- 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.

- CSCsy17364

  Symptoms: ARP packets dropped in egress on SIP-200.

  Conditions: service-policy with marking applied on the interface (with "set ip precedence" or "police ... set-prec-transmit").

  Workaround: Remove the marking.

- CSCsy26370

  Symptoms: Router carshes at af_policer_get_class_drops.

  Conditions: Router crashes while attaching policy under another policy.

  Workaround: There is no workaround.

- CSCsy26443

  Symptoms: The forwarding entries for a route learned from iBGP nexthop & local CE nexthop may show up as DROP, if both the NEXTHOP addresses are same.

  Conditions: The iBGP nexthop address & local CE nexthop address has to be same. One is in GLOBAL table & another one is in VRF table. So, this is allowed. However, due to the bug, BGP will fail to instal the right label entry in forwarding.

  This is a dayone issue.

  Workaround: Avoid using same address for the iBGP & local CE nexthop.

- 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.

- CSCsy29604

  Symptoms: CEF entry is incorrect for the imported (from another VRF) route which has the nexthop in GOBAL/DEFAULT table.

  Conditions: Route shall be pointing to the GLOBAL/DEFAULT table in one VRF. It shall be imported by another VRF. The CEF entry in second VRF will be be wrong.

  Workaround: Instead of importing the internet (static) route from another VRF, you could add a static route in this VRF itself.

- 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

- 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.

- 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.

- 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).

- 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.

- 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.

- 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.

- CSCsy87385

  Symptoms: For IPv6 adjacencies, MTU is incorrectly programmed.

  Conditions: Occurs with simple IPv6/6PE setup.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsz00624

  Symptoms: ISSU with stateful switchover (SSO) may cause router to crash.

  Conditions: Occurs on Cisco 7600 routers when SSO occurs between Cisco IOS Release 12.2(33)SRC4 and SRB5.

  Workaround: There is no workaround.

- 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.

- CSCsz11749

  Symptom Framed route downloaded from the radius as a "per-user" attribute is not getting installed.

  Conditions: Customer saw this issue on a 7600 running 12.2(33)SRC3.

  Workaround: Do not use an SP featureset image but instead us an Advanced IP Services featureset image.

Open Caveats—Cisco IOS Release 12.2(33)SRC3

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRC3. 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.

Miscellaneous

- CSCsv49767

  Symptoms: When HA is tested for ATM and TDM PW, it takes at least 10 seconds for the PW to recover.

  Conditions: Occurs after RP switchover.

  Workaround: Wait for 10 seconds

Resolved Caveats—Cisco IOS Release 12.2(33)SRC3

Cisco IOS Release 12.2(33)SRC3 is a rebuild release for Cisco IOS Release 12.2(33)SRC. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRC3 but may be open in previous Cisco IOS releases.

Miscellaneous

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsl42732

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

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

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

- 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.

- 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".

- 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.

- 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.

- 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.

- 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.

- CSCsq30261

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

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

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

- 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.

- 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.

- 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.

- 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.

- CSCsr55865

  Symptoms: Packet marking does not work in Cisco 7200, 7200p, and 7301 ipbase images.

  Conditions: pplies 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.

- 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.

- 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.

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCeh06778

Symptoms: If a default route is redistributed from RIP into BGP, then back into RIP on another router, the default route is not marked as poisoned or withdrawn on the CE router that receives the updates.

Conditions: This symptom is observed when a CE router sends the default route via RIP to a PE router, when the PE router advertises this route to a second CE router, and when the link between the first CE router and the PE router is disconnected.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsi73982

  Symptoms: Traceback occurs at SW_VLAN-SP-4-VTP_INTERNAL_ERROR.

  Conditions: Occurred because the vlan.dat file has corrupted data.

  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.

- 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.”

- 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.

- CSCsk25915

  Symptoms: While bringing up PPPoEoA over ATM AAL5MUX sessions, calls per second is very low.

  Conditions: The problem is seen when there are a large number of PPPoEoA sessions being brought up (31000 sessions).

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsk70218

  Symptoms: RF resetting the standby CPU.

  Conditions: This condition is observed when 16000 PPPoA sessions were brought up and removed.

  Workaround: There is no workaround.

- CSCsk83038

  Symptoms: The following issues occur during in-service software upgrade (ISSU):

  1. High CPU. Packets sent at 1% of the line rate.

  2. Packets switched in software.

  3. VACL capture port takes a long times to start capturing packets.

  This issue not seen during the regular SSO switchover.

Conditions: Occurs when doing the ISSU operation.

Workaround: There is no workaround.

- CSCsk99465

  Symptoms: Cisco 7600 configured with MPB in a SSO HA configuration may display a message as follows:

  ```
  %ISSU-3-NOT_FIND_MSG_SES: Cannot find message session(0) to get msg mtu
  ```

  Conditions: This behavior exists for MPB in Cisco IOS Release 12.2(33)SRC. The problem is seen when the Standby Supervisor and the line card on which MPB is configured get reset. After this, if the line card comes back online before the ISSU negotiation between the Active Supervisor and the Standby Supervisor is completed, this error message will be seen.

  Workaround: 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.

- 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.

- 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.

- 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: The workaournd would be to use priority and with absolute-value (explicit) policer.

- 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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsm56940

  Symptoms: Traceback seen while doing Telnet with SSH enabled.

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

  Workaround: There is no workaround.

- CSCsm71537

  Symptoms: The router crashes when Independent Optimized Edge Routing (OER) is configured.

  Conditions: Occurs when OER is configured.

  Workaround: There is no workaround.

- CSCso09170

  Symptoms: The following error message appears intermittently on the line card console:

  ```
  *Mar 7 10:23:15.088: %FABRIC_INTF_ASIC-DFC11-5-FABRICSYNC_DONE: Fabric ASIC 1 Channel
  1: Fabric sync done. *Mar 7 15:23:15.356 IST: DFC11: policyq_entry 0x257AC25C already
  present<<<<<<<<<<<<<<<<<<<<<<<<<<<< *Mar 7 15:23:15.588 IST:
  %LINEPROTO-DFC11-5-UPDOWN: Line protocol on Interface IBC3/0, changed state to up
  ```

  Conditions: Occurs because of the following factors:

  1. The unqueue operation is not clean, so when a policy-map is being pushed down more than once in one port-c, the error occurs.

2. The policy-map is pushed down more than once, even though it is only programmed in one member link in a single port-c.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCso30649

  Symptoms: Private VLAN configuration is not updated properly by VLAN Trunk Protocol (VTP).

  Conditions: When the VTP mode of a router with private VLAN configuration is changed from OFF to SERVER and the router receives a VTP update from the primary VTP server, the private VLAN configuration on the router is not updated correctly. This behavior is also observed when changing the mode from VTP transparent to VTP server

  Workaround: When the VLAN configuration of the VTP primary server is changed and a new update arrives on the router, the correct configuration is installed.

- 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.

- CSCso46337

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

  Conditions: Occurs after SSO.

  Workaround: There is no workaround.

- CSCso59974

  Symptoms: BGP session goes idle.

  Conditions: Occurs following a stateful switchover (SSO).

  Workaround: There is no workaround.

- 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.

- CSCso87083

  Symptoms: Router crashes.

  Conditions: System crashes when the **test sw-vlan show nvfile** command is entered on the SP.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsq39180

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

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

Workaround: Reload the router.

- 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.

- 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.

- CSCsq52836

  Symptoms: VLAN database is lost

  Conditions: Occurs on a switch running VTP3 as a primary server. After configuring translational bridging (TLB), the VLAN database is lost. After all VLANs are deleted, the creation of new VLANs fails.

  Workaround: The only way to recover this is to delete the const_nvram:vlan.dat file and reload the switch. Doing so will result in booting the switch with the factory defaults and therefore require additional VLAN configuration.

- 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.

- 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.

- 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.

- CSCsq76166

  Symptoms: Cisco IOS Embedded Event Manager (EEM) has been erroneously omitted from ipbase images.

  Conditions: This issue occurs only in Cisco IOS Release 12.2(33)SR.

  Workaround: Use an image, other than ipbase, that supports EEM.

- 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.

- 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**.

- 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.

- 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.

- CSCsq97167

  Symptoms: IP multicast traffic drops every 100 seconds.

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

  Workaround: There is no workaround.

- CSCsq97517

  Symptoms: On a newly-rebooted router, CEF states on SP will not be in sync with RP.

  Conditions: It is a very rare race condition that triggers this problem. It is not seen on many platforms.

  Workaround: There is no workaround, other than reloading the router.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsr27794

  Symptoms: BGP does not generate updates for certain peers.

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

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

- 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.

- 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

- 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.

- 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.

- CSCsr44005

  Symptoms: After stateful switchover (SSO) there may be a loss of packet delivery for 10 or more seconds on connected routes.

  Conditions: Occurs when one or more connected routes reference virtual interfaces (such as loopbacks).

  Workaround: There is no workaround.

- 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

- 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.

- CSCsr50134

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

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

  * primary path FRR cutover

  * primary path’s interface flaps

* FRR configuration is changed

Workaround: Avoid FRR configuration changes.

- 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.

- 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.

- 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.

- 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.

- CSCsr62803

  Symptoms: Pings and sessions to processor fail when **service internal** is not configured.

  Conditions: Occurs while attempting to establish a session to the processor. It fails with the following message: % IP routing table __Platform_iVRF:_ID00_ not accessible

  Workaround: There is no workaround.

- CSCsr65230

Symptoms: When attempting to add serial links to a Multilink PPP (MLP) bundle, some member links remain down or flap, and tracebacks occur.

Conditions: Occurs with SIP400 and channelized SPA interfaces.

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 **no interface** command.

  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).

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 “allows-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.

- CSCsu23152

  Symptoms: On a Cisco 7600 with Virtual Private LAN Services (VPLS) configured and participating in the VPLS domain, if there is a stateful switchover (SSO), the router stops processing the BPDUs from the MPLS cloud and could cause a STP loop.

  Conditions: This is seen on a router running Cisco IOS Release 12.2(33)SRC1. When this condition is seen, the **remote comm sw show ibc** is showing drops due to IDB.

  Workaround: Reload the router and unconfigure the VFI

- 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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsu62667

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

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu63884

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

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

  Workaround: There is no workaround.

- 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

- 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.

- 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.

- 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.

- 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.

- CSCsu87721

  Symptoms: Available memory decreased after software is upgraded on router.

  Conditions: Occurred on a Cisco 7206VXR (NPE-G1) that was upgraded from Cisco IOS Release 12.2(31)SB11 to 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.

- 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.

- 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 two 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.

- 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.

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

  Workaround: There is no workaround.

- 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

- 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.

- CSCsv12428

  Symptoms: New service instance on port-channel is not working.

  Conditions: Occurs when a service instance with bridge-domain is configured on port-channel. When a bridge domain is configured under a port-channel EVC after member links are configured for that port-channel, the bridge domain configuration will not take effect until the port-channel interface is shut down and re-enabled by a **shut/no shut**.

  Workaround: Perform a **shut/no shut** of the port-channel interface.

- CSCsv13914

  Symptoms: Traceback observed when the PPPoEoA session is brought up.

  Condition: Occurs when the interface is not up.

  Workaround: There is no workaround.

- 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.

- CSCsv23428

  Symptoms: Line protocol going down with bridge-domain and OAM-PVC configuration.

Conditions: Issue is seen only with SIP-400 cards.

Workaround: There is no workaround.

- CSCsv24742

  Symptoms: A Cisco router may report exit link out of policy (OOP) when the 32- bit interface utilization counter wraps. At 100 Mbps traffic rate, this can happen once every 6 minutes.

  Conditions: The symptom is observed on a Cisco router running Performance Routing (PfR) and when the 32-bit interface utilization counter wraps.

  Workaround: There is no workaround.

- 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.

- CSCsv35571

  Symptoms: Port-channel dot1q traffic on service instance does not flow.

  Conditions: All of the following must be true:

  * Port-channel configured with member links on ES20 line card

  * Encapsulated dot1q is configured on a service instance on the port-channel

  * Port-channel has member links on both NPUs

  * For 20-port ES20, this means ports 0-9 have at least one member link, and ports 10-19 have at least one member link.

  * For 2-port ES20, this means both ports are members of the port-channel.

  * The service instance are removed from the configuration.

  After this, traffic may stop flowing on service instances under the port-channel, particularly if service instances are repeatedly configured and removed.

  Workaround: Before removing a service instance from the port-channel, remove all of the member links on one of the NPUs.

- CSCsv51032

  Symptoms: Line protocol going down with bridge-domain and OAM-PVC configuration.

  Conditions: Issue is seen only with SIP-400 cards.

  Workaround: There is no workaround.

- 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.

- 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.

  CSCsv30540

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

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

  Workaround: There is no workaround.

  CSCsu76800

  Symptoms: “Acct-Input-Giga-word” and “Acct-Output-Giga-wor” attributes are missing in the Accounting request packets.

  Conditions: The symptoms are observed when traffic is sent that requires the giga word counters to be incremented.

  Workaround: There is no workaround.

- CSCso56038

  Symptoms: The following error message may be seen:

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

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

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

  Workaround: There is no workaround.

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

- CSCso56196

  Symptoms: Updates are not being sent or withdrawn.

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

  Workaround: Remove the idle neighbors of the update-group and add again.

- CSCso88616

  Symptoms: Service-Logoff is executed on IP sessions then switchover is triggered. After New Standby is HOT, same Service-Logoff is executed again. New Standby RP crashes.

  Conditions: The issue is seen in the Cisco 7600 platform in Cisco IOS Release 12.2 (nightly.SRC080419) NIGHTLY BUILD.

  Workaround: There is no workaround.

- 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.

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

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

  Workaround: Do not use EIGRP to redistribute BGP.

- 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 traffic is sent that requires the giga word counters to be incremented.

  Workaround: There is no workaround.

- CSCef47023

  Symptoms: The metric of the advertised RIP routes may not change from the default metric.

  Conditions: Occurs when redistributing static or connected routes into the RIP routing process with an outbound offset-list applied to the routes.

  Workarounds: Use one of the following:

  - Under the RIP process, replace the redistribute connected configuration with the respective static and/or connected network statements.
  - Under the RIP process, modify the default metric in the redistribute connected metric and/or redistribute static metric command options.
  - Use an inbound offset-list on the neighboring routers.

- CSCek49649

  Symptoms: Cisco Catalyst 6500 and Cisco 7600 modules are reachable via 127.0.0.x addresses.

Conditions: Cisco Catalyst 6500 and Cisco 7600 series devices use addresses from the 127.0.0.0/8 (loopback) range in the Ethernet Out-of-Band Channel (EOBC) for internal communication.

Addresses from this range that are used in the EOBC on Cisco Catalyst 6500 and Cisco 7600 series devices are accessible from outside of the system. The Supervisor module, Multilayer Switch Feature Card (MSFC), or any other intelligent module may receive and process packets that are destined for the 127.0.0.0/8 network. An attacker can exploit this behavior to bypass existing access control lists; however, an exploit will not allow an attacker to bypass authentication or authorization. Valid authentication credentials are still required to access the module in question.

Per RFC 3330, a packet that is sent to an address anywhere within the 127.0.0.0/8 address range should loop back inside the host and should never reach the physical network. However, some host implementations send packets to addresses in the 127.0.0.0/8 range outside their Network Interface Card (NIC) and to the network. Certain implementations that normally do not send packets to addresses in the 127.0.0.0/8 range may also be configured to do so.

Destination addresses in the 127.0.0.0/8 range are not routed on the Internet. This factor limits the exposure of this issue.

This issue is applicable to systems that run Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) and Native Mode (IOS Software on both the Supervisor Engine and the MSFC).

Workaround: Administrators can apply an access control list that filters packets to the 127.0.0.0/8 address range to interfaces where attacks may be launched.

```
ip access-list extended block_loopback
deny ip any 127.0.0.0 0.255.255.255
permit ip any any

interface Vlan x
ip access-group block_loopback in
```

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent 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. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!
access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255
!
!-- 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-127/8-netblock-class match access-group 111
!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
```

```
policy-map drop-127/8-netblock-traffic
class drop-127/8-netblock-class
police 32000 1500 1500 conform-action drop exceed-action drop
!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!
control-plane service-policy input drop-127/8-netblock-traffic
!
```

Additional information on the configuration and use of the CoPP feature is available at the following links:

http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html

Infrastructure Access Control Lists (iACLs) are also considered a network security best practice and should be considered as, long-term additions to effective network security as well as a workaround for this specific issue. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs. The white paper is available at the following link:

http://www.cisco.com/warp/public/707/iacl.html

- CSCin79116

  Symptoms: Issuing **show** commands can push the CPU utilization to 100%.

  Conditions: It has been noticed that potentially long running show commands, like **show running-config**, **show voice call summary**, and **show memory summary** could affect voice call processing adversely, even if they periodically suspend.

  Workaround: There is no workaround.

- CSCsd37025

  Symptoms: A router may crash after an NBAR policy map is removed from a interface. The crash comes after CPU hog messages for the virtual exec process, for example:

  SYS-3-CPUHOG: Task is running for (34004)msecs, more than (2000)msecs (462/13),process = Virtual Exec.

  Conditions: There are two conditions that must be met to encounter the this bug:

  1. There must be a class map configured that includes **match protocol rtp video** and **match protocol rtp audio** that is then removed.

  2. The **ip nbar protocol-discovery** command must be configured on an interface and then removed.

  The order or configuring and removing the class map and protocol-discovery does not matter.

  Workaround: There is no workaround.

- CSCse07265

  Symptoms: When defining an IP SLA probe with a reaction event of TIMEOUT or CONNECTIONLOSS and setting the probe to generate a trap, a syslog message is not generated.

  Conditions: A sample configuration that shows a trap should be generated:

```
ip sla logging traps
ip sla 1
icmp-echo X.X.X.X
timeout 200
frequency 1
ip sla reaction-configuration 1 react timeout threshold-type immediate
```

```
action-type trapOnly
ip sla schedule 1 life forever start-time now
snmp-server enable traps syslog snmp-server enable traps rtr
snmp-server host Y.Y.Y.Y public syslog rtr
```
Workaround: There is no workaround.

- CSCse12518

  Symptoms: Multicast stream may fail to egress OIL line card interface on Supervisor 720. Issue observed when stream is egress both CFC and DFC based line cards. Stream will continue to show in the OIL of the mroute table. Issue observed on 6500 running 12.2(18)SXF7 with with 67xx based line cards.

  If traffic egresses a DFC line card, output of the below commands will show the outgoing interface is not programmed:

  ```
  dfc# show mls cef ip mult source group detail
  dfc# test mcast rd-met slot <DFC slot> addr <met3 address>
  ```
  Conditions: Occurs on a switch running Cisco IOS Release 12.2(18)SXF7, 67XX line cases when switch is in egress replication mode

  Workaround: Change to ingress replication mode.

- CSCse26750

  Symptoms: BOOTLDR is not displayed with Cisco IOS Release 12.4M-based boot-images.

  Conditions: Occurred on a Cisco 7500 router running Cisco IOS Release 12.4M.

  Workaround: There is no workaround.

- CSCse40379

  Symptoms: Increasing the request-data-size via CLI in IP SLA operation crashes the device.

  Conditions: This occurs when we try at least two start/stop and one configuration change for that operation and when we increase the size from the default size for the “request-data-size” to some higher value via CLI.

  Workaround: There is no workaround.

- CSCse84264

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and traceback is seen when **show running-config** and **write memory** commands are issued. The router may also reload.

  Workaround: There is no workaround.

- CSCsg32308

  Symptoms: It is not possible to restore the NTP part of a backup from the start up configuration.

  Conditions: Occurs when you copy and paste of the following NTP statement:

  ntp-authentication-key xxxx md5 7.

  Workaround: There is no workaround.

- CSCsg68717

  Symptoms: You may see the following issues with your BGP maximum path configuration when executing a **show run** command on the router:

  1. The IBGP takes the value of ebgp and the ebgp doesn’t show the import value.

  2. In case EBGP import is “ibgp import” the greater of the two is used for IBGP import.

  3. The unequal cost configuration is ignored as well

  Conditions: Occurs during normal operation.

Workaround: There is no workaround.

- CSCsg96436

  Symptoms: EzVPN router might loose its IPSec connection due to three consecutive missed keepalives.

  Conditions: Occurs when ISAKAMP keepalives are configured with EzVPN.

  Workaround: Disable keepalives.

- CSCsh45091

  Symptoms: A router running may crash when an SNMP poll for IPSLA/SAA values is performed.

  Conditions: Unknown at this time.

  Workaround: Either do not poll IPSLA/SAA values or use an SNMP cut down view to exclude the MIBs

- CSCsh75156

  Symptoms: The **show interface serial** command incorrectly displays time slot information.

  Conditions: Occurs on an unframed E1.

  Workaround: There is no workaround.

- CSCsi70484

  Symptoms: OSPF is seen running SPF continuously.

  Syslog shows following: %OSPF-4-CONFLICTING_LSAID: Found LSA with the same host bit set but using different mask Existing: LSA ID 10.1.1.1/29 New: Destination 10.1.1.1/32

  Conditions: Seems to be triggered when we have a LSID conflict and then using a prefix list to filter the shorter prefix.

  Workaround: Eliminate the LSID conflict or remove the filtering for the conflicting prefixes.

- CSCsj13911

  Symptoms: Device does not receive reply for query between some VLANs.

  Conditions: Occurs under the following scenario:

  - First device begins to send QUERY and starts SIA Timer, due to the neighbor being down.
  - Next device does not receive REPLY for only subset of network of away segment.
  - After SIA Timer expired, device send a SIA QUERY. After that the device correctly receives the REPLY for the SIA QUERY.

  Workaround: There is no workaround.

- CSCsj50892

  Symptoms: After configuring **no local ip pool** command to remove a specific **IP address of range** under multiple **IP address of range** with one “local address pool”, whole “IP address of range” is removed. And an option to specify “IP address of range” is not valid.

  Condition: Occurs when configuring **no local ip pool** command.

  Workaround: There is no workaround.

- CSCsl32324

  Symptoms: The following message and traceback may be generated on a Cisco platform that is configured for TCL:

```
Sep 12 09:15:32.140: %SCHED-3-THRASHING: Process thrashing on watched message event.
-Process= "Tcl Serv - tty0", ipl= 4, pid= 108, -Traceback= 0x41640580 0x42946B40
0x42946E3C 0x42873898 0x42935D20 0x42935D04
```

Conditions: The problem occurs with the following configuration:

```
Router 1: Router>enable Router#tclsh Router(tcl)#config t couldn't read file
"ftp://cisco:147852@10.10.10.2/TFTP-Root/pokus1.tcl": Timed out
Sep 12 09:15:32.140: %SCHED-3-THRASHING: Process thrashing on watched message event.
-Process= "Tcl Serv - tty0", ipl= 4, pid= 108, -Traceback= 0x41640580 0x42946B40
0x42946E3C 0x42873898 0x42935D20 0x42935D04
Router 2: CCIE-R3#conf t Enter configuration commands, one per line. End with CNTL/Z.
CCIE-R3(config)#scripting tcl init tftp://192.168.1.2/init CCIE-R3(config)#exit
CCIE-R3#tclsh CCIE-R3(tcl)# CCIE-R3(tcl)#exit couldn't read file
"tftp://192.168.1.2/init": Timed out
```

The following error is displayed:

```
*Nov 13 17:46:41.427: %SCHED-3-THRASHING: Process thrashing on watched message event.
-Process= "Tcl Serv - tty0", ipl= 4, pid= 27 -Traceback= 0x60F3FF2C 0x61FCB3A4
0x61FCB6A0 0x61EF3190 0x61FBAC90 0x61FBAC74
```

If there is no "scripting tcl init tftp://192.168.1.2/init" command entered or the file can be found, the TCL shell exits correctly to the system prompt and the TCL process disappears correctly.

Workaround: There is no workaround.

- CSCsl43580

  Symptoms: The **standby delay minimum**<*seconds*>**reload** <*seconds*> command produces an incorrect value when the **show standby delay** command is entered.

  Conditions: Occurs when the delay value is greater than 255.

  Workaround: There is no workaround.

- CSCsl48997

  Symptoms: A router running Cisco IOS may enter a boot loop after a crash.

  Conditions: This only applies to PowerPC platforms, such as the NPE-G2. The problem is not seen on every crash. If the router is configured to write a core dump then it is very likely to be seen.

  Workaround: There is no workaround.

- CSCsl98238

  Symptoms: When QoS **statistics-export** is configured to send updates to a syslog server that is not on a directly connected subnet, traffic does not reach the destination server.

  Conditions: It happens when syslog server is not a directly connected subnet from the switch's perspective.

  Workaround: Put the syslog server on a directly-connected network, or create a new VLAN interface with IP address for that VLAN on the switch to allow it to be in the same network if possible.

- CSCsm71828

  Symptoms: A policy-map setting MPLS EXP bits applied on ingress of a non-EoMPLS SVI does not function correctly after the device is reloaded. **service-policy input** is present under interface configuration, but **show policy-map interface** does not show the set mpls action.

  Conditions: Occurs when a policy-map contains the **set mpls experimental** action.

  Workaround: There is no preventative workaround. When the device is reloaded, remove and reapply the affected **service-policy input** configurations. This can be automated with an IOS EEM policy.

- CSCsm84915

Symptoms: While L2TP network server (LNS) sends access-request packet to the AAA-server, NAS-port-type attribute is missing in access request.

Conditions: Occurs under normal operation.

Workaround: Configure **vpdn aaa attribute nas-port vpdn-nas** on LNS.

- CSCsm91520

  Symptoms: Cisco 7600 POS interface fast reroute (FRR) may take up to 1 second.

  Conditions: This issue happens when we remove the far-end RX fiber of the POS link.

  Workaround: There is no workaround.

- CSCso07371

  Symptoms: A Cisco 7200 with NPE-G1 may display the following error message:

  ```
  %SCHED-7-WATCH: Attempt to set uninitialized watched boolean (address 0). -Process=
  "Init", ipl= 0, pid= 3 -Traceback= 60A0EA90 610ACF70 60D59424 608B42F0 608CCB18
  608CD028 60A46BE8 60A4123C 60A3A0EC 60A43878 60A43B80 60913930 609190D0 609D6BF4
  609D6BE0
  ```

  Conditions: Unknown conditions, however, impact is minimal.

  Workaround: There is no workaround.

- CSCso35659

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

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

  Workaround: Unconfigure and clear the VLAN.

- CSCso36570

  Symptoms: An ES20 with a port configured as a Layer 2 interface allows MTU configuration on the interface as if it were a Layer 3 interface. When put into a port-channel, once the interface comes up, the MTU will propagate up to the port-channel configuration, which is an invalid configuration. This will cause SSO redundancy to be lost.

  Conditions: An ES20 interface must be configured as an L2 port using the **switchport** command. The interface must be a member of an L2 port-channel. SSO must be configured.

  Workaround: Remove the MTU configuration from the interfaces. This can be done using the **default mtu** interface-level configuration command.

- CSCso55151

  Symptoms: A router with CEF switching turned on may experience a memory leak related to ARP packets.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCso65821

  Symptoms: Custom QoS map configuration on a port will propagate to all eight ports on a line card.

  Conditions: Occurs on a Catalyst 6500 with a 6408 module and custom QoS maps configured for interfaces on the 6408 module.

  Workaround: There is no workaround.

- CSCso75238

Symptoms: When using PPP over ATM (PPPoATM), output packets may occasionally be dropped at the ATM physical interface, accompanied by error message complaining about a bad ATM virtual-circuit of ‘49185’. For example:

```
%ATMPA-3-BADVCD: ATM3/0 bad vcd 49185 packet -
```

This error message will include an additional line of output, containing a hexadecimal string, which will always begin with ‘C0210A’, such as:

```
C0210A09 000C1506 92251506 92250000 00000000 00000000
```

Conditions: This occurs only on PPPoATM sessions which are locally terminated, and if the remote PPP endpoint is sending PPP LCP Echo-Request packets.

Workaround: There is no workaround.

- CSCso80951

  Symptoms: External BGP neighbors configured in the IPv4 VRF address-family context may fall into different update groups, even if the outbound policy is identical. Two neighbors having same SOO configuration are wrongly put into different update-group.

  Conditions: Occurs when route-map configuration has SOO.

  Workaround: There is no workaround.

- CSCso89692

  Symptoms: Router is crashing.

  Conditions: This was observed and reproduced on a Cisco 877 running Cisco IOS Release 12.4(15)T4 when executing a TCL script based on Embedded Event Manager (EEM). Other platforms and IOS releases are affected.

  Workaround: There is no workaround.

- CSCsq16469

  Symptoms: After reload some interfaces will handle uRPF in software and customer can observe packet drops on those interfaces due to MLS hardware limiter for RPF traffic.

  Conditions: This problem occurs after reload and only for interfaces where uRPF is configured.

  Workaround: Perform a **shut/no shut** to restore correct uRPF operation.

- CSCsq16838

  Symptoms: The section filter does not work as expected. The same command with the same configuration gives a different output compared to that of Cisco IOS Release 12.4.

  Conditions: Occurs in Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsq36206

  Symptoms: MDT tunnels not getting created on Cisco 7206 and Cisco 7304 routers.

  Condition: The **neighbor XXXX Activate** command is not getting automatically configured in “address-family ipv4 mdt”.

  Workaround: Manually configure the “neighbor XXXX Activate” under “address-family ipv4 mdt” to solve the issue.

- CSCsq38431

  Symptoms: OSPF “summary address” is always executed, even if the subnet is becoming small. It should be checking not only prefix but also subnets. For example, 10.0.0.0/9 is summarized to 10.0.0.0/16.

Conditions: Summarized subnet is becoming smaller than original subnet.

Workaround: There is no workaround.

- CSCsq42799

  Symptoms: Downstream line rates of 98% or more are only being observed when using the new PA in “hardware enabled mode”, meaning the MLPPP member links are on the same PA. However, when the customer uses the “software mode”, meaning when the two member links (2 T1s) are across two different PSs, then the downstream line rate drops down to 2 Megs the most.

  Conditions: Customer is trying to do “software mode” for MLPPP, using two different PA-MC-2T3-EC cards, to support his customers and is not getting anywhere close to the full line rate. However, the same software mode was giving him close to the full line rate for download speeds when using the older PA: PA-MC-2T3+ cards.

  Workaround: There is no workaround.

- CSCsq47140

  Symptoms: When the fabric line card is power cycled due to fabric channel error, sometimes the line card fails to boot and displays “scp download failure”

  Conditions: Occurs on the fabric line card.

  Workaround: Manually power down line card, wait for more than one minute, then power on the line card.

- CSCsq49200

  Symptoms: OSPF NSSA external routes will not be installed if the forwarding address is set to the address of the remote end of a PPP link, and **peer neighbor-route** is configured.

  Conditions: This occurs only when the forwarding address is the remote end of a PPP link, and the entry appears as directly connected in the routing table. It does not occur for forwarding addresses that reside on directly connected multi-access networks.

  Workaround: The forwarding address must appear in the routing table as an OSPF intra- or inter-area route (Type O or IA). This can be achieved in two ways:

  – Remove the **peer neighbor-route** and advertise the remote endpoint of the PPP link via OSPF.

  – Advertise a loopback interface into the OSPF NSSA area with an IP address that is higher than the endpoint of the PPP link. This will cause that IP address to be used as the forwarding address.

  Alternatively, configure command **local-rib-criteria forwarding-address** in OSPF router context.

- CSCsq49201

  Symptoms: BGP neighbor with associated peer-session template does not use MD5 TCP connection while the template is configured with the “password” command

  Conditions: Occurs when password is configured on a non-directly inherited peer session and it gets overwritten by configuration.

  Workaround: Change the password on the peer-session to a new one, and then put the old one back.

- CSCsq58164

  Symptoms: If PPPoE session to CPE is cleared, router outputs traceback and does not delete the connected route for assigning address prefix from VRF RIB.

  Conditions: Occurs when using a framed-IPv6 prefix from RADIUS using AAA without having the VRF forwarding attached to the virtual-template. This problem is observed when router assigns IPv6 prefix by RAIDUS over PPPoE to CPE.

Workaround: There is no workaround.

- CSCsq58176

  Symptoms: When IPSec session is connected, Calling-Station-Id attribute in RADIUS Access-Request is not sent to RADIUS server. (12.2(33)SRB sends this attribute.)

  Conditions: Occurs when router is running Cisco IOS Release 12.2(33)SRC and configured for RADIUS authentication for XAUTH.

  Workaround: There is no workaround.

- CSCsq77695

  Symptoms: A router running EIGRP with three or more unequal load balancing routes might not purge some higher metric routes under certain conditions, which leads to a suboptimal routing.

  Conditions: The issue is seen when a router receives three unequal cost routes to the same destination address, having variance set to a value higher than one. Depending on the order the routes come up, higher metric routes might not be purged from the routing table.

  As an example with variance set to 2:

```
D*EX 0.0.0.0/0 [170/7734528] via 192.168.230.3, 00:00:01, Tunnel1190
               [170/26852352] via 192.168.24.4, 00:00:01, Tunnel1290
               [170/15469056] via 192.168.23.3, 00:00:01, Tunnel190
Route via tunnel1290 has 26M metric.
Lowest metric is 7.7M.
Configured variance is 2, and thus we should not see route via tunnel1290.
```

  Workaround: Manually clear the IP routing table.

- CSCsq80044

  Symptoms: Counter on a frame relay interface shows strange behavior. The first will be the enormous packet/sec value after entering **show frame-relay pvc** *nbr*. This is due to the wrap counter of 32 bits.

  The second issue is that even using **frame-relay ifmib-counter64 subif** the issue is still seen in the counters while performing **show frame-relay pvc** *nbr* 64-bit

  Conditions: Occurs while switching traffic.

  Workaround: There is no workaround.

- CSCsq80238

  Symptoms: When VPN tunnel is disconnected manually by **clear crypto session**, cikeTunHistTermReason value is set as “1 (other)”.

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

  Workaround: There is no workaround.

- CSCsq88370

  Symptoms: Relay configuration reappears after recreating the software interface and removing it.

  Conditions: Unknown conditions.

  Workaround: Explicitly remove the DHCP relay command before removing the interface.

- CSCsq90682

  Symptoms: DSCP marking is not preserved when traffic is ingressing a tunnel and egressing a backed-up interface.

  Conditions: Occurs when using a Cisco 7600 as a midpoint for MPLS TE that is configured for FRR.

  Workaround: Configure the **mls qos map exp-dscp** command globally.

- CSCsq94234

  Symptoms: Bytes output counters in the output of **show policy-map interface** command include the internal Ethernet header in calculation. On non-Ethernet types of interfaces, "bytes output" counters in the output of **show policy-map interf** command include the internal Ethernet header in calculations.

  Conditions: Symptom observed on 7600-SIP-600 card of a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRB, on all types of interfaces which do not use Ethernet encapsulation.

  Workaround: There is no workaround.

- CSCsq96144

  Symptoms: Netflow v9 has several issues on exported data.

  - In IPv4, when the IGP path to the BGP nexthop address is ECMP, BGP nexthop field on exported data becomes 0.0.0.0.
  - In IPv6, src/dst ASN and src/dst mask field on exported data becomes 0.
  - In netflow v9 for IPv6, nexthop-field(type=62) value changes dependent on how nexhop route is resolved.
  - If destination is via iBGP Peer address and the IGP path to the BGP nexhop address is resolved by OSPF and ECMP, nexhop-field(type=62) value becomes ::.
  - If destination is via iBGP Peer address and the IGP path to the BGP nexhop address is resolved by OSPF and not ECMP, nexhop-field(type=62) value becomes link-local address of nexthop.

  Conditions: This symptom is observed on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsq96324

  Symptoms: When SNMP trap is enabled, a Cisco 7600 generates a trap for Lawful Intercept after reload.

  Condition: This issue does not depend on SNMP version.

  Workaround: There is no workaround.

- CSCsq97870

  Symptoms: A router crash is observed.

  Conditions: Occurs when HSRP configuration is being modified in two different telnet sessions while the **show standby** command is entered.

  Workaround: Do not issue the **show standby** command when two active configuration sessions are open and one of them is making changes in HSRP configuration.

- CSCsr08327

  Symptoms: When MPLS CsC with BGP send-label is configured, end-to-end ping fails.

  Conditions: Sequence of configuring MPLS CsC with BGP send-label.

  Workaround: There is no workaround.

- CSCsr08468

  Symptoms: When the Cisco 7600 is getting over 100000 or more routes as External 1, some routes in OSPF database cannot be installed into routing table.

  Conditions: Occurred on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsr09554

  Symptoms: Following error message appears in the logs of a Catalyst 6500 and Cisco 7600:

  ```
  %SIBYTE-CFC1-6-SB_RMON_OVRFL: RMON register 20 overflow on mac 1
  ```
  Conditions: Occurs when service internal is configured.

  Workaround: Remove service internal from the configuration.

- CSCsr11662

  Symptoms: When an EIGRP route goes to SIA (Stuck in Active), the router does not send a query out and the active timer is set to “never”. The route stays in the active table and never gets purged.

  Conditions: Possible route flaps

  Workaround: Clear neighborship for adjacent routers with the **clear ip eigrp neighbor** <*neighbor IP*> command.

- CSCsr12987

  Symptoms: When running multicast and there exists a unicast EBGP route which covers some more specific IGP routes, the IGP routes will no longer be used for RPF tree building, which may result in loss of reachability to a multicast source. The loss of the more specific IGP routes will be reflected in the output of:

  show ip route multicast

  This may also occur when the covering route is a unicast static route.

  Conditions: This affects releases based on 12.2(33)SR. There must be overlap between a unicast BGP/Static route and some unicast IGP routes. Multicast must be running in the default mode i.e. not making use of incongruent (from unicast) multitopology support.

  Workaround: If there are no multicast specific routes, the following configuration will prevent the problem and provide better performance:

  ```
  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
  ```
  Alternatively, the following configuration may be used:

  ip multicast longest-match

  The performance of the second alternative will not be as good as the first alternative.

- CSCsr15969

  Symptoms: An MPLS traffic engineering tail end router does not proceed with RSVP signalling if the extended tunnel ID is 0.0.0.0 in the RSVP Path message.

  Conditions: MPLS traffic engineering is used. There is a third party vendor using extended tunnel ID 0.0.0.0.

  Workaround: Do not use extended tunnel ID 0.0.0.0.

- CSCsr18177

  Symptoms: An error message with traceback is generated:

  ```
  %PARSE_RC-4-PRC_NON_COMPLIANCE: ‘do show ver’ -Traceback= 405B938C 405B98D0 40547398
  40548354 405497C8 42044050 405728C0 4124D074 4124D060
  ```
  with TACACS denied “do” commands.

Conditions: With a TACACS server using authorization, and a user having the “do” command denied, in Cisco IOS 12.2(33)SRB2, when the “do” command is issued (in the global configuration mode), not only this command is denied, but it also generates a traceback. Other denied commands in the global configuration mode do not generate the traceback.

Example Cisco IOS authorization config: aaa authorization config-commands aaa authorization commands 15 default group TEST

Workaround: Not to use the “do” command.

- CSCsr19413

  Symptoms: OSPF may delete a type 3 summary route, if the router receives update of a type5 external LSA for the same prefix. It shows in two different ways:

  – If the type5 external LSA update is withdraw, the route is deleted.

  – If the type5 external LSA update is update, the route is calculated as external.

  Either way, the summary route is not calculated by OSPF, though it is supposed to be.

  Conditions: The problem is observed on later 12.4T release. For this problem to happen, there must be:

  – Type 3 summary LSA, which is supposed to be the best path to be calculated by OSPF.

    Example: 10.1.0.0/16 summary LSA

  – Type 5 external LSA, which is the exact same prefix.

    Example: 10.1.0.0/16 external LSA

  – Type 5 external LSA, which is a specific for the above.

    Example: 10.1.0.0/24 external LSA, which is a specific for 10.1.0.0/16

  Workaround: Clear ip route *

- CSCsr22860

  Symptoms: On a 7600, with the following configuration:

  ```
  interface GigabitEthernet7/0/5.100200
  bandwidth 2300
  encapsulation dot1Q 100 second-dot1q 200
  ip vrf forwarding TEST ip address 10.0.0.1 255.255.255.252
  ```

  Packets that are routed in software by CEF might be sent to the wrong VLAN (100), instead of being routed out of this interface.

  Conditions: This issue would could come up any QinQ configuration, where the packet is punted from the fastsend path.

  Workaround: Add an ACL to avoid packet punting from fastsend and sending from process switching.

- CSCsr30406

  Symptoms: The **no capability opaque** and **no capability lls** commands are not accepted. Following a reboot, the command disappear from the configuration, and an error message is displayed.

  Conditions: Occurs when NSF and NSF helper are enabled.

  Workaround: There is no workaround.

- CSCsr36998

  Symptoms: On a switch configured with AAA for login authentication and authorization, using a RADIUS server, if the users on RADIUS are defined only with AVPair for privilege level, the authorization is failing

Conditions: Failing authorization with users on Radius server defined as: test Password == “ww” Cisco-AVPair += “shell:priv-lvl=14”

If we define also the Service Type, like Service-Type += Administrative, it is working fine.

Workaround: Configure the Service Type for Radius users.

- CSCsr39272

  Symptoms: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error printed when SPA sensor temp overruns buffer

  Conditions: Cisco 7600 with Sip200 SPA.

  Workaround: There is no workaround.

- CSCsr43164

  Symptoms: Fast reroute (FRR) may not become ready after reoptimize backup tunnel.

  Conditions: The symptom may be seen under the following conditions: - Initially backup LSP laps over primary LSP - Then backup LSP is reoptimized by other path-option

  Workaround: Perform a **shut/no shut** on the backup tunnel.

- CSCsr49420

  Symptoms: Cisco router running IOS software from 12.2 to 12.4T is used as PPTP server and terminates PPTP sessions on HSRP virtual IP address. If the PPTP packets generated by Windows PPTP client are getting fragmented somewhere between the PPTP client and PPTP server (PPTP packet should be fragmented after PPTP encapsulation to trigger the issue) then PPTP server drops such packets with this message:

  ```
  *Jul 22 00:06:55: %IP-3-LOOPPAK: Looping packet detected and dropped - src=172.16.0.4,
  dst=10.0.0.30, hl=20, tl=1400, prot=1, sport=0, dport=0 in=FastEthernet1/0,
  nexthop=10.0.0.30, out=FastEthernet1/0 options=none -Process= "IP Input", ipl= 0, pid=
  69 -Traceback= 60BEE940 60BEEBEC 60BF0724 60BF1304 60BEF110 60BDFE68 60BE02B4 60BDF224
  60BDF464 60BDF774
  ```

  Here, 172.16.0.4 is a PPTP client, 10.0.0.30 is a host behind PPTP server.

  Conditions:

  - Issue happens only if PPTP session is terminated on HSRP virtual IP address. Issue does not happen if PPTP is terminated on interface IP.
  - Issue happens only when PPTP packet is fragmented after the PPTP encapsulation. It does not matter if user’s traffic was fragmented before PPTP encapsulation or not.
  - Issue happens only to specific packet sizes. For example issue may looks this way for pings sent by PPTP client over the tunnel: “ping 10.0.0.30 -l 1300” works, “ping 10.0.0.30 -l 1372” fails, “ping 10.0.0.30 -l 1400” works again. Particular affected packet sizes in customer’s network might be different.
  - All affected packets (having specific sizes and fragmented) are dropped on PPTP server, but the error message above is generated only for 1 of every 10-15 dropped packets.

  Workaround: Avoid fragmentation after PPTP encapsulation. Fragmentation is typically caused by MTU smaller than 1500 on some link between PPTP client and the PPTP server.

- CSCsr50099

  Symptoms: Update of a strict hop to a loose hop and changing it back to a strict does not change the IP explicit path to strict. It erroneously remains loose.

  Conditions: If a strict IP explicit path is configured and any one of the hops is then made loose and then changed back to strict. The path still remains loose.

Workaround: Removing all the hops of the IP explicit path and then adding the hops again reconfigures it as strict.

- CSCsr51799

  Symptoms: When a BERT test is stopped in the middle, the corresponding serial interface stays in up/down status. This issue was seen with the pa-mc-8te1 hardware.

  Conditions: Occurs after stopping a BERT test before it is completed.

  Workaround: Create another BERT test that lasts one minute and let it run to completion. Reset the interface or the line card.

- CSCsr53085

  Symptoms: On a Cisco 7200 router with NPE-400 and configured with Open Shortest Path First (OSPF) routing protocol, OSPF might not come up on protection line following an Automatic Protection Switching (APS) switchover.

  Conditions: This only occurs when Automatic Protection Switching (APS) feature is configured.

  Workaround: Use NPE-G1 in place of NPE-400

- CSCsr53390

  Symptoms: The onboard Gigabit Ethernet ports on the NPE-G2 with flow control enabled will not send pause frames if they experience a resource problem. The ports will however receive pause frames and act upon them.

  Conditions: When flow control is enabled on the NPE-G2 Gig Ethernet Ports they will not send pause frames, but will receive them.

  Workaround: There is no workaround.

- CSCsr60108

  Symptoms: Standby delay reload timer range has changed. It should be 0-10000, but it is showing 0-300.

  Conditions: When configuring standby delay timer.

  Workaround: There is no workaround.

- CSCsr65760

  Symptoms: If a copper Small Form-Factor Pluggable (SFP) is inserted in a ES20-20ge port, and in interface configuration mode the command speed is checked with '?' for options, the displayed options are 10, 100, and 1000, as expected. Changing the SFP with an optical fiber one, the **speed ?** command gives 1000, instead of offering the "nonegotiate" option.

  Conditions: Occurs on a Cisco 7600 with RSP720 and running Cisco IOS Release 12.2(33)SRB2 or Cisco IOS Release 12.2(33)SRB3.

  Workaround: The only way to restore the initial behavior, the second one described above, is to reload the whole router, as only reloading the es20 linecard is not restoring the settings.

- CSCsr66588

  Symptoms: Netflow SLB aging parameter values are not synced to SP after reload.

```
sdpcgw2#sh mls netflow aging
               enable timeout packet threshold
               ------ ------- ----------------
normal aging   true    300     N/A
fast aging     false   32      100
long aging     true    1920    N/A
slb aging      true    4000 millisec N/A
sdpcgw2#remote command switch test mls netflow debug task 0 st
```

```
< skipped>
SLB aging [enabled]: age [2000]ms period [500]ms pattern [7]
<skipped>
```

Conditions: When SLB is configured and SLB aging to be different value than default.

Workaround: There is no workaround.

- CSCsr67377

  Symptoms: Link flaps may be observed on a TenGigabitEthernet interface with XENPAK-10GB-LW when Tx cable was only unplugged.

```
*Jun 27 19:32:53 JST: %LINEPROTO-5-UPDOWN:
Line protocol on Interface TenGigabitEthernet4/1, changed state to down
*Jun 27 19:32:53 JST: %LINK-3-UPDOWN:
Interface TenGigabitEthernet4/1, changed state to down
(snip)
Line protocol on Interface TenGigabitEthernet4/1, changed state to down
*Jun 27 19:33:03 JST: %LINK-SP-3-UPDOWN: Interface TenGigabitEthernet4/1, changed
state to down
*Jun 27 19:33:04 JST: %PM-SP-4-ERR_DISABLE:
link-flap error detected on Te4/1, putting Te4/1 in err-disable state
```

  Conditions: This was observed under a test scenario of normal traffic rate through the xenpaks.

  Workaround: Configure **carrier-delay up** of one second or more.

- CSCsr67562

  Symptoms: If an intermediate router is configured with OL bit under ISIS, the receiving router withdraws the prefixes learned through this next hop, however the receiving router fails to install the same prefixes with alternate paths.

  Conditions: This problem is noticed when both the receiving and advertising routers are configured with OL bit and ISPF is enabled.

  Workaround: Disable ISPF or do not configure OL bit on the receiving router.

- CSCsr68545

  Symptoms: Error message occurs:

```
000302: Jul 24 13:00:13.575 CDT: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
-Traceback= 0x410FD1A4 0x41119DB0 0x41138324 0x41DE5714
```

  Conditions: IP SLA configured with RTT.

  Workaround: There is no workaround.

- CSCsr83639

  Symptoms: TLB exception (bus error crash) following removal of BGP configuration.

  Conditions: This has been observed on a Cisco device running Cisco IOS Release 12.2(33)SXH2a.

  Workaround: There is no workaround.

- CSCsr86719

  Symptoms: With SLB configured on Cisco 7600, in a scaled scenario with high amounts of traffic, there is, over a period of time, severe memory depletion on the SP and IPC watermark messages are seen. If this state continues, eventually malloc fails occur and EOBC no buffer messages are seen on SP and finally LC's get reset, thereby causing service disruption.

  Conditions: Only seen on Cisco 7600 with SLB configuration in a scaled scenario with high amounts of traffic.

  Workaround: There is no workaround.

- CSCsr94174

Symptoms: References to a Container0 interface may show up in the running configuration of a router running Cisco IOS. This can cause configuration sync failures on redundant systems, which prevents SSO from initializing.

Conditions: This is usually a side affect of configurations that may automatically generate interface specific commands, such as **passive-interface default** in some versions of code.

Workaround: There is no workaround.

Further Problem Description: Container0 is an internal interface that should never been seen in the running configuration.

- CSCsr94954

  Symptoms: Memory leak is seen in OER and IP SLA responder processes.

  Conditions: Occurs after enabling OER.

  Workaround: There is no workaround.

- CSCsu01272

  Symptoms: The **clear ip bgp * soft** command on a PE advertises routes from CE with wrong route target to other PEs. The other PEs do not accept these routes and lose connectivity

  Conditions: Occurs in the following scenario: **soft-reconfiguration inbound** to CE must be configured on the PE **send community both** to PE must be configured on CE

  Workaround: Remove **send community both** from CE, then enter **clear ip bgp * soft** on the CE.

- CSCsu18426

  Symptoms: BGP(IPv6): Walking the default RIB output debug message printed even after disabling all the debugs

  Conditions: Unknown.

  Workaround: There is no workaround.

- CSCsu21716

  Symptoms: When (*, G) entry is created by IGMP membership report received on downstream interface, unsolicited IGMP report is not sent for mroute-proxy.

  Conditions: IGMP membership report is received on interface with mroute-proxy configuration.

  Workaround: There is no workaround.

- CSCsu24657

  Symptoms: High CPU under interrupt is seen on the RP of the Active RSP720. This issue is applicable only to RSP720 supervisor and SRB/SRC releases only CPU utilization for five seconds: 99%/99%; one minute: 99%; five minutes: 99%.

  Conditions: This has been seen on a Cisco 7600 running Cisco IOS Release 12.2(33)SRC.

  Workaround: A reload will temporarily remove the issue. This can also be fixed by modifying memory location without any traffic disruption.

- CSCsu25699

  Symptoms: OER ICMP probes are reporting incorrect WAN link round trip delay because they are exiting the wrong external interfaces.

  Conditions: GETVPN with OER (with active icmp probes).

  Workaround: Exclude ICMP probes from GETVPN crypto ACL.

- CSCsu35742

Symptoms: Getting the error message - “set command is not supported on output direction for this interface Configuration failed!” when applying a service policy to the interface. Same error is observed when **set cos** is added to the policy-map while the service policy is attached to the interface.

Conditions: The error was observed on a 10gig subinterface with Cisco IOS Release 12.2(33)SRC1 (ES-20 hardware).

Workaround: There is no workaround.

- CSCsu39458

  Symptoms: Customer test indicates that for packets size @1500Byte, LLQ conditional policer always kicks in and as a result PQ traffic cannot exceed the configured rate. Ex. on POS OC3 interface applying an output policy-map PRIO Policy Map PRIO Class voip priority 50 (%) Sending only 100mbps of 1486byte voip packet on the POS OC3 interface, causes the conditional policer to incorrectly police the traffic to around 78mbps (50% police rate).

  Conditions: When conditional policer is enabled, will not be able to exceed the priority rate configured for big packet sizes, even if the interface is not congested. Example,for packet size greater than 1133bytes for POS OC3 or 1293 bytes for T1 interface, sending 100mbps or 1mbps , 1486byte LLQ traffic respectively on POS OC3 or T1 interface, causes the conditional policer to police the traffic to configured rate applicable only to LLQ traffic with big packet size. Seen in all releases which support for conditional policer, up to and including SRD.

  Workaround: Use packet size less than 1000 bytes for LLQ traffic. Alternately, configure explicit policer for LLQ traffic instead of conditional policer, if packet size of LLQ traffic is likely to be big.

- CSCsu45252

  Symptoms: The following MIB returns only values for IPv4 peers:

  .iso.org.dod.internet.mgmt.mib-2.bgp.bgpPeerTable.bgpPeerEntry.bgpPeersState

  Conditions: Occurs on routers running Cisco IOS Release 12.2(33)SRB2, Cisco IOS Release 12.2(33)SRB3, or Cisco IOS Release 12.2(33)SRB4.

  Workaround: There is no workaround.

- CSCsu49002

  Symptoms: ciscoIpMRouteBps sometimes indicates wrong value.

  Conditions: SUP720-3BXL, ME-C6524, SUP32, SUP2 running Cisco IOS Release 12.2(18)SXF7 or Cisco IOS Release 12.2(18)SXF13.

  Workaround: There is no workaround.

- CSCsu52016

  Symptoms: In some cases Cisco 7600 running standard MST STP might not set “agreement” flag in BPDUs coming out of designated port. This has been reported to cause connectivity slowdown with certain third-party switches.

  Conditions: This issue is specific to the following Cisco IOS releases:

  - 12.2SRA
  - 12.2SRB
  - 12.2SRC
  - 12.2SXH

  Workaround: There is no workaround.

- CSCsu53624

Symptoms: Output from **bgp multicast** is always as same as BGP unicast information in **show ipv6 protocol** command, even though the multicast address family setup is different from the unicast address family configuration.

Conditions: Occurs when the **show ipv6 protocol** command is used.

Workaround: There is no workaround.

- CSCsu55661

  Symptoms: Configuration for **spanning-tree bpdufilter enable** does not work on physical interface that is part of Virtual Private LAN Services (VPLS).

  Conditions: Issue observed on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3 when STP is disabled for Virtual Private LAN Services (VPLS) VLAN.

  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.

- CSCsu77597

  Symptoms: Frames destined to a virtual MAC address which is assigned to a subinterface are not processed by the receiving router.

  Conditions: This is seen on Cisco routers which has any first hop redundancy protocol configured on a subinterface and bridging configured on a different subinterface under the same main interface. The bridging must be transparent bridging.

  Workaround: There is no known workaround that does not change bridging functionality. You can do one of the following:

  - You can disable bridging on that subinterface
  - Configure **bridge irb** instead of using transparent bridging.

- CSCsu95857

  Symptoms: The SNMP response of cardDescr (.1.3.6.1.4.1.9.3.6.11.1.3) for some indexes returns incorrect values.

  Conditions: Unknown conditions.

  Workaround: There is no workaround.

- CSCsv00773

  Symptoms: When an label switched path (LSP) reoptimization is attempted but the MPLS-TE Tunnel Head-end fails to find a better path, if the LSP contains loose hop sub-objects, a query is sent to downstream to determine whether downstream routers can find a better path. But downstream routers does not respond Path Error Message(Error code: Notify, Error value:Better path exists) to the Head-end even though they can find a more optimal path than the one in use.

  Conditions: Occurs when loose hop sub-objects are used on MPLS-TE Tunnel Head-end and downstream routers need to expand the loose hop sub-objects.

Workaround: Use other path option method such as dynamic path option, explicit with exclude address.

- CSCsv20768

  Symptoms: The clock source will be shown as LINE and the Path Trace buffer as UNSTABLE.

  Conditions: Occurs when you configure the clock source as INTERNAL under an ATM interface and do a SSO switchover.

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

- CSCsv27234

  Symptoms: Contr looped local, PPP interface line protocol down, should be line protocol down (looped)

  Conditions: Occurs when T3 controller is put in local loopback and the clock source is line, the interfaces configured on that controller are not looped. For clock source internal it works fine.

  Workaround: There is no workaround.

- CSCsv69906

  Symptoms: Multilink bundles are in non-distributed state after a stateful switchover (SSO).

  Conditions: Occurred on a Cisco 7600 with RSP 72043, SIP-200, and SPA-4xCT3.

  Workaround: Perform a **shut/no shut** on the bundles that are in non-distributed state.

- CSCsv75792

  Symptoms: Configured LI slot is not taking the active role after switchover.

  ```
  router#sh li-slot The Configured slot list: 3 The active LI slot: 3 Configured rate:
  1000000 pps
  router# router#redundancy force-switchover
  This will reload the active unit and force switchover to standby[confirm]
  Preparing for switchover..Connection closed by foreign host. router#sh li-slot The
  Configured slot list: 3 The active LI slot: RP rate: 8500 pps router#sh run | i
  li-slot li-slot list 3 rate 1000000 router#conf t router(config)#li-slot list 3 rate
  1000000 router(config)#^Z router#sh li-slot The Configured slot list: 3 The active LI
  slot: 3 Configured rate: 1000000 pps router#
  ```

  Conditions: Occurs on routers running Cisco IOS Release 12.2(33)SRC2 and Cisco IOS Release 12.2(33)SRD.

  Workaround: Use **li-slot list** command after switchover.

Open Caveats—Cisco IOS Release 12.2(33)SRC2

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRC2. 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.

Miscellaneous

- 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.

Resolved Caveats—Cisco IOS Release 12.2(33)SRC2

Cisco IOS Release 12.2(33)SRC2 is a rebuild release for Cisco IOS Release 12.2(33)SRC. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRC2 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCeb69473

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

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

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Trying 192.168.0.1...Open login:
*** System received a SegV exception *** signal= 0xb, code= 0x1100, context=
0x82f9e688 PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

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

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

  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/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.sh tml

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

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access
http://www.cisco.com/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd804ac831.pdf

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

- 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.

- CSCsc87117

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

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

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

- CSCsc94969

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

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

  Workaround: There is no workaround.

- CSCsd80349

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

  Conditions: Occur under the following scenario:

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

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

- CSCsj88665

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

  The device may also display Spurious Memory Accesses.

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

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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsl16323

  Symptoms: Traceback with the following message displayed:

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

  Conditions: This traceback is seen after doing stateful switchover.

  Workaround: There is no workaround.

- CSCsl19708

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

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

  Workaround: There is no workaround.

- CSCsl28246

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

  Conditions: This symptom is observed under TC sessions.

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

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

```
Nov 13 11:00:56.696 EST: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
AAA is allocating only 1024*32 = 32,768 IDs. Not able to bring up any more sessions
because of accounting flow ID allocation failure.
```

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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsl97384

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

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

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

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

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

- CSCsl99156

  Symptoms: 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.
  ```

  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.**

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsm23160

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

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsm44147

  Symptoms: The standby WS-SUP720-3BXL failed to boot into SSO mode because of MCL check failure with the FPD configuration command: **upgrade fpd path sup-bootdisk:**

  Conditions: The problem happens when "sup-bootdisk:" is used as the FPD image package directory path argument in the **upgrade fpd path** *pkg-dir-path* configuration command for an active WS-SUP720-3BXL that supports "sup-bootdisk:" filesytem, but the same fiilesystem is not support by the standby WS-SUP720-3BXL.

  Workaround: For systems that have a mixture of old and new WS-SUP720-3BXL, please do not use "sup-bootdisk:" as the filesystem in the **upgrade fpd path** *pkg-dir-path* configuration command, instead use the "sup-bootflash:" filesystem as this filesystem exist on both old and new WS-SUP720-3BXL.

  Further Problem Description: The **show module** EXEC command can be used to identify the HW revision of the WS-SUP720-3BXL, if it does not have a version above 5.x then it won't have the support of the "sup-bootdisk:" filesystem.

- CSCsm44620

  Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

  Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

  Workaround: Remove the following configurations:

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

- 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.

- 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.

- 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 iptivia probes in the network. Fixed in CRS.

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

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

- 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.

- 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.

- 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.

- 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 linecard(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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 linecards. The leak is seen in some port operations, such as port mode and port state changes.

  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.

- CSCsm85197

  Symptoms: CE routes learned through a GRE tunnel may not be installed in the VRF routing table.

  Conditions: The symptom is observed when the GRE tunnel configurations are changed from unnumbered to numbered and back to unnumbered.

  Workaround: There is no workaround.

- 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.

- CSCsm89526

  Symptoms: When a new class-map configuration is added to policy-map, packet (which belongs to another existing class) drop issue will be observed.

  Conditions: Occurs on a Cisco 7600 router with ES20 and running Cisco IOS Release SW 12.2(33)SRB.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCso04897

  Symptoms: The traffic passing in a class may be less than the configured bandwidth.

  Conditions: The symptom is observed when 100 percent bandwidth is assigned to user-classes. It is seen only on SIP-200 with Serial interfaces.

  Workaround: Reserve at least one percent of bandwidth for class-default.

  Further Problem Description: The same policy was applied to a an ATM interface on a SIP-400 using 2xOC3 ATM SPA and the flows were fill as expected.

- 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.

- 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.

- CSCso10596

  Symptoms: Polling cvpdnSessionAttrDevicePhyId from the CISCO-VPDN-MGMT MIB may show that multiple users are mapped to the same Virtual-Access SNMP ifIndex. This affects statistics collection or billing using IF-MIB counters.

  Conditions: This symptom is observed when PPP renegotiates an existing PPP connection on a Virtual-Access interface.

  Workaround: When possible, use RADIUS accounting for gathering statistics or billing.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route ***.

- 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.

- 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.

- 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.

- CSCso37750

  Symptom: In Cisco-data-collection MIB, when SNMP bulk transfer is configured and unconfigured the switch crashes. Also, in the flushed syslog messages the following buffer overflow message is noticed:

  ```
  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.

- 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.

- CSCso41824

  Symptoms: A router crashes with an unexpected exception to CPUvector 300.

  Conditions: This symptom is observed when you configure MPLS trunks on an 4xT3E3 SPA with FR IETF encapsulation.

  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.

- 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.

- 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

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCso56111

  Symptoms: The LC may crash if the **mpls traffic-eng tunnels** configuration is removed from the SIP600 interface.

  Conditions: The symptom is observed with a VPLS configuration and TE-FRR protection is configured for the primary ES-20 interface/tunnel which points to the SIP600 interface TE tunnel as a back-up path. If the **mpls traffic-eng tunnels** configuration is removed from the SIP600 interface, the LC crashes immediately.

  Workaround: There is no workaround.

- 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.

- 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

- 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.

- 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.

- 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.

- 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.

- 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

- 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.

- 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.

- 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.

- CSCso78716

  Symptoms: SNMP object entPhysicalVendorType returns incorrect value.

  Conditions: Occurs only on a Cisco 7603s.

  Workaround: There is no workaround.

- CSCso79720

  Symptoms: When the **show interface** command is entered , all of the Layer 2 swith port interfaces on ES-20 are shown with the same bridge MAC.

  Conditions: Only seen on ES-20.

  Workaround: 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCso93883

  Symptoms: Upon reload of a DFC, traffic coming from the MPLS cloud might be dropped when the traffic is destined for a EoMPLS connection on a MUX-UNI

  Conditions: This is seen on 12.2(33)SRB3 and 12.2(33)SRA3. The incoming module needs to be a DFC, and the egressing port needs to be a MUX-UNI. This does not happen to regular Ethernet Over MPLS (EoMPLS) connections.

  Workaround: Perform a **shut/no shut** on the connection towards the MPLS network, then **shut/no shut** the VC.

- CSCso99860

  Symptoms: Some of the initially shipped PWR-1500-DC power supplies in Cisco 7603S chassis have incorrect SNMP OID programmed in the IDProm. The vendorOID does not match with the CANA-assigned number in CISCO-ENTITY-VENDORTYPE-OID-MIB.my

Conditions: This is applicable for those power supplies for which the vendorOID is programmed as 193 and not as 194.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsq16830

  Symptoms: Stale NFS entry left on ESM20G card when diagnostics is enabled.

  Conditions: Occurs on Cisco 7609 ESM20G cards after the router is reloaded.

  Workaround: Disable diagnostics and reset the line card.

- 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.

- 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.

- CSCsq21589

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

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

  Workaround: Reload the router that is running ISG.

- 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.

- 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".

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsq59977

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsq73727

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

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

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

- CSCsq75350

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsq91348

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

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

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

- CSCsq91788

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

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

Workaround: There is no workaround.

- CSCsq91960

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

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

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

  Workaround: There is no workaround.

- 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.

- 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

- 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**.

- 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.

- 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.

Open Caveats—Cisco IOS Release 12.2(33)SRC1

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRC1. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsl74787

  Symptoms: MR-APS 1+1 bidirectional protection switching is failing on a interface configured on a SPA-1CHOC3-CE-ATM inserted in a SIP-400. The APS switching from the working interface on to the protect interface is not occurring upon a Loss of Signal (LOS) defect detected on the APS working interface (receive fiber disconnect on the SPA-1CHOC3-CE-ATM).

  Conditions: A Loss of Signal (LOS) defect detected on the APS working interface (receive fiber disconnect on the SPA-1CHOC3-CE-ATM).

  Workaround: There is no workaround.

- CSCsq37051

  Symptoms: Router may crash while removing a VRF.

  Conditions: This was discovered during testing and is not likely to occur in customer environments. Occurs with a IPv6 VRF created using MULTI-AF commands. The router may crash if the following steps are done:

  – Delete and re-add **address-family ipv6** (under vrf definition *name*) several times.

  – Use **no vrf definition** *name* to remove the VRF.

  Workaround: Avoid this negative test.

  - If you want to delete IPv6 address-family, you may do so but do not toggle (add back and delete) the IPv6 address family configuration under VRF.
  - You may also delete VRF definition configuration and wait for its deletion before adding the same VRF name back.

- CSCsq42473

  Symptoms: Enabling Frame Relay causes pings to fail

  Conditions: Occurs on Cisco 7200 routers running c7200-ipbasek9-m images.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRC1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRC1. This section describes only severity 1, severity 2, and select severity 3 caveats. See also Resolved Caveats—Cisco IOS Release 12.2(33)SRB1, page 1239 and Resolved Caveats—Cisco IOS Release 12.2(33)SRB2, page 1183.

Miscellaneous

- CSCdv07156

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

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

  Workaround: There is no workaround.

- CSCdy22725

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

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

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

- CSCec34459

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

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

  Workaround: There is no workaround.

- CSCef15846

  There are two symptoms which are fixed by this bug.

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

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

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

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

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

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

Workaround 2: There is no workaround.

- CSCek57749

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

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

  Workaround: There is no workaround.

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

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

- CSCek75931

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

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

  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, a L2TP multi-hop node may crash

  Conditions: Occurs when a session is being disconnected.

  Workaround: There is no workaround.

- CSCsb36463

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

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

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

- CSCsc77148

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

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

  Workaround: There is no workaround.

- CSCse15434

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

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

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

- CSCse65277

  Symptoms: Standby reloads due to default ISIS metric maximum returns parser error.

  Conditions: This issue is observed while configuring the ISIS metric maximum on an interface by using the **isis metric maximum** command and later changing it in to the default metric value.

  Trigger: At this point, it will show the error, and the communication with the peer Supervisor has been lost then the standby reloads.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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 Cisco’s public website: http://www.cisco.com/warp/public/707/confaccesslists.html

- 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.

- 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 Line Card for SVI based EoMPLS or VPLS. PFC-based EoMPLS is not affected.

Workaround: There is no workaround.

- CSCsi97434

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

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

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

- CSCsj00870

  Symptoms: The following error messages are seen during system bootup, swichtover or online insertion and removal (OIR):

  ```
  c6lc2-spdbg-5-dso-b.so+0x10FAC4: verrmsg ../os/logger.c:0
  c6lc2-spdbg-5-dso-b.so+0x110168: errmsg ../os/logger.c:0
  c6lc2-spdbg-15-dso-b.so+0x2B7A04: datagram_done ../os/buffers.c:0
  c6lc2-spdbg-16-dso-b.so+0xC2DCC: logger_icc_callback
  ../const/native-sp/logger_sp.c:0 c6lc2-spdbg-13-dso-b.so+0x57BD90: icc_request_cb
  ../const/native/icc_request.c:0 c6lc2-spdbg-13-dso-b.so+0x57BE10:
  icc_request_cb_new ../const/native/icc_request.c:0 c6lc2-spdbg-4-dso-b.so+0xB25BC:
  ipc_deliver_message ../ipc/ipc_server.c:0 c6lc2-spdbg-4-dso-b.so+0xB2BA8:
  ipc_process_insequence_message ../ipc/ipc_server.c:0
  c6lc2-spdbg-4-dso-b.so+0xB3794: ipc_process_message ../ipc/ipc_server.c:0
  c6lc2-spdbg-4-dso-b.so+0xB3DF4: ipc_process_raw_pak ../ipc/ipc_server.c:0
  c6lc2-spdbg-17-dso-b.so+0x4C870: sb1250_eobc_process_rx
  ../const/sb-common/sb_common_eobc.c:0 c6lc2-spdbg-17-dso-b.so+0x4D0F8:
  eobc_rx_interrupt ../const/sb-common/sb_common_eobc.c:0
  c6lc2-spdbg-17-dso-b.so+0x50020: sb1250_eth_callback ../src-sibyte/dev/sb_eth.c:0
  ```

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

  Workaround: There is no workaround.

- CSCsj21785

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

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

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

- CSCsj56281

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

  Workaround: There is no workaround.

- CSCsj67096

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

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

Conditions: Occurs on the following configuration: * Cisco Catalyst 6000 series switches * Supervisor Engine 720 * Cisco IOS Release 12.2(18)SXF7

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

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

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

- CSCsj85065

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

  Cisco has released free software updates that address this vulnerability.

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

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

- 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.

- CSCsk07097

  Symptoms: After clearing PPPoEoVLAN session, applying a HQoS policy on the VLAN fails.

  Conditions: This issue occurs on a Cisco 10000 series router with PRE3 board. A session comes up on a VLAN/QinQ, and HQoS is applied to that session. When the session is removed, applying a HQoS policy on the VLAN/QinQ fails.

  This only occurs if the session parent policy is configured with "bandwidth remaining ratio x".

  Workaround: There is no workaround.

- CSCsk19497

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

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

  Workaround: There is no workaround.

- CSCsk26165

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

Conditions: The router must be configured for L2TP.

Workaround: There is no workaround.

- CSCsk32095

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsk54061

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

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

  Workaround: There is no workaround.

- CSCsk55423

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

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

  Workaround: There is no workaround.

- 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.

- CSCsk68320

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

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

  Workaround: There is no workaround.

- CSCsk68846

  Symptoms: Router Crashed when removing grandchild policy

  Conditions: Seen on a Cisco 7304 Router.

  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:

1. If the network has a mVPN deployment, and the path between source and receiver has to traverse through the mVPN cloud.
2. 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.

- 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.

- CSCsk85987

  Symptoms: The line protocol state of SVI interfaces is incorrectly marked “down” after an SSO switchover.

  Conditions: This is sometimes seen on the second and subsequent SSO switchovers.

  Workaround: Reload the line card that has the affected interface.

- CSCsk86381

  Symptoms: Memory leak 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.

- CSCsk93241

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsl02649

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- 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:

```
#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.

- 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 repapply. 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.

- 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.

- 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.

- CSCsl27926

  Symptoms: For GRE tunnel inside VRF feature with source address in a different VRF, some times traffic will not flow through after an SSO switchover or DFC online insertion and removal (OIR) for DFC having the ingress interface.

  Conditions: Occurs when **tunnel vrf <vrf>** is configured on GRE tunnel and SSO switchover or DFC OIR is done.

  Workaround: No viable workaround. Only way to recover from this condition is to reload router.

- 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.

- 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.

- CSCsl31683

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

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

  Workaround: Reload the SPA

- CSCsl32344

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

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

  Workaround: Reset the line card.

- CSCsl33632

  Symptoms: Router crashes when VRF is unconfigured.

  Conditions: Router crashes when **no ip vrf** is executed. This is a platform independent issue. This issue is seen while using a script. Manually this issue is not seen.

  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.

- 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 heretical 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.

- 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.

- 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.

- 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.

- 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.

- CSCsl50569

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

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

  Recovery: To recover connectivity, there are two options. Option 1 is preferable since it causes less traffic interruption. If Option 1 does not work, then Option 2 should be performed. 1. Attach to the switch processor (**remote login switch**) and issue the command: **test fpoe index 0 FFFF restore** 2. Reload the ingress SIP-400 line card: **hw-module module** *mod* **reset**

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

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

- CSCsl50774

  Symptoms: Line Card crashes repeatedly during boot after an unsuccessful FPD upgrade.

  Conditions: Affects Cisco IOS Release 12.2SRB and will prevent the line card from booting

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.

- 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 line card image. This crash will not happen if you reset the module after the upgrade is complete.

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

- CSCsl52092

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

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

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

- CSCsl52220

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

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

  Workaround: There is no workaround.

- 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.

- CSCsl54875

  Symptoms: The **test platform firmware get asic** command may reset the module. The following error messages are displayed:

  ```
  00:27:15: %PM_SCP-SP-1-LCP_FW_ERR: System resetting module 4 to recover from
  error: Line Card received system exception 00:27:15: %OIR-SP-3-PWRCYCLE: Card in
  module 4, is being power-cycled Off (Module Reset due to exception or user
  request) 00:27:15: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set Off
  (Module Reset due to exception or user request)
  ```

  Conditions: - Cat6500 switch or Cisco7600 running 12.2(33)SRB1 or SRB2 release. - This issue is NOT applicable for 12.2(18)SXF releases. - Affected Modules: WS-X6704-10GE WS-X6748-GE-TX

  Workaround: Use **test platform firmware component to capture ASIC register values.**

- CSCsl54889

  Symptoms: When ISG is configured as a DHCP relay and the DHCP client is rebooted or if the DHCP client sends a DISCOVER packet in error, ISG is unable to process subsequent DISCOVER packets.

  Conditions: This symptom occurs when ISG is configured as a DHCP relay, and the DHCP client is either rebooted or sends a DISCOVER packet in error.

  Workaround: Configure ISG as a DHCP server.

- CSCsl55521

  Symptoms: Router may experience BGP convergence issues.

  Conditions: This problem has been seen when 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.

- 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.

- CSCsl62346

  Symptoms: Class queue experiences unexpected high packet drops

  Conditions: This is noticed on Cisco 7600 series routers running Cisco IOS Release 12.2SRB and later. When a service policy is applied on ATM PVC on SPA-2xOC3-ATM hosted by 7600-SIP-400, the packet drops are unusually high and throughput on the class queue is much less than the expected.

  Workaround: Configure Weighted Random Early Detection (WRED) on the class queue by using the **random-detect aggregate** command. Or increase the queue length of the class using the **queue-limit command** command, but this is an inefficient use of buffers.

- 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.

- 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 configuraiton, 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 anything over MPLS (AToM) VCs configured after their line card reset may not come up.

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

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

- CSCsl79195

  Symptoms: Following boot, or reload, of standby supervisor, the XDR_ISSUNEGOFAIL errmsg is seen relating to the standby SP. This can only be seen on a Cisco 6500/7600 as this is specific to the supervisor card.

  Conditions: This symptom is only seen if the standby supervisor is reloaded after it has first booted far enough for the XDR peers representing it to have been created on the active RP, but before the platform signals the OIR event for the card. A typical scenario is a transient RF progression failure.

  Workaround: Reload the standby supervisor.

- CSCsl79219

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

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

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

- 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.

- CSCsl82259

  Symptoms: When ATM AAL5 mode scalable anything over MPLS (AToM) is configured on PE router and input traffic from CE uses AAL5 SNAP bridge encapsulation, traffic is dropped by the line card.

  Conditions:

  1. Scalable AToM using AAL5 mode.
  2. Incoming traffic uses AAL5 SNAP bridge encapsulation.

  Workaround: Do not use AAL5SNAP encapsulation to configure PVC.

- CSCsl83211

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

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

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

- CSCsl83415

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

Test10 : --------- a. clear ip bgp 10.0.101.46 ipv4 multicast out b. clear ip bgp 10.0.101.47 ipv4 multicast out

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

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

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

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- 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 line card
  ```

  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.

- CSCsl86633

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

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

  Workaround: There is no workaround.

- CSCsl88931

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

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

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

  Workaround: There is no workaround.

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

- CSCsl89176

  Symptoms: Router crashes while polling for VLAN information.

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

  Workaround: Configure the following commands;

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

  Note that the ACL is optional

- CSCsl89425

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

  Conditions: Occurs when configuring maximum BFD sessions or total number of BFD sessions too close to maximum limit.

  Workaround: Configure 90% of maximum allowed BFD sessions.

- 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.

- 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 line card crashes on a Cisco 7600 router running Cisco IOS Release 12.2SR image.

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

  Workaround: There is no workaround.

- CSCsl94259

  Symptoms: When applying the service policy on main interface, exceed error message is seen.

  Conditions: This symptom occurs when applying a policy or doing the OIR.

  Workaround: There is no workaround.

- CSCsl94499

  Symptoms: When applying the **mpls ip** under the top configuration mode command, the standby RP may be reset and the active RP generates the following error message:

  Dec 27 09:14:43.095 PST: %RTMGR-3-TOPO_SYNC_ERR: Failed to duplicate active topology on standby. (rc=15), id 1E000000 {default:ipv6:base}

  Conditions: The problem happens on a Cisco 7600 series router when applying the **no mpls ip** top configuration mode command.

  Workaround: Enable the IPv6 routing explicitly via the **ipv6 unicast- routing** command before issuing the **no mpls ip** command.

  Further Problem Description: There is a synchronization (or timing) issue on IPv6 routing shutdown between active and standby RPs.

- CSCsl94621

  Symptoms: For the ATM multi-VLAN to VC feature, when the remote end of the link flaps, the spanning tree instance for the VLAN gets lost, 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.

- CSCsl95249

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

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

  Workaround: There is no workaround.

- CSCsl95664

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

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

  Workaround: There is no workaround.

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

- 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. This is seen during the router upgrade with ATM ACs (configured with xconnect),configuration from rsp72043-adventerprisek9-mz.122-33.SRB2 to rsp72043-adventerprisek9-mz.122-32.8.11.SRC6.

  Workaround: There is no workaround.

- CSCsl98498

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

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

  Workaround: There is no workaround.

- CSCsm01334

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

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

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

  Workaround: There is no workaround.

- CSCsm01399

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

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

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

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

- 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
  ```
- 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 line card.

- CSCsm12247

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

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

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

  Additional Information: The changes address also situation where some WCCP clients are sending modified weight field in the WCCP message and this way create a topology change situation. This applies also to configurations using mask assignment.

- 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 swichtover.

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

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

- CSCsm13783

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

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

  Workaround: There is no workaround.

- CSCsm15406

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

  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.

- 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.

- CSCsm20994

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

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

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

- CSCsm21728

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

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

Workaround: There is no workaround.

- 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.

- CSCsm26150

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

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

  Workaround: There is no workaround.

- CSCsm27071

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

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm27455

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

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

  Workaround: No workaround available.

- CSCsm27565

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

  ```
  *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.

- 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.

- CSCsm32555

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

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

  Workaround: There is no workaround.

- CSCsm33193

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

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

  Workaround: There is no workaround.

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

- CSCsm33925

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

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

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

- CSCsm34361

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

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

Workaround: There is no workaround.

- CSCsm34469

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

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

  1. Redundancy mode SSO.
  2. PPP encapsulation.
  3. PPP multilink with the interface created.

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

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

- CSCsm36500

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

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

  Workaround: There is no workaround.

- CSCsm38142

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

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

  Workaround: There is no workaround.

- CSCsm39159

  Symptoms: ARP HA CPU tracebacks may be seen on the STANDBY PRE while it is booting up.

  Conditions: This symptom is seen under extreme cases of large ARP tables. The Cisco 10000 router could generate ARP HA tracebacks on the STANDBY PRE while it is booting up.

  Workaround: There is no workaround.

- CSCsm40013

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

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

  Workaround: There is no workaround.

- CSCsm41685

  Symptoms: The ciscoEnhancedMemPoolMIB table is empty.

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

  Workaround: There is no workaround.

- CSCsm42758

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

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

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

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

- CSCsm43482

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

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

  Workaround: There is no workaround.

- CSCsm43938

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

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

  Workaround: There is no workaround.

- CSCsm44720

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

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

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

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

- CSCsm44914

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

  Conditions: Occurs on Cisco 7600 routers configured with ISG.

  Workaround: There is no workaround.

- CSCsm45950

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

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

  Workaround: There is no workaround.

- CSCsm46290

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

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

  Workaround: There is no workaround.

- CSCsm46903

  Symptoms: The following error messages occur:

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

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

  Workaround: Perform another OIR of the line card.

- CSCsm47544

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

  - SIP200
  - Flexwan
  - Enhanced Flexwan

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

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

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

- CSCsm48357

  Symptoms: When FlexWAN card configured for Frame Relay over MPLS (FRoMPLS) is subjected to online insertion and removal (OIR), the standby will crash when FRoMPLS is unconfigured.

  Conditions: Occurs when FRoMPLS is unconfigured following an OIR

  Workaround: There is no workaround.

- CSCsm49214

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

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

  Workaround: There is no workaround.

- CSCsm49865

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

Conditions: Can occur when an interface flaps.

Workaround: There is no workaround.

- CSCsm50309

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

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

  Workaround: There is no workaround.

- CSCsm51333

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

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

  Workaround: There is no workaround.

- CSCsm51729

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

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

  The following traceback may also be seen:

  ```
  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.

- 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 line card fib-disable action none** command.

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

- CSCsm53489

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

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

  Workaround: 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 line card is the backup FRR LC/interface; traffic for software EoMPLS and Virtual Private LAN Services (VPLS) is not restored following a failover and re-optimization. It appears that software EoMPLS/VPLS core-side imposition entries do not exist on the SIP-400 line-card after re- optimization.

- CSCsm54548

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

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

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

- CSCsm54873

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

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

  This problem exists on all shipped versions of IOS XE.

  Workaround: There is no workaround.

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

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

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

  SXF is not impacted by this bug.

- CSCsm57494

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

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

  Workaround: There is no workaround.

- CSCsm58612

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

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

  Workaround: There is no workaround.

- CSCsm58677

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

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

  Workaround: There is no workaround.

- CSCsm59499

  Symptoms: TOOBIG error msgs being displayed on the console.

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

  Workaround: There is no workaround.

- CSCsm60223

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

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

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

Workaround: There is no workaround.

- CSCsm61105

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

  Conditions: The crash is seen under the following conditions.

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

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCsm62533

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

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

  Workaround: There is no workaround.

- CSCsm62748

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

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

  Workaround: There is no workaround.

- CSCsm64643

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

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

  Workaround: There is no workaround.

- CSCsm65584

  Symptoms: System convergence delay with scaled config.

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

  Workaround: There is no workaround.

- CSCsm65976

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

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

Workaround: Use the following:

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

- CSCsm66228

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

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

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

- CSCsm66678

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

  Conditions: Policing is not working in the MPLS cloud. Even though packets are getting classified correctly, policing is not working on those packets.

  Workaround: There is no workaround.

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

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

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

- CSCsm66774

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

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

  Workaround: There is no workaround.

- CSCsm69368

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

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

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

- CSCsm71240

  Symptoms: Standby unable to ping to Virtual IP address.

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

Workaround: There is no workaround.

- CSCsm71592

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

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

  Workaround: There is no workaround.

- CSCsm72807

  Symptoms: The following message is seen:

  ```
  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

- CSCsm73365

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

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

  Problem Case

  QT=0 , IT >0 apply L4RD , L4RD is NOT removed upon reauthorization ,

  QT>0 , IT>0 Default-service installed ,

  !

  class type control cm-DEF_Inet event credit-exhausted

  1 service-policy type service name DEF_Inet_L4R

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

  Working Case

  QT=0 , IT >0 apply L4RD , L4RD is removed upon reauthorization ,

  QT>0 , IT>0 Default-service installed

  !

  class type control always event credit-exhausted

  1 service-policy type service name DEF_Inet_L4R

- CSCsm74961

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

Conditions: Cisco 7600 configured as follows: *Initiator: IPoQ/DHCP *IP Address Assignment: Radius class name, ISG-DHCP Relay *Authorization: TAL (MAC+Opt82) *Network Service: VRF Mapping *Accounting: Postpaid *QoS: Session MQC *Service/features: Security ACL, ARP Ping, Open Garden

Workaround: There is no workaround.

- CSCsm75286

  Symptoms: A route-map which is configured with both IPv4 and IPv6 for a BGP peer does not work correctly when it is deleted part of the sequences.

  Conditions: Occurs when a route-map with a BGP peer is deleted part of the sequences.

  Workaround: There is no workaround.

- CSCsm75642

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

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

  Workaround: Reload the router.

- CSCsm77173

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

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

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

- CSCsm79148

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

  Conditions: SNMPwalk failing with packet too big error.

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

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

- CSCsm79995

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

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

  Workaround: There is no workaround.

- CSCsm83777

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

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

  Workaround: There is no workaround.

- CSCsm84257

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

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
```
Conditions: This has been seen on a Cisco 7600 running Cisco IOS Release 12.2(33)SRC. The bug is platform independent.

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**

- 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.

- CSCsm88496

  Symptoms: MPLS disposition traffic on ESM20 may get dropped.

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

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

- CSCsm89620

  Symptoms: Billing fails for users.

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

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

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

- CSCsm89735

  Symptoms: A router might crash when the **show idb** command is issued.

  Conditions: The crash is seen when the **show idb** command is issued after a large number of PPPoE sessions (for example, 6000 sessions) are initiated and cleared. The crash is seen with IPv6, but it is not seen with IPv4.

  Workaround: There is no workaround.

- CSCsm90366

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

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

Workaround: There is no workaround.

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

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

- CSCsm90525

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

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

  Workaround: There is no workaround.

- CSCsm91084

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

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

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

- CSCsm92365

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

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

  Workaround: There is no workaround.

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

- CSCsm92389

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

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

  Workaround: Reapply "spanning-tree bpdufilter disable".

- CSCsm92916

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

  Conditions: Occurs on the following hardware:

  – SPA-24CHT1-CE-ATM

- SPA-1CHOC3-CE-ATM
- SPA-2CHT3-CE-ATM

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

- CSCsm93088

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

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

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

- CSCsm94385

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

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

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

- CSCsm94533

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

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

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

- 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.

- 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.

- 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.

- CSCsm99651

  Symptoms: Link down notification is slow on ES-20.

  Conditions: Occurs on 10GE ports of ES-20 line card, when fiber is removed to simulate link failure, it might take up to 3 seconds for MPLS TE FRR to respond. Issue is intermittent.

  Workaround: Shutdown the port on the remote device.

- CSCsm99690

  Symptoms: Router crashing when it tries to export with Netflow Version 9 format.

  Conditions: Router is configured with Netflow Version 9 on aggregation and netflow main cache. Problem is seen when aggregation caches are configured, and export is configured to one collector in the global table and one collector in a VPN.

  Workaround: Do not use Netflow Version 9.

  Further Problem Description: Netflow Version 9 configuration should be configured with destination. When Version 9 configuration and unconfiguration tried on aggregation and main cache many times may lead to crash due to reset of aggregation functionalities set to NULL.

- CSCsm99975

  Symptoms: Routers running Cisco IOS Release 12.2(33)SRC are experiencing module resets when another router is being reset. All modules on all routers running this image are reset, excluding the Supervisor Engine 720 module.

  Conditions: Occurs on Cisco 7606 and Cisco 7609 router with 67XX modules with DFC3BXL. IPv6 is configured on interfaces on those modules and crash decodes point to IPv6.

  Workaround: There is no workaround.

- CSCso00482

  Symptoms: The output of the **show lacp internal detail** command does not display the complete name of member links correctly.

  Conditions: The problem happens when the interface has a long name.

  Workaround: There is no workaround.

- CSCso02266

  Symptoms: Cisco 7600-SIP-600 may crash when carrying a EOMPLS or VPLS VC's over TE/FRR tunnels.

  Conditions: Crash may be observed when the primary TE path goes down.

  Workaround: Avoid TE/FRR configuration for EOMPLS/VPLS VC's on sip600.

- CSCso04286

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

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

  Workaround: There is no workaround.

- CSCso06409

Symptoms: A Cisco 7600 (RSP720-3C/CXL) may experience high CPU utilization from the moment (S,G) expires due to all outgoing interfaces are down.

Conditions: This symptom occurs when indirect-connected multicast source traffic arrives at PIM-RP router without any receiver on that group, a (*,G) state with NULL RPF interface and NULL OIL is created and used to forward the traffic. Because of NULL RPF, this (*,G) state cannot be installed in Cisco 7600 hardware. The multicast data packet is punting to CPU and causes high CPU utilization.

Workaround: Partial workaround is to apply RP rate-limiter with fib-miss option.

- CSCso07811

  Symptoms: Remote-id and circuit-id are no longer formatted as Type Length Value (TLV) in radius packets.

  CLI command to enable legacy behavior (formatting remote-id and circuit-id) 1. config t 2. subscriber policy format_option82_for_cats

  New behavior:

  remote id 00046aacfc82 circuit id 00000009

  Radius see it as:

```
*Apr 16 05:33:30.695: RADIUS: User-Name [1] 16 "aabb.cc00.6500"
*Apr 16 05:33:30.695: RADIUS: User-Password [2] 18 *
*Apr 16 05:33:30.695: RADIUS: Calling-Station-Id [31] 14 "00046aacfc82"
*Apr 16 05:33:30.695: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
*Apr 16 05:33:30.695: RADIUS: Vendor, Cisco [26] 31
*Apr 16 05:33:30.695: RADIUS: Cisco AVpair [1] 25 "circuit-id- tag=00000009"
*Apr 16 05:33:30.695: RADIUS: Vendor, Cisco [26] 34
*Apr 16 05:33:30.695: RADIUS: Cisco AVpair [1] 28 "remote-id- tag=00046aacfc82"
*Apr 16 05:33:30.695: RADIUS: NAS-Port [5] 6 0
```

  Legacy behavior:

```
remote id 00046aacfc82 circuit id 00000009
```

  Radius see it as: (note the extra characters)

```
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.

- CSCso09791

  Symptoms: When configuring an incorrect de-jitter buffer value on CEM interface, the CEM group will stay down and not recover until the SPA is reloaded.

  Conditions: This symptom only occurs if the de-jitter is out of range. Acceptable range is as follows:

```
# DS0smax pay max j(ms) min j(ms) min paymax j(ms) min j(ms)
1 40 320 10 32 256 8
2 80 320 10 32 128 4
3 120 320 10 33 128 4
```

```
4 160 320 10 32 64 2
5 200 320 10 40 64 2
6 240 320 10 48 64 2
7 280 320 10 56 64 2
8 320 320 10 64 64 2
9 360 320 10 72 64 2
10 400 320 10 80 64 2
11 440 320 10 88 64 2
12 480 320 10 96 64 2
13 520 320 10 104 64 2
14 560 320 10 112 64 2
15 600 320 10 120 64 2
16 640 320 10 128 64 2
17 680 320 10 136 64 2
18 720 320 10 144 64 2
19 760 320 10 152 64 2
20 800 320 10 160 64 2
21 840 320 10 168 64 2
22 880 320 10 176 64 2
23 920 320 10 184 64 2
24 960 320 10 192 64 2
25 1000 320 10 200 64 2
26 1040 320 10 208 64 2
27 1080 320 10 216 64 2
28 1120 320 10 224 64 2
29 1160 320 10 232 64 2
30 1200 320 10 240 64 2
31 1240 320 10 248 64 2
```

Workaround: The CEM group will come up when:

- De-jitter is reconfigured in acceptable range
- CEoP SPA is reloaded.

- CSCso11822

  Symptoms: Sometimes the "channel-group" configuration is lost from member ports of a primary aggregator on removal and reinsertion of a line card.

  Conditions: The LACP port-channel should have member ports belonging to a primary aggregator on the line card that is removed and reinserted. This problem happens intermittently only when primary and secondary aggregators are present.

  Workaround: There is no workaround.

- CSCso12748

  Symptoms: Tunnels between Cisco and non Cisco peers fail to come up since the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Conditions: This symptom occurs because the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Workaround: There is no workaround.

- CSCso13791

  Symptoms: OSPF neighbor adjacency is formed and lost over a QinQ subinterface every few minutes. This may keep happening indefinitely. Traffic forwarding on this subinterface is affected as OSPF adjacency flaps.

  Conditions: This problem is observed in a Cisco 7600 series with an RSP720 Supervisor Engine if OSPF has been configured on a QinQ subinterface on an ES20 or ES40 module. The problem is not seen if single tag encapsulation is used.

  Workaround: There is no workaround.

Further Problem Description: On a subinterface that is configured with a QINQ encapsulation in a system with an RSP720 supervisor, protocol packets will be dropped, so this will affect other layer 3 protocols in addition to OSPF.

- CSCso14979

  Symptoms: Distributed CEF gets disabled for a line card.

  Conditions: This symptom can happen for a few reasons:

  1. Heavy IPC load leading to backplane congestion causing timers (started to monitor distribution) to time out.
  2. Breakdown of IPC communication between the RP and the line card.
  3. Lack of memory to install FIB updates on the line card.

  Workaround: The only way to restart distributed CEF for the disabled line card is by resetting or OIR the line card.

- CSCso19075

  Symptoms: From SNMP, using MIB object cRFCfgAdminAction.0 to perform SSO does not work. The effect is no switchover is performed.

  Conditions: This symptom happens when user tries to use SNMP to initiate a switchover.

  Workaround: Use the **redundancy** command instead of the **snmp** command.

- CSCso20519

  Symptoms: There is some probability of Cisco IOS bootup failures on the Cisco 7600-SSC-400.

  Conditions: The failures are seen at cold temperature corners in testing. There are no failures reported from the field.

  Workaround: There is no workaround.

- CSCso21611

  Symptoms: Device crashes due to memory allocation issue.

  Conditions: Observed on Cisco 7200, but this is not a platform-specific bug.

  Workaround: There is no workaround.

- CSCso21888

  Symptoms: Router may spontaneously reload.

  Conditions: Occurs on routers configured with iSPF computation algorithm in OSPF.

  Workaround: Disable iSPF.

- CSCso22098

  Symptoms: OSPF neighborship goes down on RPR+ switchover on core router. The router does not send any hello packets to the connected routers.

  Conditions: Occurs when executing RPR or RPR+ switchover. No Problem seen with SSO switchover.

  Workaround: There is no workaround.

- CSCso22328

  Symptoms: If you have a ip-session l2-connected your interface config will show "ip subscriber l2-connected" and , you are redirecting a session upon session start event for a web-portal-log-on

  !

policy-map type control web-logon

class type control always event session-start

10 service-policy type service aaa list BH-125 name L4_SERVICE

20 service-policy type service aaa list BH-125 name PBHK_SERVICE

!

class type control always event account-logon

10 authenticate aaa list WEB_LOGON

20 service-policy type service unapply name L4_SERVICE

Upon doing account-log-on form the portal , ISG does not include attribute 31 = mac-address in access-request sent to AAA.

Symptom: When doing web-log-on using CoA Account-log-on , access-request is missing attr-31 , example:

```
Mar 14 12:35:07.462: RADIUS(00000273): Send Access-Request to 10.30.81.21:1812 id
1645/74, len 252
Mar 14 12:35:07.462: RADIUS: authenticator 06 CA 9B E6 63 13 A9 DD - 6C BC C9 ED E5 74
19 49
Mar 14 12:35:07.462: RADIUS: User-Name [1] 10 "easy-vrf" Mar 14 12:35:07.462: RADIUS:
User-Password [2] 18 *
Mar 14 12:35:07.462: RADIUS: Calling-Station-Id [31] 16 "0002.1760.E1C3" << << <This
may be a problem for some policy managers.
```

Workaround: There is no workaround.

- CSCso23419

  Symptoms: The CBTS master tunnel goes down on rare occasion when the path change occur on all the members. Even after a member tunnel comes up, the master tunnel does not report up for 10 seconds.

  The CBTS members are configured with the same sequence of explicit path-options. When the link down occur on head-end on the LSP path, the new LSP are setup as the next-path on all the members in this case.

  This only impacts the reporting of the master tunnel state.

  Conditions: Configure the same sequence of explicit path-options on all the members.

  Workaround: There is no workaround.

- CSCso24243

  Symptoms: A VC associated with a VT keeps flapping.

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

  Workaround: There is no workaround.

- 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.

- CSCso27913

  Symptoms: Router crashes doing write memory with color-aware policer configuration.

Conditions: The crash occurs if the color-aware policer is referencing a class-map which has been removed from the configuration.

Workaround: Remove color-aware policer configuration before removing the class-maps to which it references.

- 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.

- 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.

- 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.

- CSCso44120

  Symptoms: Unable to perform SNMPwalk of clcFdbVlanInfoTable.

  Conditions: Occurs all the time.

  Workaround: There is no workaround.

- CSCso49598

  Symptoms: Standby reloads continuously when "MAXINT" is used with "int ran" to create logical interfaces using.

  Conditions: Occurs in SSO mode.

  Workaround: Avoid giving MAXINT as range.

Further Problem Description: At a stretch, only 1000 logical interfaces could be created through interface range. Due to some wrap-around problem, it was not showing error when MAXINT was given as option and starts creating these many interfaces which are much beyond the MAXINTERFACES supported by any existing platform. It will lead to MEMORY getting exhausted and different after effects as standby reload.

- CSCso50383

  Symptoms: In a Cisco 7600 ring topology with TE-FRR configuration, traffic might get software switched if the packet comes in on a interface and goes out of the same interface.

  Conditions: This can happen in a topology like the following:

```
R1 -------------- R2 ---------------- R3
|                                    |
|----------------- R4 ------------------|
```

  Link between R3 - R4 is protected via R3 -> R2 -> R1 -> R4 (typical ring topology). R1 and R3 are the end points of a VC. Normally traffic will take the primary TE tunnel via R-> R4 -> R1. When R3 -> R4 link is shut, traffic will go on the back tunnel, R3 -> R2 -> R1 -> R4. In R4, traffic will be sent back on the incoming interface to R1, VC destination. Now in R4 traffic will get punted to RP and route cached.

  Workaround: There is no workaround.

  Further Problem Description: These drops also ignore QoS markings and affect all service classes.

- CSCso50794

  Symptoms: The **show spanning-tree vlan <vlan id> interface port-channel <int id>** command shows only option as EFP, and all other alternate options are not available.

  Conditions: The Symptom shows up whenever there is either port-channel interface or GigaEthernet interface.

  Workaround: There is no workaround.

- CSCso53489

  Symptoms: If you remove a policer from parent class of a hierarchical policy which also has policers in child policy, the policers get removed from the child policy as well. If you then add back the parent policer and show running, the router crashes.

  Conditions: Occurs with hierarchical policer configuration.

  Workaround: Detach policy from all interfaces before removing policer from parent class.

- 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.

- CSCso55190

  Symptoms: Cisco 7600-SIP-400 crashes when changing the QoS scheduler configuration.

  Conditions: The crash has been observed on a Cisco 7604/MSFC2A/SUP32 running Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCso56101

Symptoms: Some CFM remote MEPs may not appear as up when connected by a SIP-400 line card.

Conditions: When a large number of remote MEPs are connected via an interface on a SIP-400 line card, they may not all appear.

Workaround: There is no workaround.

Further Problem Description: The remote MEPs are seen as CFM errors with a status of "lifetime timer expired" under the "show ethernet cfm errors" command.

- CSCso57001

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

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

  Workaround: There is no workaround.

- CSCso57407

  Symptoms: The standby Router resets and goes to RPR mode due to this config-sync issue. On Cisco 7600 platform upgrading an image from Cisco IOS Release 12.2(33)SRB to Cisco IOS Release 12.2(33)SRC may fail and the redundant routers will operate in RPR mode if the following command is configured under an interface.

  interface TenGigabitEthernet2/0/0
  l2protocol-tunnel drop-threshold lldp 20.
  The problem can be verified by executing the following show command.

```
 show redundancy config-sync failures mcl
Mismatched Command List
-----------------------
interface TenGigabitEthernet2/0/0
! "interface"
- l2protocol-tunnel drop-threshold lldp 20
!
"interface"
```

  Conditions: The Cisco 7600 routers running Cisco IOS Release 12.2(33)SRB or Cisco IOS Release 12.2(33)SRC will observe the problem only if the configuration command **l2protocol- tunnel drop-threshold lldp 20** is configured under the interface.

  Workaround: The problem can be worked around by entering **no l2protocol-tunnel drop-threshold lldp 20** under the interfaces.

- CSCso57695

  Symptoms: A Cisco 7200 router crashes or hangs with input QoS policing.

  Conditions: This may occur when there is a single-level output queuing policy configured and a two-level input policing policy, not necessarily on the same interface.

  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.

- CSCso66668

  Symptoms: FlexWAN line card crashes in Cisco 7600 chassis.

  Conditions: Occurs when “bre-connect” is configured on an ATM PVC.

Workaround: There is no workaround.

- CSCso66862

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

  Conditions: The crash is seen under the following conditions.

  1. Bringing up nearly 3k PPPoE and PPPoEoA sessions.
  2. Configuring **no interface virtual-template <no>** under ATM interfaces.

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCso68007

  Symptoms: Ethernet Out of Band Channel (EOBC) can halt on standby or active.

  Conditions: Occurs during very rare periods of EOBC traffic-intensive functions such as syncs between active and standby.

  Workaround: There is no workaround.

- CSCso77116

  Symptoms: End to end connectivity is broken when pseudowire is configured on a port-channel interface or sub-interface and the member links are on LAN ports

  Conditions: xconnect has to be configured on the port-channel interface or sub-interface.

  Workaround: There is no workaround.

- CSCso80159

  Symptoms: IP Subscriber session ingress traffic is routed into incorrect VRF.

  Conditions: Occurs when the first access interface is up on a non-default VRF.

  Workaround: There is no workaround.

- 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 12.2SXF or Cisco IOS Release 12.2SXH.

  Workaround: Disable Netflow. This is done with the following commands: no ip flow ingress no ip flow engress no ip route-cache flow Enter the appropriate command for each sub-interface for which NetFlow is currently configured.

- CSCso89464

  Symptoms: Command is rejected with the following error message

  ```
  " interface range invalid, max 1000 interfaces allowed - command rejected".
  ```

  Conditions: Occurs during the following sequence:

  Router (config)# interface range create vlan 100

  interface range invalid, max 1000 interfaces allowed - command rejected

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsq07541

  Symptoms: Split horizon is not getting populated on standby member of the port channel.

  Conditions: Occurs when bridge domain with split horizon is configured and there is a standby member interface of the port channel.

  Workaround: There is no workaround.

- CSCsq18938

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

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

  Workaround: Disable health monitoring tests on the WS-6708

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

  ```
  May 6 13:32:09.915 EDT: %PIM-5-NBRCHG: neighbor 10.252.3.130 DOWN on interface
  Port-channel10 non DR
  May 6 13:32:09.307 EDT: %CONST_DIAG-SP-6-HM_TEST_SP_INFO: TestFabricCh0Health[3]:
  last_busy_percent[8%], Tx_Rate[894], Rx_Rate[2454]
  May 6 13:32:09.307 EDT: %CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 3 for software
  recovery, Reason: Failed TestFabricCh0Health
  May 6 13:32:09.307 EDT: %OIR-SP-3-PWRCYCLE: Card in module 3, is being power-cycled
  off (Diagnostic Failure)
  ```

- CSCsq19159

  Symptoms: System crash or memory corruption occurs.

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

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SRC

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRC. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- 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.

- CSCsl59184

  Symptoms: Some VTYs remain stuck on incoming telnet access. When the problem occurs, the banner is displayed but no login prompt. Tacacs logs seem to be normal.

  Conditions: This symptom occurs on a Cisco 7613 router that is running Cisco IOS Release 12.2(33)SRA5.

  Workaround: There is no workaround. Customer has to switchover the supervisor manually when the problem occurs.

- CSCsl61164

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

  Conditions: This symptom occurs when netflow is running fully with data export going on. User manually changes a cache timeout with the **ip flow-cache timeout inactive** *N* command.

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

IP Routing Protocols

- CSCsl30069

  Symptoms: A Cisco Catalyst 6500/7600 might crash due to memory corruption on the Route Processor (RP).

  Conditions: This symptom occurs when running Cisco IOS Release 12.2(33)SRB2 and when BGP is configured on the box.

  Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- 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.

- CSCsl83415

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

```
Test10 :
a. clear ip bgp 10.0.101.46 ipv4 multicast out
b. clear ip bgp 10.0.101.47 ipv4 multicast out
Test 1:
c. show ip bgp ipv4 multicast nei 10.0.101.2
d. show ip bgp ipv4 multicast [<prefix>]
e. config t
```

  Crash does not happen for each of the following cases:

  1. if same CLI is cut-paste manually, there is no crash.

  2. if **clear cli** is not executed, there is no crash.

  2. if **config term** is not entered, there is no crash.

  Conditions: The symptom occurs after executing the above CLI.

  Workaround: There is no workaround.

Miscellaneous

- CSCej33698

  Symptoms: A router that is running Cisco IOS software may mistakenly fail a CRC check on files in NVRAM.

  Conditions: This symptom has been observed with large files, such as large startup configurations.

  Workaround: There is no workaround.

- CSCsi30175

  Symptoms: “Success” is sent by router instead of “Error Code 404 (Invalid Request)”.

  Conditions: This symptom is seen when LI intercept-Identifier is >8 octets and encryption is used on Cisco 7200 platform.

  Workaround: Do not use encryption.

- CSCsi88974

  Symptoms: While configuring MD, if the MediationSrcInterface is set to loopback interface, then on sending traffic, MALLOC failures are seen.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: There is no workaround.

- CSCsk04724

  Symptoms: High line card CPU utilization and low session bring up rates on SIP400.

  Conditions: This symptom occurs when the HQoS configuration is applied on sessions in egress direction at time of session bring up.

Workaround: The session bring up rate improves if sessions are spread across multiple ports on the SIP400. However, the line card CPU utilization will remain high.

- CSCsk41134

  Symptoms: ISAKMP SA negotiation will fail for RSA signature w/cef switching and in tunnel mode.

  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.

- CSCsk99465

  Symptoms: A Cisco 7600series router that is configured with MPB in a SSO HA configuration may display a message as follows:

  ```
  %ISSU-3-NOT_FIND_MSG_SES: Cannot find message session(0) to get msg mtu
  ```

  Conditions: This behavior exists for MPB in Cisco IOS Release 12.2SR since Release 12.2SRC. The problem is seen when the Standby Supervisor and the line card on which MPB is configured get reset. After this, if the line card comes back online before the ISSU negotiation between the Active Supervisor and the Standby Supervisor is completed, this error message will be seen.

  Workaround: The workaround is to avoid a double-fault situation which the Standby supervisor and the line card get reset at the same time.

- CSCsl10412

  Symptoms: A router CPU hits 100% when SPA-OCx3-ATM is reset.

  Conditions: This symptom is observed on a Cisco 7600 router with Cisco IOS Release 12.2(33)SRB1. It has an ATM interface with approximately 400 VCs. If the main interface is reset, the CPU hits 100%. When the CPU process is queried, SNMP is holding the CPU cycle.

  ```
  Router: C7600
  IOS: 12.2(33)SRB1
  SIP-400
  2xOC3 ATM SPA
  ```

  Customer ATM interface has approximately 400 VCs. A reset hits the CPU at 100%, and SNMP process holds the cycle.

  Workaround: Disable bgp traps.

- 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.

- CSCsl22117

  Symptoms: A Cisco 1000BaseT gigabit interface goes down/down (not connect) unexpectedly. No errors nor logs were observed, a part to the usual sequence of %LINEPROTO-5-UPDOWN:, %LINK-3-UPDOWN:, %LINEPROTO-SP-5-UPDOWN:, %LINK-SP-3- UPDOWN: (if the **logging events link-status** command is enabled on the interface).

  Conditions: This symptom is observed on multiple Cisco 7613 routers that are running Cisco IOS Release 12.2(33)SRB2 and equipped with WS-X6724-SFP + DFC + GLC-T (1000BaseT adapters). All affected interfaces are directly connected to Unix servers.

  Workaround:

  - OIR (unplug and plug back) the GLC-T adapter is currently the only workaround while running Cisco IOS Release 12.2(33)SRB2.
  - These symptoms were never observed with Cisco IOS Release 12.2(33)SRA3, so downgrading may be another workaround, if applicable

- CSCsl28931

  Symptoms: On a Cisco 7600 router that is 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 OIR, resulting in the traffic being flooded for those MAC entries.

  Conditions: See the following conditions:

  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 line card (which has a distributed forwarding engine) and is forwarded to a core facing line card 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. Line card OIR (removal/reinsertion) happens.

  Workaround: Clear mac address-table dynamic entries.

- CSCsl33956

  Symptoms: MLFR interfaces might flap when the T3 controller is shut.

  Conditions: The problem might occur under the following conditions:

  1. On a Cisco 7200 router having member links spread across two controllers on the same PA-MC-T3-EC Port adapter.
  2. When we do shut and no shut of one controller.
  3. Occurs only under scaled configuration of more than 40 MFR interfaces.

  Workaround: Configure a higher number LMI retries on the MFR interface using the following commands. Examples:

  interface MFR0 (on the DTE side) frame-relay lmi-n392dte 3

  or

  interface MFRO (on the DCE side) frame-relay lmi-n392dce 3

- CSCsl37041

  Symptoms: Not able to configure channel-group after RPR+ switchover.

  Conditions: After RPR+ switchover, if the channel-group is deleted and then try to configure it immediately again, the channel creation fails.

Workaround: Wait for few seconds after deletion of channel-group (after RPR+ switchover) and then create it again.

- 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.

  Workaround: Issue is not seen when running Cisco IOS Release 12.2(33)SRA5.

- CSCsl43546

  Symptoms: On the Cisco 7600 platform a reset of a line card may cause all MPLS over GRE adjacencies on the interfaces using that line card to be lost. Traffic will no longer be forwarded.

  Conditions: This problem can be caused on a Cisco 7600 by issuing the **hw-module** *module-number* **reset** command.

  Workaround: Reconfigure the interface to be admin down and then up. int *interface name* shutdown/no shutdown.

- 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, which causes a standby reset in case there is a large number of tunnels configured.

  Conditions: This symptom occurs when tunnels are configured.

  Workaround: Remove tunnels configs before doing ISSU.

- 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.

  Workaround: To recover connectivity, issue the **hw-module module** *mod* **reset** command.

- CSCsl51914

  Symptoms: On Cisco 7600/SIP400 supporting MLP interfaces, “priority percent” does not work.

  Conditions: The conditional police rate values will not get updated:

  a) when ever there is a member link addition or deletion happens from the bundle

  b) when all the members of the multilink is down and come back

  c) SPA / LC OIR

  Workaround: Use priority and with absolute-value (explicit) policer.

  Further Problem Description: The SIP-400 has a different HQF mechanism which does not use the Cisco IOS HQF structures. These structures are supposed to be updated when there is a request from the hqf common code. HQF common code is looking for some variables which are not set at the SIP-400 structure level. Hence the updates are not received by the SIP-400, by which this problem is being caused.

- CSCsl51945

  Symptoms: The HSRP IPv6 config on the standby RP may loose its address, such that the config on the standby RP appears as:

standby 1 ipv6 ::

The standby resets as well.

Conditions: This will occur if group is in init state while doing the configuration or changes its state to init after applying the configuration. If you reapply the command on the active RP without first removing it, then a config sync error will occur and the standby RP will reload.

Trigger: Standby RP on switchover stuck in standby-cold state.

Impact: Secondary RP resets, configuration sync failure.

Workaround: There is no workaround.

- CSCsl57023

  Symptoms: After switchover happens on Cisco 7600 and new Active is reset, PVC recreation fails.

  Conditions: This switchover happens on Cisco 7600 from Active to Standby.

  Workaround: There is no workaround.

  Further Problem Description: Sounds like VC is locked.

  ```
  76b(config-if)#int ATM9/1/0
  76b(config-if)#pvc 12/100
  %ATM: Exceeded the VC limit. Max VCs allowed is 8191
  76b(config-if)#
  *Dec 3 10:52:18.543: %ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=0, VPI=0, VCI=0) on Interface ATM9/1/0, (Cause of the failure: ATM interface temporarily unavailable)
  -Traceback= 4069D894 4069DDD8 4021864C 4023ABC0 40625030 4229DC5C 40650128 4176D2A4 4176D290
  ```

- CSCsl58941

  Symptoms: The VPN SPA on a Cisco 7600 series router stops decrypting traffic for all the tunnels suddenly. All tunnels are up, but from the **show crypto session** command, the packets decrypted counter is not increasing. Encrypted counters are increasing. BGP and PIM traffic is affected.

  Conditions: This symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRB2. This has not occurred with Cisco IOS Release 12.2(33)SRA3.

  Workaround: Reload the SPA module.

- CSCsl60168

  Symptoms: System unexpected reloads due to memory corruption in the IO memory pool. This occurs 7 minutes after the switch has been commanded to reload.

  ```
  %SYS-3-OVERRUN: Block overrun
  %SYS-6-BLKINFO: Corrupted redzone blk
  ```

  Conditions: This symptom occurs in normal operation.

  Workaround: There is no workaround.

- CSCsl61806

  Symptoms: All BW queues will be having en eir of 10g odd and maxrate of 0. LC throws the message “Exceed eir” as the sum of all queue eir is exceeding 540G.

  Conditions: It will affect an environment which has a large config with 1000 EVCs under a port channel. When shape rate is changed dynamically on the cass default and make a shut/ no shut on the port channel eir is going out of bound and maxrate is going zero. It is not consistent.

  Workaround: An LC reload in problem condition will recover the condition.

- CSCsl62851

  Symptoms: The router experiences XDRDISABLE condition and prints the following two messages:

  ```
  %XDR-6-XDRDISABLEREQUEST: Peer in slot 9/1 (23) requested to be disabled due
   to: XDR Keepalive Timeout. Disabling linecard
   %FIB-2-FIBDISABLE: Fatal error, slot 9/1 (23): XDR disabled
  ```

  Conditions: This symptom happens when there are a lot of IPC failures in the RP => LC path, but there is no specific trigger. Primary causes of this failure could be:

  1. There is a lot of control traffic between RP and LC.
  2. IPC failures/error conditions which in turn could have led to application (XDR) level failure.

  Workaround: Do an OIR of LC.

- CSCsl63272

  Symptoms: Traffic does not go through some of the HW Ethernet over MPLS (EoMPLS) VCs in port mode.

  Conditions: The symptom is not known yet.

  Workaround: Remove the Xconnect from the configuration and add it again.

  Further Problem Description: There are two TCAM entries for the same VC. The first one is associated with a wrong adjacency. The second one is associated with correct adjacency. Since the first one is used the traffic loss is observed.

- CSCsl65179

  Symptoms: Setting priority queue limit for PFC QoS configurations resets non-priority queue limits to default values.

  Conditions: Changing the priority queue limit to default setting will reset non-priority queue limits to default values. If CoS values are mapped to queues with default queue limits of 0 then traffic with these CoS values will be dropped until non-default configuration is reapplied.

  Workaround: After changing priority queue limit reapply non default non-priority queue limits.

- CSCsl67938

  Symptoms: Memory leak in “XDR LC Background” process is observed on SP.

  Conditions: This symptom is observed on a Cisco 7606 router that is running Cisco IOS Release 12.2(33)SRB2. This is also seen on Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround.

- CSCsl68034

  Symptoms: Traffic might fail on dMLP bundles when the SPA OIR is done.

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

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

- 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.

- CSCsl72073

  Symptoms: Virtual-access keeps flapping on a Cisco 7200 series router under traffic.

  Conditions: This symptom occurs when LFIoFR (LFI over Frame Relay) is configured on a Cisco 7200 series router. The flapping occurs only when there is data traffic on the link at line rate and QoS is active.

  Workaround: Define a class to match keep-alive packets using the **match not protocol ip** command. No flaps are seen with this configuration.

- CSCsl72281

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

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

  Workaround: There is no workaround.

- CSCsl72636

  Symptoms: A Cisco router may experience traffic drop on frame-relay point-to- point subinterfaces during a SSO/NSF failover. This only occurs when a large number of frame-relay point-to-point interfaces are used.

  Conditions: This symptom is observed on a Cisco router that is running either Cisco IOS Release 12.2(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.

- CSCsl72677

  Symptoms: SNMP counters produce inconsistent results on WS-X6724-SFP when subinterfaces are configured and polled.

  Conditions: This symptom occurs when using the following SNMP OID:

  `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.`

  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

- CSCsl74289

  Symptoms: An IPsec tunnel between a Cisco 7600 router and a Cisco 2811 router works without NAT box in the middle. When the NAT box is present, the tunnel does not come up stopping at Phase 2.

  Conditions: This symptom occurs in the NAT-T in an IPSec and VRF scenario.

  Workaround: There is no workaround.

- CSCsl76647

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

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

  Workaround: There is no workaround.

- CSCsl76939

  Symptoms: After shut/no shut and SSO, some IMA groups may not pass traffic.

  Conditions: With 2k ATOM MPLS VCs configured on 42 IMA groups, if we perform the (shut/no shut + switchover), then some of the MPLS VC circuits are not passing the traffic. This is not real test scenario, which customer will be performing in real time scenario.

  Workaround: If we perform the SIP module OIR or SPA OIR, then all the MPLS circuits will come UP and traffic will pass at line rate.

- CSCsl77920

  Symptoms: IP addresses are not assigned from the desired DHCP pool.

  Conditions: This happens when the DHCP class-name is downloaded via the Per-User Profile.

  Workaround: If the solution requires the DHCP class-name download, then do it via the Service-Profile and download the service.

- CSCsl80385

  Symptoms: While reconfiguring an EVC under port channel after a sequence of steps, the following error message might be seen:

  ```
  %GENERAL-DFC3-2-CRITEVENT: ETHER EFP CLIENT: Could not add qinq
  ```

  Conditions: This occurs (not consistently) when following steps are being done:

  1. Boot up the router with a port-channel and 1000 xconnect EVCs.
  2. Unconfigure one of the service instance and add the config to a physical interface.
  3. Unconfigure the same service instance in step 2 and reconfigure it back under the same port-channel as before.

  Workaround: There is no workaround.

  Further Problem Description: When this error is seen the service instance will stop passing traffic in ingress direction.

- CSCsl80722

  Symptoms: L2 protocols are not tunneled with Cisco Route Switch Processor 720 (RSP720).

  Conditions: This symptom occurs with RSP720.

  Workaround: Use SUP720-3BXL instead.

- CSCsl80899

  Symptoms: Rare crash occurs when a peer 7600 router is reloaded.

  Conditions: This symptom is seen when a Peer 7600 router is reloaded in a back to back Cisco 7600 topology with thousands of locally terminated subscriber sessions.

  Workaround: There is no workaround.

- 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.

- CSCsl85297

  Symptoms: Supervisor 720 keeps reloading after loading as SSO standby mode, with Cisco IOS Release 12.2(33)SRB2.

  Conditions: The problem occurs with configuration sync:

  ```
  %SCHED-3-SEMLOCKED: rf proxy rp agent attempted to lock a semaphore, already
  locked by itself -Traceback
  %IP_DEVICE_TRACKING-4-TABLE_LOCK_FAILED: Table already locked by process-id xx
  (rf proxy rp agent)
  Config Sync: Bulk-sync failure due to PRC mismatch. Please check the full list
  of PRC failures via: show redundancy config-sync failures prc

  Config Sync: Starting lines from PRC file:
  interface xxx
   ! <submode> "interface"
  - ip route-cache same-interface
   ! </submode> "interface"
  ```

  Workaround: There is no workaround.

- CSCsl86316

  Symptoms: VPN subsystem: Excessive CPU utilization/Tracebacks in VTEMPLATE Backgr results in the rtr becoming unstable.

  Conditions: L2TP scenario.

  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. There is no known impact because of this message.

  Conditions: This message can be seen if port-channel configuration exists on the Cisco 7600.

  Workaround: There is no workaround.

- CSCsl87445

  Symptoms: Traceback is generated by DHCP process:

  ```
  %DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR
  ```

  and finally crashes:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header
  ```

  Conditions: With DHCP relaying and snooping working, and receiving DHCP packets with Option 82 inserted, the switch will cause several DHCP tracebacks and finally crashes due to memory errors. This is seen in Cisco IOS Release 12.2(33)SRB2 but not in the Cisco IOS Release 12.2SXF train.

  Workaround: There is no workaround.

- CSCsl88651

  Symptoms: SP crashes the router on reload of an adjacent core router.

  Conditions: In a typical mVPN scenario with Edge (PE) and Core (P) routers, with Bi-Dir in the core and PIM-SM on the mvrf. It is observed that on reloading one of the core routers, the edge router i.e. the PE router crashes. The crash if observed when the core router is trying to come up after reload. The scenario in which this issue is discovered is mVPN+L3VPN on the PE router. I have 100mVPNs and 500 L3VPNs.

  Workaround: There is no workaround. Issuing the **reload** command on core router creates the problem. This is specific to Cisco IOS Release12.2SRC.

- CSCsl88658

  Symptoms: A Cisco 7600 router that is having a large scaled configuration (eg, 20k+ VPLS VCs + 4k+ Scalable EoMPLS), configured in SSO Redundant mode and without LDP targeted session Graceful Restart, after an SSO Supervisor redundant failure, may experience a series of messages %L2-SP-4-NOMEM: Malloc failed: L2-API purge all earl entries failed 0 and some MAC Entries in the L2 MAC Table are not purged, resulting in the corresponding entries in the MAC Address table not being flushed. Under normal circumstances of bidirectional conversation, the new packets will repopulate the MAC tables and no external visible effect is observed. If the conversation is not bidirectional, the traffic ma y be interrupted until the entry ages out, and the traffic should resume as normal.

  Workaround: This problem may not cause any impact in most of the cases. If desired, one workaround is to reduce the aging timer for the dynamic mac address entry or clear the mac address table for the corresponding VPLS VLANS after an SSO switchover (which will happen automatically if there is no traffic sourced by the corresponding MAC address).

- CSCsl88708

  Symptoms: Flapping MPLS IP while there is VPN traffic through, or flapping MPLS IP after SSO or sending MPLS traffic with EoS bit =0 causes the router to crash.

  Conditions: The problem has been seen on s72033-adventerprisek9-mz.122-32.8.11.SRC3 and s72033-adventerprisek9-mz.nightly.src_throttle_121507 images.

  Workaround: There is no workaround.

- CSCsl88931

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

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

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

  Workaround: There is no workaround.

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

- CSCsl91046

  Symptoms: Traffic coming into GigabitEthernet interface on OSM card is dropped on the LC.

  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.

  Workaround: Shut / no shut of the interface resolves the issue.

  Further Problem Description: Issue has not been seen consistently. Issue is seen with SRC image.

- CSCsl92632

  Symptoms: On ATM interface on Flexwan after removing service-policy and shut/no shut cause ALIGN-3-SPURIOUS and then OIR the LC cause RP crash.

  Conditions: This symptom occurs when ATM interface with multilink PPP resets after shut/no shut.

  Workaround: There is no workaround.

- CSCsl94621

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

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

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

- CSCsl94829

  Symptoms: There was ESM20 line card crash observed during bootup of SRC6 image.

  Conditions: During router reload this problem was reported once so far.

  Workaround: The line card comes up fine after recovery.

- CSCsl96417

  Symptoms: Result is router crash.

  Conditions: This symptom occurs on ISSU upgrade with ATM ACs (configured with xconnect), the router crashes on running the **issu runversio**n command.

  Trigger: During the router upgrade with ATM ACs (configured with xconnect), configuration from rsp72043-adventerprisek9-mz.122-33.SRB2 to rsp72043-adventerprisek9-mz.122-32.8.11.SRC6 and in the **issu runversion**.

  Impact: Router crashes.

  Workaround: There is no workaround.

- CSCsl97835

  Symptoms: In a system with scaled configuration, with a operational rep segment, when a rep port role is configured as non-edge and then swapped to edge, the standby supervisor can crash.

  Workaround: The port where the rep config is being changed (to rep edge or non-edge role) should be shut down first before making these changes, make the required changes and then unshut the port. This would prevent the standby from crashing.

- CSCsm04643

  Symptoms: PPPoA Client unable to obtain IPv6 Auto config address.

Conditions: This is observed on Cisco 7200 routers that are loaded with Cisco IOS 12.2 Release SRC images configured for PPPoA with PAP enabled.

Workaround: There is no workaround

Wide-Area Networking

- CSCsk15296

  Symptoms: When more than one dLFIoATM bundle is configured between 2 routers on an ATM SPA the ping fails across all the bundles except the first one.

  Conditions: This happens only if I have the same VPI and multiple VCIs.

  That is, in the below output, I have associated every ATM subint to a diff virtual-template. The ping goes through across 4/1/0.1 and 4/1/0.5 (which have same VC and diff VP) but does not go through 4/1/0.2,3 and 4 (with same VP as 4/1/0.1 but diff VC)

```
76A#sh atm pvc
VCD /                                              Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
2/0/0.1    1              1   101 PVC     SNAP       UBR  599040              UP
2/0/0.2    2              1   102 PVC     SNAP       UBR  599040              UP
2/0/0.3    3              1   103 PVC     SNAP       UBR  599040              UP
2/0/0.4    4              1   104 PVC     SNAP       UBR  599040              UP
2/0/0.5    5              2   102 PVC     SNAP       UBR  599040              UP
76A#
```

  Workaround: Configure the virtual-template first and the ATM PVC next.

- CSCsk30718

  Symptoms: The memory of LAC and LNS exceeds the set target when PPPoE sessions are initiated.

  Conditions: This issue is seen when PPPoE sessions are initiated.

  Workaround: There is no workaround.

- CSCsl47374

  Symptoms: When CPS values for autobahn76 with LAC as Cisco 7200 G2 Ix Access as LNS and LNS as Cisco 7200 G2 Ix Access as LAC are low when compared with CPS results from Images SB4, XN3 and XD9.

  Conditions:

  1. Cisco 7200 G2 as LAC using autobahn76 image and Ix Access as LNS.
  2. Cisco 7200 G2 as LNS using autobahn76 image and Ix Access as LAC. This only happens when there are multiple tunnels/vpdn-groups on the LAC with the same local name going to the same vpdn-group on the LNS.

  Workaround: There is no workaround.

  Further Problem Description: When CPS Result for Autobahn76 was compared with CPS results from Images SB4,XN3 and XD9.it indicates a degradation on AB76.

  CPS was Calculated with Standalone LNS and LAC using Ix Access.

  For Image c7200p-advipservicesk9-mz.autobahn76_102207 results are give below:

```
7200 G2 as LAC and Ix Access as LNS.
```

```
 4k pppoe sessions/4k L2tp Tunnels-----111.11 CPS   99 % CPU utilisation of LAC
was observed
 8k pppoe sessions/8k L2TP tunnels-----69.57  CPS   99 % CPU utilisation of LAC
was observed

 Standalone LNS and Ix Access as LAC.

 4k pppoe sessions/4k L2tp Tunnels-----108.11 CPS
 8k pppoe sessions/8k L2TP tunnels-----117.65 CPS
```

This is an uncommon configuration. Normally when one needs to have multiple tunnels from the LAC to the same LNS, one configured multiple vpdn-groups on the LAC with different local-names and for each of these a corresponding vpdn-group is created on the LNS with the corresponding terminate-from name.

- 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.

Resolved Caveats—Cisco IOS Release 12.2(33)SRC

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRC. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCdv48842

  Multiple Cisco products contain vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. The vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact. These vulnerabilities are identified by various groups as VU#617947, VU#107186, OUSPG #0100, CAN-2002-0012, and CAN-2002-0013.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml

- CSCed73481

  Symptoms: When “sh ip cache ver flow” on the router, it fails to display the AS numbers for each flow. This does not affect traffic forwarding.

  Conditions: This symptom occurs during normal use.

  Workaround: There is no workaround.

- CSCed93927

  Symptoms: The “%RADIUS-3-NOSERVERS: No Radius hosts configured” error message appears after the receipt of a RADIUS Access-Accept packet, preventing accounting updates from being sent.

Conditions: This symptom is observed on a router with a very specific RADIUS server host configuration after you have reloaded the router.

Workaround: Perform the following steps:

1. Remove specific RADIUS commands by entering the following:

no radius-server host 10.0.0.1 auth-port 1645 acct-port 0 non-standard key 7

no radius-server host 10.0.0.1 auth-port 0 acct-port 1646 non-standard key 7

2. Remove all server group configurations by entering the following commands:

no aaa group server radius ACS

no aaa group server radius RAD

3. Reinstall the server group configurations by entering the following commands:

aaa group server radius ACS server 10.0.0.1 auth-port 1645 acct-port 1646 deadtime 10 ! aaa group server radius RAD server 10.0.0.2 auth-port 1645 acct-port 1646 deadtime 10

- CSCef64439

  Symptoms: A PRE requires a long time to enter the STANDBY HOT state after a switchover.

  Conditions: This symptom is observed on a Cisco 10000 series when two PREs are forced to switchover back and forth.

  Workaround: Enter the **snmp-server ifindex persist** command.

- CSCef78565

  Symptoms: Port-ID TLV advertised by the current CDP implementation (which corresponds to cdpCacheDevicePort in CISCO-CDP-MIB and identifies the port CDP packet is sent on) does not always consistently correspond to the value of ifName object across various interface types.

  Conditions: The issue is observed for different interface types, including POS, Port-channel, FastEthernet subinterfaces.

  Workaround: There is no workaround.

- CSCeh64791

  Symptoms: A memory leak may occur when you delete a RADIUS server group.

  Conditions: This symptom is observed when the server is configured with a key.

  Workaround: There is no workaround.

- CSCej57779

  Symptoms: A reload of a Cisco 7600 router, with a huge number (for example, 1000) of VRF configured with BGP/VPN learning redistributed routers, may cause some VRFs to not learn distributed routes from the peer.

  Conditions: This symptom has been observed in Cisco IOS Release 12.2SRA when a huge number of VRF are configured. This symptom is not applicable to Cisco IOS Release 12.4.

  Workaround: The symptom can be resolved on the per VRF basis by removing the VRF instance and the BGP/VPN configuration for this instance and then adding them back.

- CSCek32177

  Symptoms: A TACACS+ AV address that is defined as “255.255.255.254” may not be processed correctly.

  Conditions: The symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(5.8)T or a later release but may not be release-specific.

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur when RADIUS is configured.

- CSCek39431

  Symptoms: On a Cisco 7500 platform, a Cisco IOS Image can not be loaded from an ATA Flash disk if it is formatted with Cisco IOS Release 12.2(31.04.04)SRB or Release 12.2(32.08.01)SR.

  Conditions: This symptom occurs when formatting the ATA disk with Cisco IOS Release 12.2(31.04.04)SRB or Release 12.2(32.08.01)SR.

  Workaround: Format the disk with an older Cisco IOS version.

- CSCek58840

  Symptoms: When a new PPP session is set up, the following warning message is generated, and the session fails:

  ```
  LAC: %IDMNGR-3-ALLOCFAIL: Warning: Failed to allocate memory for keylist in event_init
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB1. The PPP sessions start failing after the router has been up for about two weeks with many policy-map changes on the PVCs, a few cleared sessions by the clients, and one switchover. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek63810

  Symptoms: A Cisco 10000 series may run out of memory after a number of ATM port flaps have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 28,000 PPPoA Point-to-Point Termination and Aggregation (PTA) sessions. Each time that the ATM ports that carry the sessions flap and in this process remain down long enough for the sessions to time-out, more memory is lost. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek69519

  Symptoms: When the execution of the **show aaa user all** command waits at the “More” prompt and when you cancel the command, the console is locked up for up to one minute and the CPU usage increases to near 100 percent during this time.

  Conditions: This symptom is observed on a Cisco router that is configured with many broadband sessions.

  Workaround: There is no workaround.

- CSCek78644

  Symptoms: SNMP does not use the source address in a VRF.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4 or Release 12.4T. However, the symptom may also affect other releases.

  Workaround: Ensure that an SNMP interface is not defined in a VRF.

- CSCir01027

  Symptoms: SNMP over IPv6 does not function.

Conditions: This symptom is observed on a Cisco router that integrates the fix for caveat CSCsg02387. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg02387. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

Workaround: Use SNMP over IPv4.

- CSCsa40461

  Symptoms: A Cisco router that is running Cisco IOS Release 12.3(7)T or later releases and configured to use the VRF-aware TACACS+ feature will be unable to perform TACACS+ authentication for enable authentications if the TACACS+ server lies within a VRF.

  Workaround: Use a TACACS+ server that is reachable via the global routing table.

- CSCsc99912

  Symptoms: The MPLS forwarding table entry contains no CE information.

  Conditions: This symptom occurs when two PEs are connected without any P routers, the MPLS routing information are not propagated to the PE on each end.

  Workaround: There is no workaround.

- CSCsd70700

  Symptoms: A traceback is generated on the standby RP after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7500 series that has an ATA disk installed in any of the PCMCIA slots.

  Workaround: There is no workaround.

- CSCse85200

  Symptoms: Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Conditions: Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary.

- CSCsf12539

  Symptoms: Tracebacks may be generated for all accounting messages.

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

  Workaround: There is no workaround.

- CSCsf98394

  Symptoms: When the **initiator radius-proxy** command is enabled on an ISG, extra characters are shown with the identifier in the output of **show sss session** and **show radius-proxy client session** commands.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the user name has at least 8 characters.

  Workaround: Use a user name with less than 8 characters.

- CSCsg24971

  Symptoms: A memory leak may occur on a line card, eventually causing IPC to fail.

Conditions: This symptoms is observed on a Cisco platform that is configured for NetFlow. The symptom affects distributed platforms only.

Workaround: There is no workaround.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCsh19482

  Symptoms: A Cisco 10000 series may crash and generate a "%C10K-2-RPRTIMEOUT_CRASH:" error message.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for NetFlow.

  Workaround: There is no workaround.

- CSCsh76038

  Symptoms: AAA enable authentication via a TACACS+ server fails.

  Conditions: This symptom occurs when the **aaa authentication enable default group tacacs+** command or the **aaa authentication enable default group** command pointing towards a TACACS+ server group is configured.

  Workaround: There are two possible workarounds.

  1. On the TACACS+ server, configure a user named "$enab{x}$", where {x} is the desired privilege level, such as using "$enab15$" for regular enable mode. This user's password will be the enable password.
  2. Change to a Cisco IOS release that does not yet include CSCin98780.

  Further Problem Description: When using a RADIUS server, enable authentication is done by authenticating a user named "$enab{x}$". When using a TACACS+ server, enable authentication is done by using the user's actual username, which allows TACACS+ to define separate enable passwords for each user.

  CSCin98780 erroneously caused the Cisco IOS software to authenticate "$enab{x} $" as a username for enable authentication for TACACS+ servers. This causes enable authentications in existing installations to fail, since TACACS+ server user databases do not normally contain a "$enab{x}$" user. This fix, CSCsh76038, corrects the issue, and any Cisco IOS release with this fix will transmit the user's actual username again in any enable authentication request.

- CSCsi04892

  Symptoms: When you enter the **no ip sla schedule** *operation-number* command, error messages may be generated.

  Conditions: This symptom is observed on a Cisco router when you unconfigure an Ethernet SLA feature.

  Workaround: There is no workaround.

- CSCsi13207

  Symptoms: The output of the **show ip cache flow** command for NetFlow on an LNS shows the physical ingress interface as the source interface for packet flows instead of the virtual-access interface.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(28)SB3 and that functions as an LNS when the following configuration is present:

  – The physical ingress interface that faces the LAC is "fas0/0" and has the **ip flow ingress** command enabled.

  – The **flow-sampler one-in-hundred** command is enabled on the virtual-template interface.

  Workaround: Do not enter the **ip flow ingress** command on the physical ingress interface. Rather, enter the **ip flow ingress** command on the virtual-template interface, bring down the tunnel, and then bring up the tunnel.

- CSCsi28884

  Symptoms: The attribute list may not be downloaded for a particular service.

  Conditions: This symptom is observed on a Cisco platform that is configured for AAA when local authorization is configured and when the attribute list is downloaded. The following shows a configuration in which the symptom occurs:

```
policy-map type service abcd
 aaa attribute list cisco
 service local

aaa attribute list cisco
 attribute type addr-pool "cisco" protocol ip
 attribute type ppp-author-list "cisco"
 attribute type ppp-authen-list "cisco"
```

  Workaround: Ensure that the same name is used for the *policy-map-name* argument of the **policy-map type service** *policy-map-name* command (abcd in the example above) and the *list-name* argument of the **aaa attribute list** *list-name* command (Cisco in the example above).

- CSCsi48665

  Symptoms: When you configure SNMPv3 group access to contexts, each context may need to be configured with a separate CLI command. For large configurations, thousands of CLI command may need to be entered, which is not acceptable.

  Conditions: This symptom is observed, for example, when the **snmp-server group** *groupame* **v3 auth context** *context-name* command must be entered for each group and each context. If there are many VLANs, the command must be entered for each group that is given access to each VLAN, which may mean that thousands of CLI command must be entered.

  Workaround: SNMP allows you to specify that a context name is a prefix, and match any context that starts with that name. Use SNMP to create rows in the vacmAccessTable and ensure that the vacmAccessContextMatch object is set to a prefix instead of match. Note that after you reboot the router, you must reconfigure this workaround.

- CSCsi80159

  Symptoms: A Cisco router that functions as an ISG may not send RADIUS attribute 44 in the RADIUS Access Request when the **vrf default** keywords are present in the command line, as in the following example:

```
radius-server attribute 44 include-in-access-req vrf default
```

This situation affects the prepaid billing service for ISG-based customers because the billing system cannot re-authorize a subscriber after its quota runs out. The billing system is not able to consolidate the AAA accounting sessions without RADIUS attribute 44 in the RADIUS Access Request for re-authorization. Even if the ISG prepaid threshold is zero, re-authorization fails because the service quota is exhausted, but subscriber's session remains active.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or one of its rebuilds because in these releases the **vrf default** keywords are added by default.

Workaround: There is no workaround.

- CSCsj16007

  Symptoms: A PDSN member reloads at find_elt.

  Conditions: This symptom is observed on a PDSN using Cisco IOS Release 12.3 (14)YX8.

  Workaround: There is no workaround.

- CSCsj55691

  Symptoms: There is a crash on the router.

  Conditions: For the problem to occur, there needs to multiple https requests sent in quick succession to an HTTPS server that is up and running, but the service or application processing the request should be unavailable.

  Workaround: There is no workaround.

  Further Problem Description: The crash will not occur if the HTTPS server and the service handling the request are operating normally.

- CSCsj83966

  Symptoms: The message CPU HOG will appear in the screen

  Conditions: When a lot of interfaces are coming up/down at the same time, the syslog use to process 100 trap at one time which causes CPU HOG.

  WorkAround: The condition will not appear if there are comparatively less number of interfaces. Also, unconfigure the trap from sh run will prevent from this issue

- CSCsj89470

  Symptoms: An LNS that has sampled NetFlow enabled may crash.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as an LNS.

  Workaround: Disable sampled NetFlow. If this is not an option, there is no workaround.

Interfaces and Bridging

- CSCef80036

  Symptoms: Issuing a microcode reload causes %IPC-5-INVALID message with tracebacks to appear on the router console.

  Conditions: This symptom occurs on a Cisco 7500 (RSP4) series router that is loaded with Cisco IOS Release 12.2(25)S1.

  Workaround: There is no workaround.

- CSCeg55131

  Symptoms: Spurious memory access occurs when removing channel groups in the T1/E1 cards.

Conditions: This symptom has been observed with a PA-MC-8TE1+ port adapter on a Cisco 7500 router that is running Cisco IOS Release 12.0S.

Workaround: There is no workaround.

- CSCeh17935

  Symptoms: When you perform an Online Insertion and Removal (OIR) of an ATM port adapter, tracebacks are generated.

  Conditions: This symptom is observed on a Cisco 7200 series when the ATM port adapter is up and has a VC configured, when traffic passes through the ATM interface of the port adapter during the OIR, and when the ATM interface of the port adapter is oversubscribed.

  Workaround: There is no workaround.

- CSCek65222

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

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

  Workaround: There is no workaround.

- CSCek76288

  Symptoms: With MLPoATM configured, a router crashes when using the **show ppp multilink** command after disabling the PA by the **hw-module slot** *slot- number* **stop** command.

  Conditions: This symptom has been observed on a Cisco 7200 NPE-G1 loaded with Cisco IOS interim Release 12.4(13.13)T2.

  Workaround: There is no workaround.

- CSCin46297

  Symptoms: In a High Availability routers set-up having Sonet controllers and configured for Multi-router APS, a SSO switchover will lead to inconsistent Sonet APS state.

  Conditions: The inconsistent APS state is seen only when we do a SSO switchover.

  Workaround: After the SSO switchover, a manual shut/no shut on the Sonet Controller is needed on the new Active Sup card, to restore the correct APS state.

- CSCsf20174

  Symptoms: An enhanced FlexWAN module may reload with certain traffic flows.

  Conditions: This symptom is observed rather rarely on a Cisco 7600 when the enhanced FlexWAN module is configured with an ATM port adapter, has 1483 configurations, and processes traffic.

  Workaround: There is no workaround.

- CSCsi41769

  Symptoms: A PVC that is shut down by OAM may continue to receive and forward traffic. This situation causes problems in an APS 1+1 redundancy configuration in which the standby router has a PVC that is shut down by OAM but continues to receive all traffic.

  Conditions: This symptom is observed on a Cisco router that has an ATM port adapter.

  Workaround: In an IPv4 configuration, shut down the subinterface manually or enter the **ip verify unicast reverse-path** command. In an MPLS configuration, shut down the subinterface manually.

- CSCsi56413

  Symptoms: The output may be stuck on a POS interface that is configured for Frame Relay encapsulation. When this situation occurs, the output queue is not emptied, and LMI remains down.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(12) or later. This happens only with very specific hardware configurations including NPE-G1 and PA-POS-OC3SMI. The issue observed when aforementioned Port Adapter is located at slot 4 and not seen with other hardware configurations.

  Workaround: Place POS PA in other slot(s). PA location reconfiguration in chassis should fix the problem.

- CSCsi66859

  Symptoms: A router crashes when both “xconnect” and “bridge-group” are configured on an interface and packets are received on that interface.

  Conditions: This symptom happens only when “xconnect” and “bridge-group” are configured on an interface, and packets are received on the interface.

  Workaround: Do not configure both “xconnect” and “bridge-group” on an interface. These commands are mutually exclusive in terms of functionality, so there is no deployment scenario in which they would be configured together.

- CSCsi85935

  Symptoms: Alignment errors drive the router to crash due to a bus error (TLB exception). These reloads can occur about 2-3 times day.

  Conditions: This symptom occurs on a Cisco 3745 with NM-8AM running Cisco IOS Release 12.3(7)T11 and Release 12.4(13a) while there is great volume of the traffic through module NM-8AM. Replacement of all the HW equipment did not solve the issue.

  Workaround: Reduce traffic through NM module or install Cisco IOS 12.3 (not T train or 12.4 image) provokes that reloads stop.

IP Routing Protocols

- CSCdy42103

  Symptoms: A watchdog timeout may cause a software-forced reload on a router.

  Conditions: This symptom is observed on a Cisco 7500 router that is using the Border Gateway Protocol (BGP).

  Workaround: There is no workaround.

- CSCec68752

  Symptoms: A router may crash when you enter a long string for the *name* argument in the **ip nat outside source route-map** *name* **pool** *pool-name* command.

  Conditions: This symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCed68668

  Symptoms: A Cisco router that runs Cisco IOS Release 12.3(5.13)T may reload because of a bus error. The output of the **show version** command may show the following:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY
  ```

  Conditions: These symptoms occur when **clear ip nat *** is executed on the CLI.

Workaround: Do not perform **clear ip nat ***.

The following link provides general information about bus errors: http://www.cisco.com/warp/public/122/crashes_buserror_troubleshooting.shtml

- CSCef24703

  Symptoms: OSPF may continue to originate a default route when using default-information originate route-map xxxx and watching a learned route via bgp to satisfy the route-map. Thus far, this problem has been seen in 12.2 through the most recent 12.3T code.

  Conditions: This problem is observed when the watched route is in the bgp table as an ibgp route, even if the preferred path is the ebgp path.

  Workarounds: Either filter the watched route between the ibgp routers so it isn't learned via ibgp, only ebgp, or use "bgp redistribute-internal" under router bgp instead.

- CSCef41448

  Symptoms: BGP update replication is not good.

  Conditions: This symptom is observed on Cisco IOS 12.2(25.04)S01.

  Workaround: There is no workaround.

- CSCef45830

  Symptoms: A stale BGP route does not time out, which can be observed in the output of the **show ip route vrf** command.

  Conditions: This symptom is observed in a BGP multipath configuration.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

- CSCef97738

  Symptoms: BGP may pass an incorrect loopback address to a multicast distribution tree (MDT) component for use as the source of an MDT tunnel.

  Conditions: This symptom is observed when you reload a Cisco router that runs Cisco IOS Release 12.0(28)S1 and when there is more than one source address that is used in BGP, such as Lo0 for IPv4 and Lo10 for VPN. If the IPv4 peer is the last entry in the configuration, the MDT tunnel interface uses lo0 as the source address instead of lo10. The symptom may also occur in other releases.

  Workaround: Remove and add the MDT statement in the VRF.

- CSCeh01390

  Symptoms: MSDP does not create (S,G) state and does not trigger (S,G) joins for the relevant entries in the MSDP cache, when (*,G) changes to Non NULL.

  Conditions: This happens only when IGMP modifies the (*,G) olist from NULL to Non-NULL.

  Workaround: There is no workaround.

- CSCeh11675

  Symptoms: Ping passes from inside to outside only when the NAT translation entry in NAT router (uut) is empty. When the first ping passes and an entry is made in NAT translation table all further pings fail. Packets are dropped at NAT router, and ICMP, host unreachable messages are returned. When the entry in the NAT translation table expires, ping passes again.

  Workaround: There is no workaround.

- CSCeh15802

  Symptoms: OSPF has been configured to be redistributed into a specific VRF in another routing protocol, which uses the **address-family ipv4 vrf VRFNAME** command. For example:

```
router eigrp 1
  address-family ipv4 vrf vrf1
  redistribute ospf 32 vrf vrf1
```

  But using the **show run** command, the VRF is not seen on the redistribute command line. For example:

```
router eigrp 1
 auto-summary
 !
 address-family ipv4 vrf vrf1
 redistribute ospf 32
 auto-summary
 exit-address-family
```

  This is incorrect, and after reload, the OSPF process will be created such that it is attached to the default routing table instead of the VRF.

  Conditions:

  – OSPF process is associated to a VRF
  – OSPF is redistributed in EIGRP address-family vrf

  Workaround: There is no workaround.

- CSCeh49504

  Symptoms: BGP redistribution into EIGRP based on a standard community or AS path does not work as expected.

  Conditions: This symptom is observed when the **match community** or **match as-path** route-map commands are enabled.

  Workaround: There are two steps to this workaround:

  1. Apply an inbound route map on the BGP neighbor. The inbound route map must include the **set metric** command to set the BGP multi-exit discriminator (MED) based on the standard community or AS path.
  2. Match on the BGP MED in the route map that is used in the BGP redistribution.

  Further Problem Description: Set actions in one particular statement that includes the **match community** or **match as-path** command are applied to all routes that match any subsequent statement in the same route map, instead of only to the routes that match the particular statement to which the set actions were applied.

- CSCej78303

  Symptoms: A router may crash when you disable the **ipv6 multicast-routing** command.

  Conditions: This symptom is observed when you enable and disable the **ipv6 multicast-routing** command multiple times while IPv6 Multicast traffic is being processed.

  Workaround: There is no workaround.

- CSCek35039

  Symptoms: A route map may not match a BGP IP next-hop address in the VPNv4 table.

Conditions: This symptom is observed on a Cisco router when a route map is used to control the redistribution of BGP into EIGRP by matching the IP next-hop address.

Workaround: There is no workaround.

- CSCek64468

  Symptoms: TE tunnels do not come up in the rsvp_aggregation branch.

  Conditions: This symptom occurs with the development image trying to setup TE tunnels.

  Workaround: There is no workaround.

- CSCek68469

  Symptoms: A router may reload during the “ip_static_delete_dlroute_entry” process.

  Conditions: This symptom is observed when you enter the **no aaa route download 5** command.

  Workaround: There is no workaround.

- CSCek78315

  Symptoms: A router may give spurious memory access or crash when the **debug ip ospf hello** command is enabled on the router, which has sham-links configured.

  Conditions: This symptom has been observed with sham-links configured. Only Cisco IOS images with the fix CSCse35155 integrated are affected. The **debug ip ospf hello** command is enabled during the adjacency start on the sham-link interface.

  Workaround: Do not start the **debug ip ospf hello** command in a sham-link environment.

- CSCsa53394

  Symptoms: When SNMP traps are generated on a Cisco IOS router the s**how alignment** command displays spurious memory access and tracebacks in the OSPF trap generation routine.

  Conditions: This symptom occurs on a router that is running Cisco IOS Release 12.2(18)SX with the Open Shortest Path First (OSPF) MIB.

  Workarounds: There is no workaround.

- CSCsa65155

  Symptoms: IS-IS may not update redistributed BGP network changes.

  Conditions: This symptom is observed when the **network** *network-number* command is enabled to introduce connected networks into a BGP topology and when, afterwards, BGP is redistributed into IS-IS. The symptom occurs after one of the interfaces that forms a network connection goes down and comes up again; the network re-enters the BGP topology but is no longer redistributed into IS-IS.

  Workaround: There is no workaround.

- CSCsb85290

  Symptoms: Reverse Path Forwarding may not occur for IPv6 Bootstrap Router message (BSM) packets.

  Conditions: This symptom is observed on a Cisco platform that receives and needs to forward BSMs.

  Workaround: There is no workaround.

- CSCsc35609

  Symptoms: In certain circumstances, if the static reservations are configured via the **ip rsvp listener** commands, an interface going down can cause the router to crash.

Conditions: This problem is seen under the following conditions:

1. Router is running RSVP; the **ip rsvp bandwidth** command is enabled.
2. Router has configured a receiver proxy with the **ip rsvp listener** command.
3. Router receives Path messages matching the proxy and sends out Resv messages corresponding to the received Path messages.
4. The interface on which the Path message is received goes down.

The problem is not seen if any of these conditions do not hold. For example, routers not running RSVP, or running RSVP only as a midpoint, or routers running MPLS/TE, do not see this problem.

Workaround: There is no workaround. Discontinuing the use of the **ip rsvp listener** command will prevent the crash.

- CSCsc96746

  Symptoms: PIM may not select the path with the highest IP address when it should do so.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with equal-cost RPF paths.

  Workaround: There is no workaround.

- CSCsc98828

  Symptoms: PIM becomes disabled on an output interface, preventing packets from being sent, and causing the SR flag to be set after 60 seconds on the router that functions as the first hop.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 PIM.

  Workaround: There is no workaround.

- CSCsd39528

  Symptoms: Duplicate Interface Index (ifIndex) numbers may be assigned to the multicast tunnel interfaces. This situation may prevent traffic from being switched from these multicast interfaces, and may cause the router to crash with a bus error when these multicast tunnels are deleted and then re-created.

  You can verify that the symptom has occurred by entering the **show idb** command and by looking for duplicate ifIndex entries for the multicast tunnel interfaces.

  Conditions: This symptom is observed on a Cisco router that is configured with IPv6 PIM tunnels.

  Workaround: There is no workaround.

- CSCsd63038

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

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

  address-family ipv4 mdt

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

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

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

- CSCsd68993

  Symptoms: IPv6 multicast traffic forwarding may fluctuate.

Conditions: This symptom is observed on a Cisco router that is configured for PIM and that is configured with more than 2000 multicast streams.

Workaround: There is no workaround.

- CSCse05106

  Symptoms: When NAT is configured and flow is sent, no netflow entries are software-installed, and no shortcut is created.

  Conditions: This symptom occurs if no netflow IP entries are software-installed.

  Workaround: There is no workaround.

- CSCsg07742

  Symptoms: The attributes that are configured in a site map may not automatically be applied to the BGP table when the associated interface is running other routing protocols such as RIP or OSPF.

  Conditions: This symptom is observed on a Cisco router when routes are redistributed into BGP.

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

- CSCsg84690

  Symptoms: A default route with an incorrect mask may not be installed.

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

  Workaround: There is no workaround.

- CSCsh12384

  Symptoms: Removing a loopback interface when RSVP sessions are active causes a traceback.

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

  Workaround: There is no workaround. However, there is no functional impact to the router.

- CSCsh14457

  Symptoms: A Cisco router that is running modular image (-vz- version) configured for OSPF and BFD may experience corner case crash.

  Conditions: This symptom occurs with a high number of very unstable OSPF/BFD neighbors.

  Workaround: Upgrade to fixed software version.

- CSCsh20140

  Symptoms: A small memory leak may occur when ISPF is enabled. When you deconfigure OSPF, the following error message and traceback are generated:

  ```
  %SYS-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk
  30E3268.
  -Process= "Exec", ipl= 0, pid= 3,
  -Traceback= 0x69F968 0x813670 0x8137C4 0xD57928 0xD6A230 0xB37824 0xB38550
  0x6E33F0 0x706EBC 0x7ABDD0 0x7ABDCC
  ```

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsb38978. A list of the affected releases can be found at http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsb38978. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Do not configure ISPF.

- CSCsh42565

  Symptoms: Traffic engineering (TE) tunnels go down when an intermediate link has the **ip ospf network non-broadcast** command enabled.

  Conditions: This symptom is observed in an OSPF network over TE tunnels that are established on non-broadcast links.

  Workaround: Do not use non-broadcast links. Rather, use another OSPF network type. If this is not an option, there is no workaround.

- CSCsh68376

  Symptoms: Routes that are learned from a route reflector may not be refreshed.

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

  Workaround: Perform a soft clear on the affected router to refresh the route.

- CSCsh96955

  Symptoms: The next hop for a BGP route is marked as "inaccessible," preventing the route from being advertised to peers or installed in the routing table.

  Conditions: This symptom is observed on a Cisco router when all of the following conditions are present:

  - The route is an IPv6 route with an IPv6 next hop.
  - The route is learned from an IPv6 eBGP router that is one hop away.
  - Peering occurs between loopback addresses.
  - The **disable-connected-check** command is configured for the peer from which the route is learned.

  Workaround: Disable the **disable-connected-check** command on the peer from which the route is learned. Rather, configure eBGP multihop.

- CSCsi01481

  Symptoms: Error messages are seen when the IPv6 Static RP address is unconfigured.

  Conditions: This problem is a platform independent failure.

  Workaround: There is no workaround.

- CSCsi16903

  Symptoms: An IGMPv3 mode 4 group report with empty source list {} gets translated incorrectly to a mode 6 group report when using an ssm-mapped source. Expected behavior would be to translate to a mode 5 group report.

  Conditions: This symptom occurs when IGMPv3 mode 4 group report with empty source list {} is translated by static ssm-map.

  Workaround: Avoid using empty source list {} by specifying source and therefore not needing SSM static mapping.

- CSCsi33147

  Symptoms: Prefix LSA does not get updated after interface un-shutdown.

  Workaround: There is no workaround. Bounce the interface again will fix the issue.

  Further Problem Description: This is rare timing issue. So far it is seen in a lab only when virtual link is configured.

- CSCsi35541

  Symptoms: An CPUHOG may be experienced after executing the **clear ip route *** command.

  Conditions:

  - Many connected routes, CPUHOG seen with 1000+ subinterfaces.
  - OSPF process which is not running, because it can not pick up a router-id.

  Workaround: Avoid having configured OSPF process which can not start because no router-id is available.

- CSCsi47635

  Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

  Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

  Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCsi48304

  Symptoms: After a reload, the following error message may be displayed if an OSPFv3 router redistributes large numbers of the external routes:

  ```
  %OSPFv3-3-DBEXIST: DB already exist
  ```

  No impact to the operation of the router has been observed.

  Conditions: Redistribution is configured, then router is reloaded.

  Workaround: There is no workaround.

- CSCsi59438

  Symptoms: When you enter the **ip multicast limit rpf** command, protection may fail after the RPF link becomes operational.

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

  Workaround: Clear the state of the corresponding multicast route by entering the **clear ip mroute** command.

- CSCsi97586

  Symptoms: A Cisco MGX-RPM-XF-512 resets after deleting Multicast VPN routing from a VRF and then deleting that VRF.

  Conditions: This symptom has been observed on a system running Cisco IOS Release 12.4(6)T5 configured for Multicast VPN routing while deleting an interface.

  Workaround: There is no workaround.

- CSCsj00161

  Symptoms: OSPFv3 may install into the routing table IPv6 routes load balancing between paths to Null0 and reachability path over the physical interface.

  Conditions: This problem may be seen if the **summary-address** command is configured with exactly the same address as one of external routes received from a different router.

  Workaround: There is no workaround.

- CSCsj15027

  Symptoms: If the length field of the message header is less than 19 or greater than 4096, then the Error Subcode MUST be set to Bad Message Length. The Data field MUST contain the erroneous Length field in the notification message, but those are not set in notification message.

  Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl65407

  Symptoms: A routing loop was formed in MPLS/VPN network topology with EIGRP as the PE-CE routing protocol.

  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 be necessary as well.

- CSCuk54975

  Symptoms: Routes are not redistributed into BGP and network statements to originate routes in BGP do not work.

  Conditions: This symptom is observed when the **redistribute static** command is enabled.

  Workaround: There is no workaround.

ISO CLNS

- CSCei36669

  Symptoms: A CPUHOG and traceback occur when a malicious IS-IS LSP packet is received.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S.

  Workaround: There is no workaround.

- CSCsh63324

  Symptoms: The following error message may be generated when IS-IS is configured:

  ```
  %SYS-2-CHUNKPARTIAL: chuck name ISIS NSF cp ch
  ```

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS configuration when the **nsf cisco** command is configured under the **router isis** command.

  Workaround: There is no workaround. However, the error message appears to be of a cosmetic nature and does not appear to affect the functionality of the router.

- CSCuk55515

  Symptoms: Fifty percent of the packets that are destined for an IP-over-CLNS tunnel (CTunnel) are dropped by CEF.

  Conditions: This symptom is observed when the router is configured for IPv4 CEF switching and when the next hop for the CEF-switched packets must be reached via the CTunnel.

  Workaround: There is no workaround.

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.

- CSCeb02520

  Symptoms: A Cisco Route Processor Module (RPM-PR) router that is configured as an Edge Label Switch Router (ELSR) may reset when you enter the **show queue sw1** EXEC command when there is a Multiprotocol Label Switching (MPLS) interface.

  Conditions: This symptom is observed on a Cisco RPM-PR when multiple virtual circuits (VCs) are enabled under an MPLS interface. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCeb77318

  Symptoms: When a load-balanced server uses the Don't Fragment (DF) bit in its responses, and fragmentation is needed in order to reach the client, a gateway may report this situation by using Internet Control Message Protocol (ICMP), message type 3 (destination unreachable), code 4 (datagram too big). The gateway message is translated at a router and forwarded to the correct server, but the checksum may be invalid, causing the server to ignore the message and preventing the segment size from being decreased.

  Conditions: This symptom is observed when you use Cisco IOS Server Load Balancing (SLB) with Network Address Translation (NAT).

  Workaround: Do not configure NAT when you use Cisco IOS SLB.

- CSCeb78526

  Symptoms: A router that is configured for LAN Emulation (LANE) may reload because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a Cisco router only when the creation of switched virtual circuits (SVCs) fails.

  Workaround: There is no workaround.

- CSCec90275

  Symptoms: Packets are duplicated on the Provider Edge (PE) router. A packet is switched out once in the fast switching path and another time in the process path.

  Conditions: This symptom is observed when the path between the source and the receiver goes through multiple PE routers, and all the PEs have fast-switching enabled.

Workaround: Unconfiguring ip mroute-cache from the interfaces solves the duplication.

- CSCed76056

  Symptoms: TTL is not decreased for packets, coming from GRE Tunnel interface, when CEF is enabled.

  Conditions: This symptom was seen on Cisco 2600 and Cisco 3725 routers that are running Cisco IOS Release 12.3(6).

  Workaround: Configure the **no ip route-cach cef** command on Tunnel interface.

- CSCee20888

  Symptoms: IPv6 over ISDN does not work.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(7)T1.

  Workaround: There is no workaround.

- CSCee49035

  Symptoms: An incorrect update-source interface is selected for a multicast tunnel interface in an MVPN configuration.

  Conditions: This symptom is observed when the provider edge (PE) router is also an ASBR with eBGP peers or has non-VPNv4 peers with higher IP addresses than the peer that has VPNv4 enabled. MVPN requires that the BGP update source address of a VPNv4 peer is selected as the MTI source address.

  Workaround: There is no workaround.

- CSCee66058

  Symptoms: SNMP users that have MD5 configured may become lost after a switchover in an RPR+ environment.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 12000 series that run Cisco IOS Release 12.0(27)S1 in RPR+ mode.

  Workaround: There is no workaround.

- CSCee77867

  Symptoms: A standby PRP that functions in SSO mode continues to reset.

  Conditions: This symptom is observed on a Cisco 12406 that runs a Cisco IOS interim release for Release 12.0(29)S and that is has an ATM VC bundle configuration.

  Workaround: Reload the standby PRP without the ATM VC bundle and re-apply the ATM VC bundle after the standby PRP has booted.

- CSCee78208

  Symptoms: When IP TCP header compression is configured over a PPP link attached to a Cisco 7200 router which has an LLQ service policy attached to the PPP link, the LLQ rates that are being seen at the other end of the PPP link are much less than the configured rate.

  Workaround: There is no workaround.

- CSCee93228

  Symptoms: Under certain unknown circumstances, a traceroute may trigger a process watchdog.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(26)S2. However, the problem is not specific to a Cisco 12000 series or to Cisco IOS Release 12.0S and may occur on other platforms and in Release 12.2T and Release 12.3.

  Workaround: There is no workaround.

- CSCef62324

  Symptoms: Router may crash upon removal of an ATM subinterface with PVCs.

  Workaround: There is no workaround.

- CSCef85231

  Symptoms: When SSO redundancy mode is configured and you enter the **no** form of the **mpls ldp neighbor targeted** command to deconfigure a previously configured command, the standby RP may reload. The symptom may also occur when you enter the **no** form of the **mpls ldp neighbor implicit-withdraw** command. For example, any of the following command sequences may cause the symptom to occur:

  ```
  Example 1:
  mpls ldp neighbor 10.0.0.1 targeted ldp
  ...
  no mpls ldp neighbor 10.0.0.1 targeted ldp

  Example 2:
  mpls ldp neighbor 10.0.0.1 targeted ldp
  ...
  no mpls ldp neighbor 10.0.0.1 implicit-withdraw
  ```

  Conditions: This symptom is observed when the **mpls ldp neighbor targeted** command is configured and when the Label Distribution Protocol (LDP) is globally disabled. (By default, LDP is globally enabled, but it can be disabled by entering the **no mpls ip** global configuration command.) The symptom does not occur when other commands are configured for the specific neighbor, for example, if an MD5 password is configured for the neighbor as illustrated in the command sequence below:

  ```
  no mpls ip
  mpls ldp neighbor 10.0.0.1 targeted ldp
  mpls ldp neighbor 10.0.0.1 password foo
  no mpls ldp neighbor 10.0.0.1 targeted ldp
  ```

  This symptom occurs in releases that integrate the fix for caveat CSCee12408. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCee12408.

  Workaround: Configure a password for the neighbor as shown in the Conditions above before you enter the **no** form of the **mpls ldp neighbor targeted** command or the **no** form of the **mpls ldp neighbor implicit-withdraw** command.

- CSCeg27616

  Symptoms: CE to PE ping loss through VRF cloud when CEF is turned on PE.

  Conditions: The problem is seen on Cisco routers that are running Cisco IOS Release 12.2(27.1)S.

  Workaround: There is no workaround.

- CSCeh06200

  Symptoms: You may not be able to gain access to a router via HTTP when the idle time is set on a TACACS server. Telnet via TACACS works as expected.

  Conditions: This symptom is observed on a Cisco router that functions as an Access Point (AP) and that is configured for TACACS.

  Workaround: There is no workaround.

- CSCeh32706

  Symptoms: An inter-AS TE LSP fails to send a signal after a router is rebooted as an ASBR.

  Conditions: This symptom is observed when there are parallel links between ASBRs with a combination of point-to-point and broadcast interfaces that are configured with the MPLS Traffic Engineering--Inter-AS TE feature and (passive) link flooding.

  Workaround: Shut down the broadcast interface between the ASBRs.

- CSCeh52330

  Symptoms: When using SPA-CT3 in a SIP1 module the following error message might appear on the console screen.

  ```
  SLOT 7: 06:46:34: %INTR_MGR-3-INTR: SPA-4XCT3/DS0[7/0] EFC Parity Error
  06:46:34: %Fatal Error: Hardware error (EFC Parity Error) detected for SPA 7/0
  ```

  Conditions: This error message would appear if the T3 controller flaps continuously for a long time.

  Workaround: There is no workaround.

  Further Problem Description: Apart from the above error message appearing on the console, there are no apparent side effects because of it. The interfaces continue to function normally.

- CSCeh59149

  Symptoms: An "%ATM-3-FAILCREATEVC: ATM fails to create VC" error, and tracebacks are seen when trying to configure a new ATM PVC.

  Conditions: This problem is seen when trying to create new ATM PVCs following a redundancy force-switchover.

  Workaround: There is no workaround.

- CSCeh66159

  Symptoms: Pim interface counters on the incoming interface do not reflect the traffic stats correctly.

  Conditions: This is seen to happen with MDS (multicast distributed switching) is enabled on the router.

  Workaround: There is no workaround.

- CSCeh71960

  Symptoms: Alignment traceback will be shown on Standby RP after SSO.

  Conditions: This problem occurs when ATM interfaces are present in the configuration.

  Workaround: There is no workaround.

- CSCeh72672

  Symptoms: After a switchover two VRF aggr labels are seen.

  Conditions: This problem is observed if the BGP graceful restart is not configured and after a switchover.

  Workaround: Configure BGP graceful restart.

- CSCei39688

  Symptoms: When a CEF initialization failure occurs, an ATM PVC that is configured for OAM may not pass traffic even though the PVC link status is up:

  ```
  Router#show ip interface brief | include ATM
  ATM3/0/0                   unassigned      YES manual up      up
  ATM3/0/0.100               unassigned      YES unset  up      up
  ```

```
ATM3/0/0.300               10.1.1.1        YES manual up      up
ATM3/0/0.999               unassigned      YES unset  up      up

Router#show cef interface brief | include ATM
ATM3/0/0                        unassigned      up      dCEF
ATM3/0/0.100                    unassigned      down    dCEF
ATM3/0/0.300                    10.1.1.1        down    dCEF
ATM3/0/0.999                    unassigned      down    dCEF

Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached            ATM3/0/0.300
```

When CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic that is destined for the IP address of the subinterface is dropped.

Conditions: This symptom is observed on a Cisco router and occurs only when OAM is configured on the PVC.

Workaround: To prevent the symptom from occurring, do not configure OAM on the PVC. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM subinterface. After the workaround has been applied, the output of the **show ip cef** command shows the following:

```
Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached            ATM3/0/0.300
10.1.1.0/32     receive
10.1.1.1/32     receive
10.1.1.3/32     receive
```

- CSCei58681

  Symptoms: Port does not come up in a Port channel

  Conditions: This symptom is observed when converting L2 port channel into L3 port channel then removing the minimum links command and do a Shut/NO Shut on the member port.

  Workaround: Reset the associated line card where the port channel member does not come up.

- CSCei59601

  Symptoms: A Cisco 7200 series router unexpectedly reloads.

  Conditions: This behavior is observed on Cisco IOS Release 12.2(28.05.06)SX.

  Workaround: There is no workaround.

- CSCei67410

  Symptoms: A router may crash when a rare race condition occurs between the Virtual Exec/Exec process and processes that contend with the resources that are used during the execution of the **show sss session all** command.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the router accesses memory that was overwritten by another process.

  Workaround: Avoid entering the **show sss session all** command while the circuit state change. If this is not an option, there is no workaround.

- CSCei67700

  Symptoms: frde failed to match control packets on FR over AToM

Conditions: The problem can be observed on a Cisco 7500 router.

Workaround: There is no workaround.

- CSCei68902

  Symptoms: With around 15 MFR bundles, router reloads and sometimes spa_reload leads to some of the bundles staying in down state.

  Conditions: The router needs to have a SPA-CTE1 configured for Multilink Frame-relay and the LC or the SPA needs to be reloaded to hit.

  Workaround: One or two reloads of the SPA should recover the problem

  Further Problem Description: This problem has not yet been seen on SPA-CTE1. It has only been seen on a SPA-CT3. Since both share the design where the problem has been fixed, this DDTS is going to track the fix for SPA-CTE1

- CSCei83160

  Symptoms: PIM neighbors do not recognize each other via a VRF tunnel interface because multicast does not receive MDT updates from BGP. The output of the **show log** command shows the following debug message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (3) received in update for prefix
  2:55:1111:192.168.31.1/32 from 192.168.31.1
  ```

  Conditions: This symptom is observed on a Cisco router and is not platform-dependent. The symptom occurs when a VRF instance is configured with BGP as the Exterior Gateway Protocol (EGP).

  Workaround: There is no workaround.

- CSCei92291

  Symptoms: A customer who is running Cisco Catalyst 6500 in native mode with Cisco IOS 12.2SXF software may encounter “Error in setting Reload Reason” error message at the time of write memory.

  Workaround: There is no workaround.

- CSCei93090

  Symptoms: EIGRP does not learn routes when the **ip pim sparse-dense-mode** command is configured on a Gigabit Ethernet interface.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS interim Release 12.4(4.3).

  Workaround: There is no workaround.

- CSCej21515

  Symptoms: ATM SPA SRAM parity or SDRAM ECC errors may occur if the SPA was brought up at one temperature and there is then a significant change in temperature. In the case of SRAM parity errors, the SPA will be reset. In the case of ECC errors, the corrupted packet will be dropped, and the SPA will continue operating normally.

  Conditions: This problem would only be seen when there is a significant temperature change from the time when the SPA was initialized. Only a small percentage of ATM SPAs may see this problem and even those that are at risk will not come up in this state every time the card is initialized.

  Workaround: There is no workaround.

- CSCej21520

  Symptoms: In HA environment, removing “aps protect 1” from ATM SPA interface, can cause console lock for a few minutes.

  Conditions: Router should be a 7600, with a secondary supervisor, and APS configured on an ATM SPA.

  Workarounds:

  1. User reloads the *secondary* supervisor (by using the **redundancy reload peer** command) and then issues a **no aps protect 1** command, while the secondary supervisor is still booting.
  2. User connects a console cable to the secondary supervisor and responds to the **no aps protect 1** command on the secondary console also.

- CSCej31343

  Symptoms: Active RP crash when unconfiguring ip vrf vpn after SSO.

  Conditions: Problem is found on HA-SSO capable routers with Cisco IOS Release 12.2(31.4)S image.

  Workaround: There is no workaround.

- CSCej83531

  Symptoms: The test failed at ping to dns-server in subtest change_hostname_ip of ipsec_realTimeDNs testing.

  Conditions: The above symptom happens on Cisco routers with Cisco IOS Release 12.4(4.7)PI3c.

  Workaround: There is no workaround.

- CSCek24782

  Symptoms: A Cisco platform that is configured for ISDN and AAA may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 5400XM that functions under stress. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCek26296

  Symptoms: Service policy configured with a single bandwidth+shape class it is not getting the guarantee.

  Conditions: Problem is seen on OSM-8OC3-POS interface with Cisco 7600 Sup3 router

  Workaround: There is no workaround.

- CSCek26742

  Symptoms: The line protocol remains down on SPA-8XCHT1E1 after rpr+ switchover. This issue is seen only on the Cisco 7600 router and not on Cisco 12000 series router.

  Conditions: A SPA-8XCHT1E1 needs to be present in the Cisco 7600 system.

  Workaround: There is no workaround.

- CSCek27892

  Symptoms: Disordered output of show policy-map.

  Conditions: It can be observed on Cisco 7500 and Cisco 7200 platform.

  Workaround: There is no workaround.

- CSCek30891

  Symptoms: Traffic loss may occur during reoptimization on a Cisco router that functions as a transit node for zero-bandwidth MPLS TE label switched paths (LSPs). The traffic loss stops when the TE tunnel headend switches traffic over to the new LSP.

  Conditions: This symptom is observed on a Cisco router when reoptimization is triggered on the headend either periodically, manually, or as a result of a topology change.

  Workaround: There is no workaround.

- CSCek34117

  Symptoms: The SIP200, installed with ATM SPA, would crash under scalability configuration + MQC QoS applied.

  Conditions: Interface flapping occurs under traffics.

  Workaround: There is no workaround.

- CSCek37085

  Symptoms: The **service-policy output** *policy-map-name* control-plane configuration command does not function.

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

  Workaround: There is no workaround.

- CSCek39331

  Symptoms: In a FR MBP scenario, on the DTE side, a FR subinterface in shutdown state continues to receive and forward traffic.

  Conditions: This behavior is seen on SIP200, SIP400, FW2 and may impact other line cards on Cisco 7600.

  Workaround: There is no workaround.

- CSCek39946

  Symptoms: Ping failure or no connectivity with ATM Local switching after SSO Switchover

  Conditions: Configure ATM local switching with SIP-200 Linecard and ATM OC3 SPA on a redundant system that has been configured with Stateful Switchover (SSO). Perform a forced switchover and verify connectivity after the standby supervisor becomes active.

  Workaround: Do shut & no shut on the atm interfaces where connect has done. Show connect will show as up, then local switching will work. Ping will go pass after this.

- CSCek41338

  Symptoms: A router reloads when you enter the **peer default ipv6 address pool** *pool-name* command in template-configuration mode.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6.

  Workaround: A workaround is not applicable because the **peer default ipv6 address pool** *pool-name* command in template-configuration mode is not supported in an IPv6 configuration and should not be entered as such.

- CSCek42751

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

Workaround: Reboot the router once more.

- CSCek44532

  Symptoms: A standby RP may reload repeatedly when you enter the **issu loadversion** command during a period of high checkpointing activity. When you enter the **show checkpoint statistics** command on the active RP, the output shows that the checkpointing IPC flow control status remains set to zero indefinitely:

  ```
  CHKPT FLOW_ON status = 0
  ```

  Conditions: This symptom is observed on a Cisco router when the standby RP reloads as part of the In-Service Software Upgrade (ISSU) process while, for example, a large number of PPPoA sessions are being disconnected.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command to cancel the ISSU process, and then reload the router.

- CSCek44674

  Symptoms: Ping failed Across Network from Source CE1 to Dest CE3.

  Conditions: The symptom occurs on Cisco 7600 router that is running Cisco IOS Release 12.2(32.8.11)SR and Release 12.2(32.8.1)SRA.

  Workaround: There is no workaround.

- CSCek49107

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

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

  Workaround: There is no workaround.

- CSCek51851

  Symptoms: When more on slavenvram:startup-config is in progress and switchover is performed, the standby keeps constantly reloading and does not come up.

  Conditions: This problem is seen on Sup720 platforms.

  Workaround: There is no workaround.

- CSCek53704

  Symptoms: When you first configure and attach more than 255 class maps in a single policy to an interface and when you then remove the policy map, the router crashes.

  Conditions: This symptom is observed on a Cisco router and occurs because a maximum of 255 class maps (that is, 254 user-defined class maps and one default class map) are supported in a single policy map.

  Workaround: There is no workaround. Ensure that you do not configure more than 255 class maps, including the default class map, in a single policy map.

- CSCek57267

  Symptoms: CPUHOG and IPCOIR errors may occur on a Cisco router when you change the IP address of a loopback interface that is associated with a large number of active PPP sessions.

  Conditions: This symptom is observed on a Cisco 10000 series that runs slowly when interfaces flap. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCek59453

  Symptoms: When you configure an ATM VC on which PPPoE sessions are established, a spurious memory access may be generated.

  Conditions: This symptom is observed on a Cisco router when the VC is torn down.

  Workaround: There is no workaround.

- CSCek60629

  Symptoms: A Cisco 10000 series may crash because of an address error (that is, a load or instruction fetch exception) when multiple combined command-line interface (CLI) changes are made.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ when you attempt to make multiple policy map changes on a PVC that has a small number of active sessions with a moderate amount of downstream traffic. The symptom appears to be both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek64188

  Symptoms: An error message indicating memory leak and pending transmission for IPC messages is displayed as follows:

  ```
  *Dec  3 01:31:31.792: %IPC-5-WATERMARK: 25642 messages pending in xmt for the
  port Primary RFS Server Port(10000.C) from source seat 2150000
  *Dec  3 01:32:01.489: %SYS-2-MALLOCFAIL: Memory allocation of 4268 bytes
  failed from 0x9F32944, alignment 32
  ```

  Conditions: This issue is triggered by CSCeb05456 and is applicable only if your Cisco IOS image has integrated the fix of CSCeb05456.

  Workaround: Periodically, reload the router so that the IPC buffer pool will be reinitialized.

- CSCek67698

  Symptoms: A session cannot be set up because you cannot apply a service policy to the session.

  Conditions: This symptom is observed on a Cisco router when a VRF is present in the service profile of an IP-routed subscriber and when the initiator is configured for DHCP.

  Workaround: Remove the VRF from the service profile.

- CSCek67782

  Symptoms: When you enable or disable the **fair-queue** or **random-detect** command, the router may unexpectedly reload because of a TLB exception.

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

  Workaround: There is no workaround.

- CSCek67845

  Symptoms: SSO and ISSU may not function for PPP- and MLP-related links.

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

  Workaround: There is no workaround.

- CSCek68014

  Symptoms: After a router is reloaded through a Telnet session via vty lines, the router may wait for an input character on the console instead of booting up.

Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when you perform a remote upgrade.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **reload** command via the console.

- CSCek68047

  Symptoms: Authentication may be skipped during account logon.

  Conditions: This symptom is observed when an IP session is brought up with a default service before account logon.

  Workaround: Do not configure a default service before account logon.

- CSCek71346

  Symptoms: The MPLS forwarding table is not shown on a router, causing packet drops in end-to-end connectivity across the MPLS cloud.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router after a switchover has occurred.

  Workaround: There is no workaround.

- CSCek71514

  Symptoms: On a Cisco router that has the **mpls ldp igp sync delay** *delay-time* command enabled, the master timer may be accessed prior to being initialized, and the following error message is generated:

  ```
  %SYS-3-MGDTIMER: Uninitialized timer, init with uninitialized master, timer = 53E62C0.
  -Process= "Init", ipl= 0, pid= 3
  ```

  Because the master timer was not properly initialized, other symptoms may occur, including the following:

  – When the LDP session comes up, further error messages and a traceback regarding the master timer may be generated:

  ```
  LDP-SYNC: Et1/0: Delay notifying IGP of sync achieved for 60 seconds R1
  (config)#
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime_internal, timer = 198A980.
  -Process= "Tag Control", ipl= 0, pid= 61
  -Traceback= 2AEAE4 3642DC 364580 364ADC 364BAC 9BF154 9C22C0 9C24D8 9D4500
  9CD544 9D1C8C 34AD58 34AD54
  ```

  – When the “Delay notification” error message is generated (see above), the output of the **show mpls ldp igp sync** command may shows “0 seconds left” for the synchronization delay time, which contradicts the “Delay notification” error message:

  ```
  LDP-SYNC: Et1/0: Delay notifying IGP of sync achieved for 60 seconds R1
  (config)#
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime_internal, timer = 198A980.
  -Process= "Tag Control", ipl= 0, pid= 61
  -Traceback= 2AEAE4 3642DC 364580 364ADC 364BAC 9BF154 9C22C0 9C24D8 9D4500
  9CD544 9D1C8C 34AD58 34AD54
  ```

  – OSPF may remain in the “sending maximum metric” state, and the routing table may not be updated, as can be shown in the output of the **show ip ospf mpls ldp interface** command:

  ```
  R1#show ip ospf mpls ldp interface
  Ethernet1/0
  ```

```
Process ID 1, Area 0
LDP is not configured through LDP autoconfig
LDP-IGP Synchronization : Required
Holddown timer is not configured
Interface is up and sending maximum metric
```

Conditions: These symptoms are observed when an RPR+ switchover has occurred or when you configure the **mpls ldp igp sync delay** *delay-time* command while LDP is not enabled or while LDP is enabled but not fully active (for example, when all the interfaces are down).

Workaround: There is no workaround to prevent the initial error message and traceback from being generated. However, after the initial error message and traceback have been generated, you can prevent any further symptoms from occurring by reconfiguring the synchronization timer and re-enabling the **mpls ldp igp sync delay** *delay-time* command on the affected interface as in the following example:

```
R1(config-if) no mpls ldp igp sync delay
R1(config-if) mpls ldp igp sync delay 60
R1(config-if) no mpls ldp igp sync
R1(config-if) mpls ldp igp sync
```

- CSCek71805

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

  Symptom 1: A PA-8B-ST port adapter may be powered down when you boot the router.

  Condition 1: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

  Workaround 1: Perform a software OIR to bring up the port adapter.

  Symptom 2: The ISDN layers may not come up.

  Condition 2: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

  Workaround 2: Enter the **debug bri-interface** command to bring up the ISDN layers.

- CSCek71844

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

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

  Workaround: There is no workaround.

- CSCek72621

  Symptoms: IPv6 neighbor discovery may stop caching sourced outgoing packets during resolution.

  Conditions: This symptom is observed on a Cisco router after IPv6 neighbor discovery has cached 16 messages for resolution when these messages are locally generated.

  Workaround: There is no workaround.

- CSCek73386

  Symptoms: A Cisco router with an ESCORT jacket card crashes.

  Conditions: This symptom is observed with a Cisco 7200 router that is loaded with Cisco IOS Release 12.4XD if an ESCORT jacket card is present.

  Workaround: There is no workaround.

- CSCek74474

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

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

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

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

- CSCek74740

  Symptoms: Shaping and random detect may not be enabled when you attempt to do so.

  Conditions: This symptom is observed on the fourth native Gigabit Ethernet port on a Cisco 7201 that runs Cisco IOS Release 12.2SB but may not be platform- and release-specific.

  Workaround: There is no workaround.

- CSCek74858

  Symptoms: When the **glbp** *group* **weighting track** *track_number* command is configured on the active processor of an HA capable router, the equivalent command does not get synced to the standby processor configuration. After the processor switchover, the GLBP weighting track command will have no affect on the operation of the group.

  Conditions: This symptom has been observed on HA capable routers in RPR, RPR+ or SSO mode, and supporting GLBP.

  Workaround: There is no workaround. The configuration will have to be entered into the new active processor configuration after switchover.

- CSCek75732

  Symptoms: A router may crash when you attach a service policy to range of PVCs.

  Conditions: This symptom is observed when a policy map has a bandwidth configured and when the service policy is attached in the ingress direction.

  Workaround: There is no workaround.

- CSCek76933

  Symptoms: A router may crash when you configure an ATM PVC on an ATM point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router when the ATM point-to-point subinterface is already part of a bundle.

  Workaround: Configure the ATM PVC on an ATM multipoint subinterface.

- CSCek78330

  Symptoms: A router that is configured with ATM PVCs may generate the following type of error messages:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-
  Access2.1 linked to wrong idb Virtual-Access2.1
  ```

  Conditions: This symptom is observed on a Cisco router that has virtual-template subinterfaces.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **no virtual-template subinterface** command, save the configuration to the startup configuration, and reload the router.

- CSCin92033

  Symptoms: On bootup of Serial PAs, the following messages may be seen on the console:

  ```
  "Failed to assert Physical Port Admini State Down"
  ```

  Conditions: These messages seem harmless but may cause the router cards to reload a couple of times before stabilizing.

  Workaround: There is no workaround.

- CSCin97208

  Symptoms: When more on slavenvram:startup-config is in progress and switchover is performed, the standby keeps constantly reloading and does not come up.

  Conditions: This problem is seen on Sup720 platforms.

  Workaround: There is no workaround.

- CSCin97912

  Symptoms: After LC reset, Intf comes as up-up even if peer is down

  Conditions: This symptom occurs when two FE SPAs are connected back-to-back. Both the ports are configured up. During reloading one of the line cards and shutdown the port on the other End. When the line card on one END will come up online. The SPA on the line card has to detect that the peer is down and the port on that SPA should go down-down. Interface comes up.

  Workaround: Shut/No Shut.

- CSCir00786

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

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

  Workaround: Perform the following tasks:

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

- CSCir02274

  Symptoms: Some issues are observed during unit testing on EVC PC, which needs the hw_index determination for EVC PC. For that, add two macros

  ```
  + #define SIP10G_PC_MLINK_ON_PXF0 0
  + #define SIP10G_PC_MLINK_ON_PXF1 1
  ```

  Conditions: This symptom is seen during unit testing for EVC PC.

  Workaround: There is no workaround.

- CSCsa49566

  Symptoms: An error message similar to the following may be logged on a router:

  ```
  %FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface
  ```

```
for unknown if with illegal if_number: 0
```

This message is followed by a traceback.

Conditions: This symptom is observed on a Cisco router when a virtual interface or a virtual loopback interface is created.

Workaround: There is no workaround.

- CSCsa99158

  Symptoms: Unexpected START records seen in accounting.

  Conditions: Authentication done by RADIUS server. Authorization done by IOS AAA locally.

  Workaround: There is no workaround.

- CSCsa99983

  Symptoms: New AToM or L2TPv3 sessions may not come up.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink Frame Relay (MFR) over L2TPv3/AToM when there are services with incomplete MFR over L2TPv3/AToM configurations and when the router has run for a long period of time.

  Workaround: There is no workaround.

- CSCsb12329

  Symptoms: The ifAdminStatus shows that ATM layer and ATM AAL5 Layer of ATM sub-interface are down even though there is **no shutdown** command. This situation prevents from monitoring the proper administrative status of the ATM sub-interface via SNMP.

  Conditions: This symptom is observed when ATM main interface or sub-interface is operationally down, which could be caused by circuit line problem, facing equipment's down, etc.

  Workaround: There is no workaround on SNMP. Rather, use **show interface** CLI command.

- CSCsb12969

  Symptoms: All VIPs or FlexWAN modules reload unexpectedly on a platform that is configured for Modular QoS CLI (MQC).

  Conditions: This symptom is observed on a Cisco 7500 series (with VIPs) and a Cisco 7600 series and Cisco Catalyst 6500 series (both with FlexWANs) when the following steps occur while the physical interface is in the UP state:

  1. An input policy and output policy map are already attached to an ATM or Frame Relay PVC. When you attach the same policy map to the main interface, an error message is generated and the configuration is rejected.
  2. You remove the policy map from the PVC and attach the same policy map to the main interface.
  3. You remove the policy map from the main interface.

  At this point, all VIPS or FlexWAN modules reload, even though no traffic is being processed during the above-mentioned steps.

  Workaround: There is no workaround.

- CSCsb42241

  Symptoms: A Cisco 7500 series router configured for dMLPPP may experience an unexpected reload of the VIP when the members of the bundle flap.

  Conditions: This symptom is seen on a Cisco 7500 series router that is configured for dMLPPP.

  Workaround: There is no workaround.

- CSCsb47257

  Symptoms: A Cisco router may reload due to a bus error.

  Conditions: This symptom is observed on a Cisco router that is configured for IPSec. This crash may occur when the peer sends a certificate wrapped in an PKCS7 envelope and the validation fails. When the peer tries to resend the certificate the router may crash.

  Workaround: There is no workaround.

- CSCsb48739

  Symptoms: Cisco GTP server load balancer forwards the create request to an alternate GGSN even when there exists a sticky IMSI object when the create request comes after the session object idles out.

  Conditions: This problem is seen only when the second create request comes after the session idles out.

  Workaround: There is no workaround.

- CSCsb68178

  Symptoms: Traceback %MPLS_IPRM-3-DB_PATH is seen on 6VPE.

  Conditions: This symptom is observed on 6VPE with “address-family vpnv6” configured for bgp.

  Workaround: There is no workaround.

- CSCsb76401

  Symptoms: If you load Cisco IOS Release 12.2(29.X)SX and Release 12.2(18)SXF image in active and standby, configuration mode will be locked out indefinitely.

  Workaround: Load same image on both active and standby.

- CSCsb83521

  Symptoms: The following error message may be generated after an SSO switchover:

  ```
  %SCHED-3-STUCKMTMR: Sleep with expired managed timer 55BE2914 time 0x1CD561
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that is configured for High Availability (HA).

  Workaround: There is no workaround.

- CSCsc04015

  Symptoms: When querying the cbQosCMStatsTable of the CISCO-CLASS-BASED-QOS-MIB, byte and bitrate statistics are not available for Port Adapters (PAs). The value returned for byte and bitrate statistics are always zero. This information is available on the CLI. The customer is getting zero value when polling cbQosCMPostPolicyByte64 in Cisco IOS Release12.2(18)SXE2 (7600/SUP720).

  Conditions: This problem only occurs in the Cisco 7600/6500 FlexWAN and PAs interfaces.

  Workaround: There is no workaround.

- CSCsc08602

  Symptoms: Lack of code 50 support is no stickies built when a code 50 message is processed.

  Conditions: This symptom occurs when a code 50 message is sent to an RLB server.

  Workaround: There is no workaround.

- CSCsc14208

  Symptoms: When you change the IP address of a loopback interface that functions as the ID for a TE router, TE auto-mesh tunnels do not reestablish a connection with that router. Also, static TE tunnels for which the destination is modified to match the new loopback IP address cannot reestablish their connection and the tunnels remain down.

  Conditions: This symptom is observed when all of the following conditions occur:

  - OSPF is configured to flood TE advertisements in a given area via the **mpls traffic-eng area** *area-number* command.
  - OSPF is configured to use the loopback interface for which the IP address is modified as the ID for the TE router via the **mpls traffic-eng router-id** *loopback* command.
  - TE tunnels or auto-mesh tunnels are configured with the destination set as the IP address of the loopback interface that is mentioned above.
  - You change the IP address of the loopback interface that is used as the ID for the TE router.

  Workaround: If you need to change the loopback address that is used as the ID for the TE router, follow these steps:

  1. Shut down the loopback interface.
  2. Modify the IP address of the loopback interface.
  3. Bring up the loopback interface.

  When the loopback interface address was changed and the symptom has occurred, clear the OSPF routing process in order for the tunnels to be reestablished by entering the **clear ip ospf process** command.

- CSCsc27474

  Symptoms: The output of the **show ip mcache** command does not display the MAC header on a router that is configured for multicast and Multilink Frame Relay (MLFR).

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(5) but appears to be release-independent.

  Workaround: There is no workaround.

- CSCsc30268

  Symptoms: When you reload one line card, all other line cards in the chassis may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0(32)S or an earlier release and on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SX.

  Workaround: There is no workaround.

- CSCsc30451

  Symptoms: On routers with a lot of IPSec tunnel interfaces (VTI) configured, after rebooting, many tunnel interfaces remain in state “line protocol down” even though IPSec SAs are correctly establish. As a consequence no traffic can be sent through the affected tunnels from that router.

  Conditions: This was observed on a router with approximately 200 tunnel interfaces, 90 of them remain down after rebooting.

  On the VPN peer for one of those tunnels, the interface was up.

  Workaround: Do a **shutdown**, followed by a **no shutdown** on one affected tunnel interface will bring it up correctly.

- CSCsc43862

  Symptoms: Ping failure on SPA interfaces

  Conditions: This can happen with SPA inserted in a C7600-SIP-200. The problem is caused by fabric channel sync failure during bootup of a C7600-SIP-200. To verify if a ping failure is caused by this problem, check the **show logging** command under the C7600-SIP-200 console for the following error message:

  ```
  00:00:43: Serial Primary Channel SYNC FAILED!
  ```

  To get the C7600-SIP-200 console, use the **attach** *slot #* command.

  Workaround: Reloading the affected C7600-SIP-200 can correct the sync failure problem.

- CSCsc46105

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

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

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

- CSCsc46301

  Symptoms: A Cisco 7600 series router that is running GTPSLB crashes.

  Conditions: This symptom occurs when removing real server without taking the real out of service with gtp imsi configured.

  Workaround: Clear the GTP imsi sticky entries before removing the real:

  clear ip slb sticky gtp imsi

- CSCsc61309

  Symptoms: When DHCP for IPv6 is configured on an interface, memory may not be freed when a packet is dropped, causing memory allocation failures.

  Conditions: This symptom is observed, for example, when the interface is not configured for IPv6, when the interface is not in the up state, or when encryption is configured on the interface.

  Workaround: There is no workaround.

- CSCsc61784

  Symptoms: The **show interface** *interface* **stats** command output incorrectly shows fastswitched packets as process switched packets.

  Conditions: This symptom is observed on a Cisco 7200 platform on T1/E1 interfaces only.

  Workaround: There is no workaround. Do not rely on the counters displayed by the **show interface** *interface* **stats** command output.

- CSCsc68615

  Symptoms: The router crashes with IPv6 tunnel.

  Conditions: This symptom is observed after tunnel forwarding is complete and unconfguring the applied configs is done.

  Workaround: There is no workaround.

- CSCsc77704

  Symptoms: Cisco router may experience a hang in which access is not available via console or telnet. Router must be reloaded to recover.

  Conditions: The specific conditions and/or trigger are not known. This problem is being seen in Cisco IOS Release 12.3(14)T5.

  Workaround: There is no workaround.

- CSCsc78707

  Symptoms: The **mpls l2transport route** command may be rejected as an invalid input.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCsc84768

  Symptoms: BFD configuration under Ethernet type of interfaces will be lost.

  Conditions: This symptom has been observed when the Removal / Insertion of the Ethernet type of interface is done.

  Workaround: There is no workaround.

- CSCsc95559

  Symptoms: When a policy class is configured only with the **trust** command, the output CoS may be set to zero for incoming MPLS packets, instead of to the incoming MPLS EXP bit (that is, assuming that the **no mls qos mpls trust exp** command is not configured).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when incoming MPLS packets are layer 2-switched.

  Workaround: Add a **police** command that does not perform actual policing, for example, with an exceed-action “transmit”.

- CSCsc98850

  Symptoms: On a Catalyst 6000 series switch, the following message may be logged:

  ```
  macedon_tunnel_set_pmtu: Could not send pmtu information vlan 65535 pmtu 0
  ```

  Conditions: This symptom is seen when tunnel path-mtu-discovery is configured under a Tunnel interface.

  Workaround: This is a cosmetic issue that does not impact functionality nor performance of the switch.

- CSCsd01885

  Symptoms: In FLEXWAN module, CAM entries are not flushed when the PVC goes DOWN.

  Conditions: This symptom is observed on a Cisco Catalyst 6000.

  Workaround: There is no workaround.

  Further Problem Description: Depending on customer network design, this can lead to backholing traffic.

- CSCsd05513

  Symptoms: When using service policy on an OSM-POS port some MIB objects have wrong values:

  1. The TX cbQosCMPrePolicyByte64 counter is always 0. It is not incremented with traffic.
  2. The TX cbQosCMDropByte64 counter is always 0 even when the policer is dropping traffic.

3. The class-default counters for RX and TX (cbQosCMPostPolicyByte), (cbQosCMPrePolicyByte), (cbQosCMDropByte) are not incrementing even when traffic is sent in this class.

Conditions: This symptom occurs when using service policy on an OSM-POS port.

Workaround: There is no workaround.

- CSCsd15625

  Symptoms: CEF adjacencies are not established with subinterfaces having ISL encapsulation

  Conditions: This issue is only seen when subinterfaces with ISL encapsulation are configured. It is not seen with dot1q encapsulation.

  Workaround: There is no workaround.

- CSCsd19880

  Symptoms: The new style atm pvc command does not work properly. The command is accepted but the pvc will not come up. The ATM legacy ping fails.

  Conditions: This symptom occurs when applying the new style atm pvc command. The command will be accepted, but the PVC will not come up.

  Workaround: Use the old style atm pvc command. It works fine.

- CSCsd22834

  Symptoms: The following errors may be seen while using a 7600-SIP-200 card:

```
SLOT 1: *Dec 13 06:46:12.642 CST: %SIP200_MP-4-PAUSE: Non-master CPU is
suspended for too long, from 0x4060E438(2) to 0x4060E764 for 369087 CPU cycles.
-Traceback= 4060EA2C 40615DE8 405B7A48 405B7CF8 405B8160 405B8628 40646F8C
40663798 4069FB9C 406AC76C 406A50F4 406A58AC
SLOT 2: *Dec 13 06:46:12.642 CST: %SIP200_MP-4-PAUSE: Non-master CPU is
suspended for too long, from 0x4060E438(2) to 0x4060E764 for 368286 CPU cycles.
-Traceback= 4060EA2C 40615DE8 405B7A48 405B7CF8 405B8160 405B8628 40646F8C
40663798 4069FB9C 406AC76C 406A50F4 406A58AC
```

  Conditions: This symptom can be seen on any system using SIP-200 cards.

  Workaround: There is no workaround.

- CSCsd27088

  Symptoms: ARP/CDP Packet loss is seen on a SIP400 interface on a system that is running Cisco IOS Release 12.2(18)SXF4.

  Conditions: This symptom is seen with input QoS service policy with the "set-mpls-exp-imposition-transmit" defined in the policy. Example:

```
policy-map QOS_POLICY_IN
   class class-default
   police cir 3072000 bc 576000 be 1152000 conform-action
set-mpls-exp-imposition-transmit 5 exceed-action drop
```

  Workaround: Remove input service policy.

- CSCsd30533

  Symptoms: Duplicate IPsec flows may be created on the responder side during IPsec Quick Mode (QM) negotiation, leaving one flow with IPsec SAs and the other flow empty. This situation may cause multiple IPsec SAs to be created.

Conditions: This symptom is observed during the creation of IPsec SAs when the IPsec module fails to find the existing flow.

Workaround: There is no workaround.

- CSCsd30932

  Symptoms: Issuing the **trust-point storage** command sometimes causes a crash.

  Conditions: This symptom only occurs when an error occurs on a previous execution of this command. The second execution of the command results in a crash.

  Workaround: If an error occurs when issuing this command, the trustpoint must be removed and re-created to avoid a crash.

- CSCsd34114

  Symptoms: A router that has the **ip local pool** command enabled in an IPv6 configuration may reload under rare circumstances.

  Conditions: This symptom is observed when the local pool must allocate prefixes to the same user name on multiple interfaces in a specific order, then releases one of the prefixes, and then attempts to allocate a new prefix.

  The interfaces that the prefixes are allocated on, and the ordering of the events, must follow a very specific pattern in order for the symptom to occur.

  Workaround: Use per-user prefixes from a RADIUS server, or in a DHCP-PD configuration, use the prefix allocation per DUID.

  Further Information: IP local pools in an IPv6 configuration are used by DHCP-PD and by IPv6 Control Protocol (IPv6CP) for IPv6 over PPP links. However, the symptom is unlikely to occur with IPv6CP.

- CSCsd55004

  Symptoms: A FRR backup tunnel undergoes reoptimization, resulting in the teardown of the old lsp that is carrying traffic for primary lsps that have cutover to the backup tunnel.

  Conditions:

  - TE tunnel protecting interfaces/links
  - Usual triggers for re-optimization (link up, timer expiry, etc.)

  Workaround: There is no workaround.

- CSCsd56696

  Symptoms: Traffic is not shaped to the expected rate.

  Conditions: This symptom is observed when adaptive shaping is configured in egress direction and around 60kpps BECNs are received on this interface.

  Workaround: There is no workaround.

- CSCsd70673

  Symptoms: Traceback from DCEF720 @ sw_vlan_read_configuration(0x20d42764)+0xf4.

  Conditions: The problem is seen on dCEF720 line card after booting up the test image.

  Workaround: There is no workaround.

- CSCsd74729

  Symptoms: A crypto map may become “incomplete” and IPsec negotiation may fail.

Conditions: This symptom is observed on a Cisco platform when the **ip vrf forwarding** *vrf-name* interface configuration command is removed from an interface or changed.

Workaround: Remove and re-apply the crypto map configuration to the interface.

- CSCsd81275

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

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

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

  Workaround: There is no workaround.

- CSCsd87915

  Symptoms: The bug happens when RSVP Graceful Restart is configured on a router, and a neighbor router is performing an SSO switchover.

  When the RSVP refresh interval is modified to 5000mSec, a TE LSP will not be recovered followed a switchover.

  Conditions: This symptom occurs on Cisco IOS 12.2S and 12.0S releases that are supporting RSVP Graceful Restart help-neighbor mode.

  Workaround: Configure the RSVP refresh interval to 30 seconds (default value) or longer.

- CSCse01124

  Symptoms: The Hot Standby Router Protocol (HSRP) may not come up and may remain in the "Init" state, which can be verified in the output of the **show standby brief** command.

  Conditions: This symptom is observed when dampening is configured on a native Gigabit Ethernet interface of a Cisco 7200 series or on a Fast Ethernet interface of a PA-FE-TX port adapter. Other types of interfaces are not affected.

  Workaround: When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Gigabit Ethernet and Fast Ethernet interfaces of all routers of the standby group.

  To prevent the symptom from occurring, remove dampening from the Gigabit Ethernet and Fast Ethernet interfaces.

- CSCse09460

  Symptoms: Aggregate RAM is not programmed after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for QoS when the SSO switchover is initiated by a script.

  Workaround: There is no workaround.

- CSCse11678

  Symptoms: Removing a member link when there are 3 member links in the bundle causes ping failures.

  Conditions: This symptom is seen when the bundle must exists on a SIP1. The problem does not happen with a bundle on a FlexWan or Enhanced Flexwan.

  Workaround: Shut/No shut on the bundle.

- CSCse15728

  Symptoms: On a Cisco 7600 series router with a VPNSM (VPN Services Module), upon receiving IPSec packets with invalid SPI (Security Parameter Index), the router fails to send the peer device IKE DELETE NOTIFY messages, thus causing the encrypted traffic to be blackholed.

  Conditions: This symptom occurs on a Cisco 7600 series router with a VPN Services Module (VPNSM).

  Workaround: There is no workaround.

- CSCse21536

  Symptoms: It is possible for the tunnel path mtu discovery information to get out of sync between the route processor and VPN-SPA. This causes tunnel path-mtu discovery to stop working

  Conditions: This problem happens when tunnel path-mtu-discovery command is removed form the tunnel configuration when the tunnel interface is shut down. Once the tunnel is unshut, the GRE tunnel will not have the path mtu configuration, but VPN-SPA will have it and remember the last path mtu found. Path mtu discovery will not work after getting into this state, even if it is reenabled in the tunnel interface.

  Workaround: To get out of this state, the tunnel needs to be completely removed. It can later be added, and path mtu discovery will behave correctly.

- CSCse43316

  Symptoms: One cannot configure a Virtual Private Network Routing Forwarding Table with the Command Line Interface configuration command **ip vrf** *VPN_VRF_Instance_Name*. The error message

  ```
  %IP_VRF-3-VRF_CREATE_FAIL: VRF id alloc failure
  ```

  is returned in repsonse to the configuration command.

  Conditions: This symptom occurs whenever one attempts to define a Virtual Private Network Routing Forwarding Table instance in the configuration context.

  Workaround: There is no workaround.

- CSCse49846

  Symptoms: System takes more time to resume complete traffic flow after events like RPF change occurs. It looks to be a case of performance degradation in ION images.

  Conditions: The problem appears to be happening with 6708-10GE card in the path, but it is not exactly determined if 6708-10GE is the cause of this issue. Installation of entries in hardware appears to be taking more time than expected on RPF change events which causes more time for traffic to resume at expected rates.

  Workaround: There is no workaround.

- CSCse52755

  Symptoms: An ELMI link between a PE router and CE router may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router when the following conditions are present:

  – The PE router is configured with a SIP-400 that has a SPA with a Gigabit Ethernet interface that connects to the CE router.

  – The Gigabit Ethernet interface has an Xconnect-based Ethernet Virtual Circuit (EVC) configuration.

  Workaround: On the PE router, enter the **ethernet cfm enable** global configuration command.

Further Problem Description: The symptom occurs because the ELMI packets that are sent by the CE router and are destined for the PE router are tunneled to a remote side instead of being punted to the RP of the CE router.

- CSCse53002

  Symptoms: A memory leak occurs in the IPSec key engine process, and the output of the **show memory summary** command shows that the memory block that is used as "KMI num ipsec" is leaking.

  Conditions: This symptom is observed on a Cisco router when traffic is being processed.

  Workaround: There is no workaround.

- CSCse55425

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

  Conditions: The conditions under which the problem manifest itself are unknown, and appear to be random. The symptom exists only when using a channelized T3 card and configuring one of the T1s.

  Workaround: A router reload clears the issue.

- CSCse89861

  Symptoms: L2TP cannot be established via an authorization of the domain.

  Conditions: This symptom is observed when a domain is not authorized and when only the username@domain is sent, regardless of the configuration of the **vpdn authen-before-forward** router configuration command.

  Workaround: There is no workaround.

- CSCse95800

  Symptoms: WRED counters are not being updated.

  Conditions: This symptom is observed on a Cisco router when WRED is attached to the parent class and when the child class has a police statement.

  Workaround: There is no workaround.

- CSCsf24836

  Symptoms: A line card may crash, and the following error messages may be generated:

  ```
  %INTR_MGR-DFC4-3-INTR: Queueing Engine (Blackwater) [0]: IPM Invalid packet
  ID
  %ESM20-DFC4-3-UNEXPECTED_GLOBAL_INT: Unexpected Global Interrupt:
  Blackwater_0/Icewater_0 Error
  %DFCWLC-DFC4-2-UNRECOVERABLE_FAILURE: DFC WAN Line Card Unrecoverable Failure
  for Device: Queueing Engine (Blackwater)
  ```

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

  Workaround: Remove the SPAN configuration.

- CSCsf28509

  Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsf96592

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

  Symptoms 1: The input interface when switching the tunnel encapsulated packet remains set to the original input interface. When the encapsulated packet leaves the box through the same interface as the payload was originally received, ICMP Redirect messages might be generated in error.

  Conditions 1: This symptom exists when tunneled packets leave out of the interface the original payload was received on.

  Workaround 1: There is no workaround.

  Symptoms 2: TE tunnel adjacencies might miss the L2 encapsulation size in the byte counts.

  Conditions: This symptom applies to all MPLS/TE tunnels.

  Workaround 2: There is no workaround.

- CSCsg00673

  Symptoms: When you enter the **show memory statistics** command and query the same data via SNMP, the values do not match for transient memory.

  Conditions: This symptom is observed on a Cisco router that is queried via SNMP.

  Workaround: There is no workaround.

- CSCsg07870

  Symptoms: The new active supervisor engine may crash after an SSO switchover has occurred.

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

  Workaround: There is no workaround.

- CSCsg12385

  Symptoms: When the **ipv6 verify unicast reverse-path** command is enabled on an interface, the following error message may be generated:

  ```
  %COMMON_FIB-3-NOSWSBDECODE: No IPv6 uRPF subblock control decode function for
  GigabitEthernet2/0/10 (Pixar-2)
  ```

  Conditions: This symptom is observed in a configuration with a stack of two or more Cisco Catalyst switches or routers.

  Workaround: There is no workaround.

- CSCsg22981

  Symptoms: A router may crash because of a bus error when sending L2X data packets.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg26096

  Symptoms: When you enter the **hw-module reset** command on a 1-port CHOC-3/CHSTM-1 SPA that is installed in a Cisco 7600 series at the local end, the network clock at the remote end may become out-of-range (OOR), that is, the network clock goes beyond the acceptable limits of pps, without an error message being generated.

Conditions: This symptom is observed when the Network Clocking feature is configured on the 1-port CHOC-3/CHSTM-1 SPA.

Workaround: There is no workaround.

- CSCsg36725

  Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

  Conditions: This symptom is observed on a Cisco 10000 series but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg44331

  Symptoms: A router may crash when a policy map that is in use by sessions is modified while the sessions are disconnected.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

  Workaround: Clear all sessions before you modify the policy map.

- CSCsg44431

  Symptoms: A DHCP-initiated IP subscriber session may not respond to DHCP control packets.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the subscriber session has features enabled that affect the handling of the DHCP control packets.

  Workaround: Apply access control lists (ACLs) to the subscriber session to permit bidirectional DHCP control traffic between the ISG and the DHCP client. To do so, enter the **access-list** *access-list-number* **permit udp any any eq bootps** command.

- CSCsg44555

  Symptoms: An MPLS TE tunnel with a third-party vendor headend, a Cisco midpoint, and a Cisco tailend may occasionally transition to the up/down state on the midpoint while still appearing in the up/up state on the headend and tailend. When this situation occurs, traffic may continue to flow on the tunnel even though the tunnel is in the up/down state at the midpoint or it may come to a halt.

  Conditions: This symptom is observed when the Cisco router that is the tailend for the MPLS TE tunnel uses a bandwidth or burst size that is not a multiple of 1 Kbps or 1 Kbyte and that rounds up the Resv burst size to the next higher multiple of 1 Kbps or 1 Kbyte.

  Workaround: Specify a tunnel bandwidth that is a multiple of 8 Kbps.

- CSCsg53728

  Symptoms: A router may crash when an input service policy is attached to an interface.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for Control Plane Policing (CoPP) while traffic is flowing.

  Workaround: There is no workaround.

- CSCsg61922

  Symptoms: The **show l2tp session all vcid** command generates incorrect output.

  Conditions: This symptom is observed on a Cisco router that has an L2TPv3 tunnel.

  Workaround: There is no workaround.

- CSCsg70932

  Symptoms: A Cisco 7200 series that is configured for QoS may crash when traffic is sent.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2 and that has a Port Adapter Jacket Card in which a 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) in installed that has an interface with a service policy.

  Workaround: There is no workaround.

- CSCsg76546

  Symptoms: An attempt to attach a policy map to an ATM PVC or ATM interface may fail and a "policy-map not configured" error messages may be generated even though the output of the **show policy-map** command shows that the policy map is configured.

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for an ATM PVC or ATM interface on a SPA.

  Workaround: There is no workaround.

- CSCsg78729

  Symptoms: PE routers may not report an alarm indication signal (AIS) after the interface on a connected CE router is shut down. Instead of reporting an AIS, the PE routers report a loopback timeout.

  Conditions: This symptom is observed on routers when the following conditions are present:

  – The PE routers are connected through an L2TPv3 tunnel.

  – The CE router that is connected to one of the PE routers is connected to another CE router through a PVC.

  – OAM is enabled on all the routers.

  Workaround: There is no workaround.

- CSCsg83772

  Symptoms: When a prepaid service is automatically applied on account logon to a PPPoE session via RADIUS, the service may remain in a locked state even after the session has been cleared.

  Conditions: This symptom is observed when many PPPoE sessions are set up and brought down. To verify that the symptom has occurred, look at the output of the **show subscriber session** and **show sss server output** commands. If the output of the latter command shows a number greater than 1 for "SVM-Feature-Info", the symptom has occurred:

```
Service "biznes_xxx":
    Version 1:
      SVM ID                : 6C0001E7
      Child ID              : B40001EA
      Locked by             : SVM-Feature-Info       [15]
      Locked by             : SVM-Printer            [1]
      Locked by             : TC-Child               [1]
```

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

- CSCsg85441

  Conditions: When you configure a large number of individual PVCs (about 52,000) and enter the **show running-config** command, it may take about 50 seconds before the command output is displayed.

Symptoms: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may also affect other platforms.

Workaround: There is no workaround.

- CSCsg89189

  Symptoms: A router may reload when you enter the **show subscriber session detailed** command while sessions are being modified.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not enter the **show subscriber session detailed** command while sessions are being modified.

- CSCsg90929

  Symptoms: When you configure MR-APS between a Cisco 7304 and another router such as a Cisco 7500 series or Cisco 7600 series with PA-MC-STM-1 port adapters, the following tracebacks are logged on the Cisco 7304:

  ```
  -Process= "APS process", ipl= 0, pid= 191
  -Traceback= 406DC2E0 40741174 400C24BC 400C2BF0 400C6D9C 400C79EC 400C8814
  400C8894 400C90B8
  ```

  Conditions: This symptom is observed on a Cisco 7304 when the working or protect PA-MC-STM-1 port adapter in the active state.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs with the following Cisco IOS software images:

  On the Cisco 7304:

  - Release 12.2(27)SBC5 (PGP ver.4)
  - Release 12.2(28)SB5 (PGP ver.4)

  Note that Release 12.2S could also be affected.

  On the Cisco 7600 series:

  - Release 12.2(18)SXD5 (PGP ver.3)
  - Release 12.2(33)SRA1 (PGP ver.4)

- CSCsg91545

  Symptoms: A warning message is seen on SP:

  ```
  %MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST: ACL TCAM inconsistency seen at index XXX
  ```

  Conditions: This symptom occurs with certain configurations after a switchover. Also when IPv6 ACLs are applied and removed from the interface.

  Workaround: This is a warning message and no workaround is required.

  Further Problem Description: This message indicates that the ACL TCAM consistency checker has detected and fixed a discrepancy between the software shadow copy of the TCAM and the hardware. This occurs because some fields in the TCAM entry may not be cleared in the hardware. (This will not cause any issue as entries will be corrected by consistency checker.)

- CSCsg95072

  Symptoms: The **show atm vc** command may be missing VCs.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or a rebuild of Release 12.2(31)SB when at least one ATM line card is installed and VCs are configured.

Workaround: You can display the ATM VC information by using a more specific command: enter the **show atm vc interface atm** *card/subcard/port* command.

Further Problem Description: The missing VCs tend to be from select ATM subinterfaces.

- CSCsg96495

  Symptoms: An error message of type is seen: IDBINDEX_SYNC-3-IDBINDEX_ENTRY_SET for an interface. And the **show idb** command shows an if- index value of -1 for one or more IDBs on either the Standby or Active RP.

  If this happens on a Standby RP, there is no effect on traffic. However if the RP switches over to become Active, it will prevent traffic from flowing on the affected interfaces.

  Conditions: This symptom is most likely to happen if a platform has a bug such that OIR insertion notifications are synced to the Standby RP before the corresponding interface index values have been synced. The normal order is to always guarantee the index values arrive first.

  Workaround: If this happens on an HA protected Active RP (which affects traffic), check whether the Standby RP has good if-index values for all interfaces by running the **show idb** EXEC command on the Standby RP. If so, then do an RP switchover, so the RP with good interface indexes becomes the Active RP.

  If the Standby RP shows this symptom, reload the Standby RP and check that after it comes up, it has good interface index values, which should happen in most cases.

  Further Problem Description: This DDTS is to provide a platform-independent code workaround that allows the interface index values to self-recover after the correct if-index values are synced to the Standby RP.

  If the condition is seen on an Active RP, this DDTS fix will allow it to recover following an OIR deletion/insertion rather than remaining in the error condition.

  The root-cause of the incorrect syncing order will still need to be fixed by the platform that has this symptom. But this DDTS will lower the severity by allowing it to self-recover in most cases on its own without user intervention.

- CSCsg97717

  Symptoms: The PXF engine of an NSE-150 crashes when you enter the **ip pim bidir-enable** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for MVPN with a single VRF when multicast traffic is flowing through this VRF.

  Workaround: There is no workaround.

- CSCsg99331

  Symptoms: The **show host** command will not show full host name.

  Conditions: In case of hostname is used, only the first character on the host name is displayed or used in the query.

  Workaround: There is no workaround.

- CSCsh01626

  Symptoms: A “%SYS-2-MALLOCFAIL” error message may be generated, indicating that there is no free memory available in the router.

Conditions: This symptom is observed only on a Cisco 7200 series that is configured with an NPE-G2 and that runs a Cisco IOS software image that is based on Release 12.2S.

Workaround: There is no workaround. To clear the symptom, reboot the router.

- CSCsh04911

  Symptoms: On a Cisco 7304 that is configured for AToM, a software-forced reload may occur on an NSE-100.

  Conditions: This symptom is observed when egress NetFlow is configured on an AToM attachment circuit.

  Workaround: There is no workaround.

  Further Problem Description: The configuration that is stated in the Conditions is essentially a misconfiguration. NetFlow can collect information only about Layer 3 IP packets. However, the AToM attachment circuit is transmitting Layer 2 frames, so the egress NetFlow is not valid.

- CSCsh05677

  Symptoms: A Cisco device that is running Cisco IOS configured with MPLS and Netflow may show all traffic out an interface being process switched. This will cause high CPU under the IP Input process.

  Conditions: This issue is seen when **ip flow ingress** is configured on any interface on the device, and MPLS is also enabled. All traffic out of the MPLS enabled interface will be process switched as evident in the **show interface statistic** command.

  Workaround: Enable MPLS aware netflow via the **ip flow-cache mpls label-positions 1** command. This will prevent the process switching of traffic. However additional MPLS fields will be added to the netflow export records.

- CSCsh07031

  Symptoms: L2TP connectivity may not function across the native Gigabit Ethernet interface of an NPE-G2.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 when EIGRP is configured as the routing protocol.

  Workaround: There is no workaround.

- CSCsh12653

  Symptoms: When an ISG receives VSAs that cannot be parsed by the SIP parser, the ISG disconnects the established session and does not respond with a CoA Nak message.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when an incorrect VSA is sent via a CoA message and when the SIP parser returns a DENY message to the ISG.

  Following are examples of incorrect VSAs:

  - a vc-weight that is larger than the maximum that is allowed: cisco-avpair = “atm:vc-weight=3000”
  - a non-existent service-policy name: cisco-avpair = “atm:vc-qos-policy-out=non_exist_policy” cisco-avpair = “atm:vc-watermark-max=1”

  Workaround: There is no workaround.

- CSCsh13739

  Symptoms: The usage of the PXF engine increases to 100 percent. This situation may cause interface flapping, error messages that state that OSPF neighbors are unreachable, and a failure of the standby processor.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with either an NSE-100 or an NSE-150, that has a POS interface that is configured for Frame Relay and that has an output shaping service policy, and that receives traffic that matches the output shaping service policy. In addition, the router is configured with a cross-connect, more specifically, an interface that is configured for Xconnect service and that is connected to a remote peer.

  Workaround: There is no workaround.

- CSCsh15456

  Symptoms: A router may crash when you remove a QoS policy from an interface or modify the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure a QoS policy, attach it to the interface, run traffic, and then, after a long time, remove the QoS policy or modify the policy map.

  Workaround: There is no workaround.

- CSCsh15817

  Symptoms: IP SLA operations on a router that has a response time reporter (RTR) enabled may fail at the source. The UDP socket events are not received by the RTR responder process, and the UDP socket events are missing when a UDP packet is routed through a VRF.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.2SB. You can verify that the symptoms are occurring through any of the following commands:

  - debug rtr trace
  - debug ip udp
  - debug socket

  Workaround: Use IP SLA operations without VRFs.

- CSCsh27931

  Symptoms: A platform may crash when an arithmetic exception crash occurs. Before this situation occurs, the following error message is generated:

  ```
  %COMMON_FIB-SP-4-UNEQUAL: Ratio of unequal path weightings (1 1 40 ) prevents
  oce IP adj out of GigabitEthernet3/2, <ip addr> from being used.
  ```

  Conditions: This symptom is observed on a Cisco platform that functions in an IS-IS configuration when TE tunnels are shut down.

  Workaround: There is no workaround.

- CSCsh28556

  Symptoms: When configuring frame relay queueing, bandwidth is taking 28kbps, and more than 28 kbps cannot be configured.

  Conditions: This symptom happens only when service policy is applied under map- class frame-relay and then binding it under the DLCI with frame-relay traffic shaping enabled under the interface.

  Workaround: There is no workaround.

- CSCsh28899

  Symptoms: IS-IS routes are not learned at remote sides.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when the router connects to the remote sides through a native Gigabit Ethernet (GE) interface.

  Workaround: Do not use a native GE interface. Rather, use a GE port adapter such as the PA-GE.

- CSCsh34529

  Symptoms: An ATM interface configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure an ATM main interface on a SPA.
  2. You configure PVCs on the ATM main interface.
  3. You shut down the SPA.
  4. You reload the standby supervisor engine and wait until it comes up.
  5. You bring up the SPA from the active RP.

  At this point, the ATM interface configuration is lost on the standby RP.

  This symptom is observed with both 8-port OC-3c/STM-1 ATM SPAs and Circuit Emulation over Packet (CEoP) SPAs.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh37008

  Symptoms: If the chassis is WS-C6509-NEB-A or CISCO7609 with one fan, the system cooling capacity is 76cfm. WS-X6708-10GE module requires 84cfm cooling capacity. It would be powered down by default.

  Conditions: This symptom is observed on WS-C6509-NEB-A or CISCO7609 chassis with one fan, and system has WS-X6708-10GE inserted.

  Workaround: User can add the following configuration if running image without this fix:

  Router(config)#environment temperature-controlled

- CSCsh45466

  Symptoms: A memory leak may occur on a router that is configured with IP ACLs.

  Conditions: This symptom is observed when you enter the **show access-list** command to see a list of ACLs that contains dynamic elements.

  Workaround: There is no workaround.

- CSCsh51778

  Symptoms: An ISG that receives incorrect VSAs for a policy map may no longer accept any VSAs even if the VSAs are correct.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that runs Cisco IOS Release 12.2(28)SB, Release 12.2(31)SB, or Release 12.2(31)SB1.

  Workaround: There is no workaround.

- CSCsh54999

  Symptoms: A router may crash when the dynamic ACL timer expires.

Conditions: This symptom is observed on a Cisco router only when the **show access-list** command is entered before the timer expires.

Workaround: There is no workaround.

- CSCsh55768

  Symptoms: All packets received by a Cisco Catalyst 3550 Switched Virtual Interface (SVI) are dropped. In the output of the **show interfaces** command for the SVI, the number of packets in the SVI input queue reaches the maximum number and the input queue drop counter increments.

  Conditions: All of the following conditions must be true for the problem to occur:

  - The switch is a Cisco Catalyst 3550 switch.
  - The Cisco IOS software feature set is IP Base or IP Base Crypto.
  - The Cisco IOS software version is Release 12.2(35)SE, Release 12.2(35)SE3, or Release 12.2(35)SE5.
  - IP routing is enabled.
  - The switch SVI interface receives certain IP multicast packets. Examples of applicable packets are EIGRP or RIPv2 packets.

  Workaround: Any of the following items are a workaround:

  - Upgrade the switch software to Cisco IOS Release 12.2(37)SE.
  - With affected Cisco IOS versions, do not use the IP Base or IP Base Crypto feature set. The IP Services and IP Services Crypto feature sets are not affected.
  - Downgrade the switch software to a Cisco IOS release prior to Release 12.2(35)SE.
  - Configure an access list to block the offending IP multicast packets.
  - Configure a passive interface on the router adjacent to the switch to prevent the receipt of EIGRP or RIPv2 packets by the switch SVI.

- CSCsh57509

  Symptoms: A Cisco router that is configured for RIPv2 may not delete a path from the routing table when it should do so.

  Conditions: This symptom is observed after the router has learned multiple paths for a prefix with different next hops from one neighboring router and after the neighboring router stops advertising one of the paths.

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

- CSCsh57611

  Symptoms: Frame Relay end-to-end keepalives may unexpectedly time out.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2(31)SB2.

  Workaround: There is no workaround.

- CSCsh59375

  Symptoms: A DHCP interface may not be switched when you enter the **ip dhcp smart-relay** command.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS interim Release 12.4(12.15a) and that is configured for MPLS VPN.

  Workaround: There is no workaround.

- CSCsh66935

  Symptoms: A router crashes in avl_get_next_threaded.

  Conditions: This symptom happens in extremely rare cases when deleting many tunnels with tunnel protection enabled.

  Workaround: There is no workaround.

- CSCsh68976

  Symptoms: A small memory leak is observed when any of the following commands is issued:

  - **show hw-module** *slot* **transceiver 0 idprom brief**
  - **show hw-module** *slot* **transceiver 0 idprom detail**
  - **show hw-module** *slot* **transceiver 0 idprom dump**

  Conditions: This symptom occurs when the above commands are issued.

  Workaround: Do not issue these commands:

  - **show hw-module** *slot* **transceiver 0 idprom brief**
  - **show hw-module** *slot* **transceiver 0 idprom detail**
  - **show hw-module** *slot* **transceiver 0 idprom dump**

- CSCsh69341

  Symptoms: In a Server Load Balancing (SLB) configuration, input features (except for Policy Based Routing [PBR]) that should not be processed are unexpectedly executed in a special switching path.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch that runs Cisco IOS Release 12.2SXH and on a Cisco 7600 series that runs Release 12.2SXH or Release 12.2(33)SRB and that are configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom may cause SLB to behave in an unexpected way. For example, when an input access control list (ACL) is applied on an interface, SLB is supposed to bypass the ACL, which is considered an input feature, so SLB packets can reach their destination without a problem. However, because of the symptom, the ACL is active and may stop SLB packets from reaching their destination.

- CSCsh74270

  Symptoms: A router may crash when you attach a map class to a Frame Relay data-link connection identifier (DLCI) interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output service policy with a priority kbps/percentage value.

  Workaround: There is no workaround.

- CSCsh76558

  Symptoms: The **show stacks** command on any router platform that uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the **show stacks** output is printed.

  Conditions: The problem is seen when a **show stacks** command is issued or when any other command that causes this command to be executed (for example, **show tech-support**) is issued. This is seen in router platforms that have IPC processes.

  Workaround: There is no workaround.

- CSCsh85531

  Symptoms: Some E1 channels may remain down after you have reloaded a router.

  Conditions: This symptom is observed on a Cisco 7200 series that function as a PE router and that connects to a CE router. Both routers are connected through 1-port multichannel STM-1 (PA-MC-STM-1) port adapters, and the **framing no-crc4** command is enabled on all interfaces of both routers.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of the PA-MC-STM-1 at the PE side to enable all interfaces to come up.

- CSCsh92854

  Symptoms: When the **ip cef** command is enabled, output bytes of a virtual-access interface do not increment correctly.

  Conditions: This symptom is observed on a Cisco router that has a PPPoVPDN virtual-access interface when the VPDN traffic is sent over an ATM interface. The symptom does not occur when the VPDN traffic is sent over a Gigabit Ethernet interface.

  Workaround: If this is an option, disable CEF on the interface from which the VPDN traffic is switched. However, doing so may affect the performance of the platform. If this is not an option, there is no workaround.

- CSCsh93436

  Symptoms: Layer 2 Tunnel Protocol version 3 (L2TPv3) will have transport problems, which may include an inability to receive packets from the transport layer.

  Conditions: When this symptom is present, L2TPv3 tunnels will not come up.

  Workaround: There is no workaround.

- CSCsh93517

  Symptoms: SCTP may have transport problems, which may include an inability to receive packets from the transport layer.

  Conditions: This symptom occurs when SCTP has transport problems.

  Workaround: There is no workaround.

- CSCsh93653

  Symptoms: A router crashes when you configure a local ISG service policy with any routing protocol such as BGP or ISS.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 when you enter the following commands:

  ```
  Router(config)# router bgp 1
  Router(config-router)# service
  Router(config-router)# policy-map type service <policy-map-name>
  Router(config-service-policymap)# service local
  ```

  Workaround: Configure and download service profiles via a RADIUS server.

- CSCsh94637

  Symptoms: An NPE-G1 may crash because of a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address TLB (store) exception, CPU signal 10,
  PC = 0x61F1D0D0
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 and that is configured for L2TP. The symptom may not be platform specific.

Workaround: There is no workaround.

- CSCsh95788

  Symptoms: A router that is running Cisco IOS software may unexpectedly restart.

  Conditions: This symptom can occur when the following interface mode command is removed:

  ipv6 nd prefix framed-ipv6-prefix

  Workaround: There is no workaround.

- CSCsh96662

  Symptoms: There are no label forwarding entries for VPNv6 prefix on Inter-AS option B boundary.

  Conditions: This symptom occurs when the VPNv6 prefix is learned from an IPv4 neighbor (not IPv6 enabled).

  Workaround: Switch the neighbor to peer through IPv6.

- CSCsh98088

  Symptoms: PDSN is reloaded when the **no vpdn-group CDMA** command is configured.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T PDSN software when **source-ip** is configured in the **vpdn-group** subcommand.

  Workaround: Use the global **vpdn source-ip** command instead of the **source-ip** command that is configured within the individual VPDN groups.

- CSCsi00136

  Symptoms: Cisco IOS software fails to properly detect the presence of NAT with some implementation, leading to unsuccessful phase 1 or phase 2 establishment.

  Conditions: This symptom occurs when the remote peer sends more than 2 NAT-D (NAT DISCOVERY) payload in the phase 1 establishment.

  Workaround: There is no workaround.

- CSCsi03714

  Symptoms: A router may crash when a DLCI configuration is removed from an MFR subinterface.

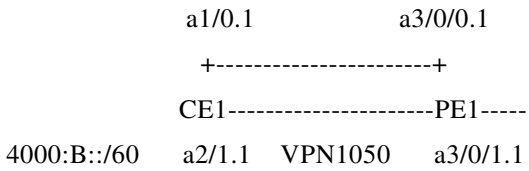
  Conditions: This symptom is observed on a Cisco 7200 series when the MFR interface has a map class with a service policy attached.

  Workaround: There is no workaround.

- CSCsi07822

  Symptoms: When using the IPv6 VPN over MPLS (6VPE) capability and EBGP multihop where loadsharing is being done on the VRF. If one of the loadsharing paths on the PE is flapped, loadsharing across the appropriate paths may no longer occur. This is because the RIB is unable to resolve the route to the next hop via the flapped interface.

  Conditions: Assuming we have the topology below and eBGP multihop loadsharing is being done by PE1:



332:332:332::332/128 444:444:444::444/128

EBGP multihop session between PE1 and CE1 via loopback addresses 444:444:444::444/128 and 332:332:332.332/128 respectively.

################################
Loadsharing before the interface flap
################################

```
PE1# show bgp vpnv6 unicast vrf VPN1050 4000:B:0:270::/60

BGP routing table entry for [1050:1]4000:B:0:270::/60, version 3760 Paths: (1
available, best #1, table VPN1050) Advertised to update-groups: 1 3510 102
332:332:332::332 (FE80::217:95FF:FEE4:1A90) from 332:332:332::332 (10.1.1.32) Origin
IGP, localpref 100, valid, external, best Extended Community: RT:1050:1 mpls labels
in/out 13509/nolabel

PE1#
PE1# show ipv6 route vrf VPN1050 4000:B:0:270::/60

Routing entry for 4000:B:0:270::/60 Known via "bgp 6777", distance 20, metric 0, type
external Route count is 1/1, share count 0 Routing paths: 332:332:332::332 Last
updated 02:17:03 ago
PE1#
```

###
Let's look at the RIB for the next hop; we should see both paths.
###

```
PE1# show ipv6 route vrf VPN1050 332:332:332::332

Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0
Redistributing via bgp 6777 Route count is 2/2, share count 0 Routing paths:
2004:1000:9250:A910::2 Last updated 00:48:21 ago 2006:106:106:2006::2 Last updated
00:00:20 ago
```

################################
CEF looks good as shown below
################################

```
PE1# show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail

4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via
332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via
2004:1000:9250:A910::/64 attached to ATM3/0/0.1 recursive via 2006:106:106:2006::2
recursive via 2006:106:106:2006::/64 attached to ATM3/0/1.1
PE1#
```

Now shut down one of the interfaces on PE1

```
PE1(config)# int a3/0/1
PE1(config-if)# sh
PE1(config-if)# end
PE1#
```

###
CEF now only has one recursive output chain to the destination after the interface is shut down - Good
###

```
PE1# show ipv6 cef vrf VPN1050 4000:B:0:270::/60 detail

4000:B:0:270::/60, epoch 24 local label info: other/13509 recursive via
332:332:332::332 recursive via 2004:1000:9250:A910::2 recursive via
2004:1000:9250:A910::/64 attached to ATM3/0/0.1
```

```
PE1#

##############################################
Now bring back up the a3/0/1 interface and observe CEF
##############################################

PE1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
PE2(config)# int a3/0/1
PE2(config-if)# no sh
PE2(config-if)# end
PE1#

#############################################################################
Let's see if RIB and CEF have resolved the next hop via this interface - It does not as demonstrated
below
#############################################################################

PE1# show ipv6 route vrf VPN1050 332:332:332::332

Routing entry for 332:332:332::332/128 Known via "static", distance 1, metric 0
Redistributing via bgp 6777 Route count is 1/1, share count 0 Routing paths:
2004:1000:9250:A910::2 Last updated 00:56:35 ago

PE1# show ipv6 cef vrf VPN1050 332:332:332::332/128 detail

332:332:332::332/128, epoch 24 local label info: other/3305 1 IPL source [no flags]
Dependent covered prefix type inherit cover NULL recursive via 2004:1000:9250:A910::2
recursive via 2004:1000:9250:A910::/64 attached to ATM3/0/0.1
PE1#
```

Workaround: Toggle the associated CE interface a few times.

- CSCsi12104

  Symptoms: When you repeatedly change active routers by enabling preemption and then change the priorities on the router interface, the router may crash.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.5)T after you have shut down the interface of the active router.

  Workaround: There is no workaround.

- CSCsi14211

  Symptoms: A CPUHOG condition may occur when an LDP session goes down.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP, that has more than 30 LDP sessions with peers, and that exchanges more than 5000 label bindings for each LDP session. The symptom occurs when the LDP session goes down shortly after it comes up.

  Workaround: There is no workaround.

- CSCsi15221

  Symptoms: A Cisco 7200 series with an NPE-G2 may hang during the boot process.

  Conditions: This symptom is observed when several native Gigabit Ethernet ports with "MV64460" hardware come up simultaneously, for example, while the router boots. To verify if the Gigabit Ethernet ports of your router have "MV64460" hardware, look in the output of the **show interfaces** command.

  Workaround: There is no workaround.

- CSCsi17158

  Symptoms: Catalyst Series 4xxx and 35xx switches that run Cisco IOS software may crash with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions.

  Conditions: This symptom occurs when an SSH server is enabled.

  Workaround: This vulnerability can be mitigated. For Cisco IOS software, the SSH server can be disabled by applying the **crypto key zeroize rsa** command 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 software may also be disabled by 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 through the use of access control lists (ACLs) on the VTY lines as shown at the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

  More information on configuring ACLs can be found on Cisco’s public website:

  http://www.cisco.com/warp/public/707/confaccesslists.html

  An example of a VTY access list can be found below:

  access-list 2 permit 10.1.1.0 0.0.0.255

  access-list 2 deny any

  line vty 0 4 access-class 2 in

  end

- CSCsi19924

  Symptoms: Ping failures with MLPPP are seen on an SPA-8XCHT1/E1.

  Conditions: This symptom occurs when MFR with xconnect/ATOM and MLPPP are configured on the same SPA on a Cisco 12000 series platform.

  Workaround: Reload the SPA.

- CSCsi21733

  Symptoms: An SPA-2XOC48POS/RPR goes to Out Of Service after encountering an SPA BUS ERROR. TRANSCEIVER-6-REMOVED messages are followed by an SCC failure, resulting in the SPA going to Out Of Service.

  Conditions: This symptom occurs when there are many L1 errors (B2-BER) found on the link and when the interfaces flap many times before the BUS ERROR.

  Workaround: Reload the LC.

- CSCsi22585

  Symptoms: DNS requests from a PC client may time out.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG, that is located between a PC and a DNS server, and that redirects DNS requests to a local DNS server.

Workaround: There is no workaround.

- CSCsi23968

  Symptoms: When IKE phase 1 is cleared and IPSec requests a rekey, IKE fails to rekey.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(13.5)T. IKE rekeys phase 1 after two attempts instead of five attempts. IKE does rekey successfully within the time frame of two attempts. However, when the network connection to the peer is down and not restored within the time frame of two attempts, the rekey fails. In this situation, IKE should make five attempts. Note that the symptom is not release specific.

  Workaround: There is no workaround.

- CSCsi25578

  Symptoms: When a Cisco IOS LNS router receives a L2TP Incoming Call Request (ICRQ) message with same assigned session ID as an existing session of another tunnel from the same LAC, it disconnects the session because of unknown Attribute-Value Pair (AVP).

  Conditions: This symptom occurs under the following conditions:

  – When L2TPv2 is used.

  – When the LAC is not a Cisco router that reuses the same session immediately for different tunnels. (A Cisco LAC will always advance the session even it is for a different tunnel. It is rare to run across this condition.)

  Workaround: There is no workaround.

- CSCsi28462

  Symptoms: A router may reload when using SASL.

  Conditions: This symptom occurs when SASL is being used. Some of the affected commands include:

  bingd device *port* **sasl profile** *sasl-profile*

  bingng device *host port* **sasl user** *user* **password** *password*

  netconf beep listener *port* **sasl** *sasl-profile*

  netoconf beep initiator *host port* **user** *user* **password** *password*

  Workaround: There is no workaround.

- CSCsi30780

  Symptoms: ATM Stateful Switchover (SSO) takes more than 5 seconds.

  Conditions: This symptom occurs when ATM traffic is sent and an SSO is done.

  Workaround: There is no functionality breakage.

- CSCsi30993

  Symptoms: The output of the **show vtemplate** command shows an inaccurate number of active interfaces and subinterfaces.

  Conditions: This symptom is observed on all platforms that are running Cisco IOS Release 12.2SB software and using any feature that requires the use of Virtual-Access interfaces.

  Workaround: There is no workaround.

- CSCsi31041

  Symptoms: When the **service local** command is configured under a policy map, service is denied.

Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured for AAA.

Workaround: There is no workaround.

- CSCsi32790

  Symptoms: When both sides of a CE are configured with “pvc-oam manage” and an interface on the PE is shut down, the CE side does not detect that the interface went down.

  Conditions: This symptom occurs when both sides of a CE are configured with “pvc-oam manage” and an interface on the PE is shut down.

  Workaround: The ATM OAM TIMER process had got deleted because of a return inside the while loop. The return statement is changed to continue, and the function micro_block_get_or_alloc() is used instead of micro_block_get().

- CSCsi40658

  Symptoms: With a Cisco 7600 configured for xconnect with interface vlan, a crash may happen when the interface vlan is unconfigured, with a **no interface vlan** *num* command.

  Conditions: This symptom occurs only when there are a large number of pseudowires configured.

  Workaround: There is no workaround.

- CSCsi42061

  Symptoms: When I try to do the bundle configuration on an ATM interface, I see that the random-detect attach red-test command is not accepted.

  Conditions: Configure ATM bundle, attach PVC, and then we see that the random detect command is not recognized.

  Workaround: There is no workaround.

- CSCsi43776

  Symptoms: Some CLI commands on any router platform that supports ISSU and uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the place where the process name would be printed.

  Conditions: This symptom is seen in router platforms that have ISSU related IPC processes. The bug ID CSCsh76558 fixed this issue for the **show stacks** command. This bug tracks a more generic fix.

  Workaround: There is no workaround.

- CSCsi45831

  Symptoms: There may be a delay in the creation of IP sessions over an interface that is configured for QinQ support.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the **initiator dhcp class-aware** command is enabled to place the clients in a specific VRF.

  Workaround: There is no workaround.

- CSCsi46028

  Symptoms: On routers that are configured for WCCP, interfaces that are connected to the content engine can become wedged.

  Conditions: This issue was introduced by CSCuk61396; only the images that have the fix for CSCuk61396 are affected by this issue.

  Workaround: There is no workaround. If an interface gets wedged, the only way to recover the system is to do a reload.

- CSCsi46897

  Symptoms: PPP may crash when an **snmpwalk** command is executed on the cbQosSetStatsTable object.

  Conditions: This symptom is observed when a service policy with a child policy that contains marking (“set”) actions is applied to an interface before the **snmpwalk** command is executed on the cbQosSetStatsTable object of the CISCO-CLASS-BASED-QOS-MIB.

  Workaround: There is no workaround.

- CSCsi48273

  Symptoms: L2VPN Local switching configs are not synced to the standby on reload on both active and standby PRE-2.

  Conditions: This symptom occurs only on reload of both the active and the standby.

  Workaround: There is no workaround.

- CSCsi49907

  Symptoms: A memory leak may cause a slow response and timeouts during the setup of new IP sessions, and the connection speed for established sessions may be very slow. To verify that there is a memory leak, enter the **show memory debug leak summary** command, and look for “Alloc PC” in the output.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 and that has the following configuration commands under a BVI or on an IP interface:

  service-policy type control XXXX

  ip subscriber routed

  initiator dhcp class-aware

  Workaround: There is no workaround.

- CSCsi51014

  Symptoms: Disk access freezes a router.

  Conditions: This symptom occurs after some fsck execution.

  Workaround: Format the disk, but all the content in disk is lost.

- CSCsi52268

  Symptoms: A router may run out of memory when you scale sessions with QoS and distribute them among a large number of subinterfaces.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 10000 series with a PRE3 that is configured for Hierarchal Queuing Framework (HQF). The symptom is not platform-specific. The symptom occurs when the following conditions are present:

  - Sessions are being scaled.
  - Per-session shaping and/or queuing is configured.
  - The number of sessions per subinterface is small.
  - Hierarchical queuing policy maps on sessions with aggregate shaping are configured, meaning that the subinterfaces are shaped as well. The subinterfaces are either shaped VLAN-QinQ subinterfaces or shaped ATM VC subinterfaces.

  Workaround: There is no workaround.

- CSCsi53232

  Symptoms: The active IMA link flaps when the IMA interface is down because of insufficient active links.

  Conditions: This symptom is observed on an IMA interface configured on a CEM SPA on a Cisco 7600 platform connected to a 7200 T1-IMA PA at the other end.

  Workaround: There is no workaround.

- CSCsi53353

  Symptoms: IPv6 EBGP sessions fail with the following message in "debug bgp events":

  ```
  %BGP-4-INCORRECT_TTL: Discarded message with TTL 32 from <ip>
  ```

  Conditions: This symptom occurs when BTSH is configured between the peers.

  Workaround: Disable BTSH between the IPv6 peers.

- CSCsi53469

  Symptoms: A router may hang for approximately 7 minutes.

  Conditions: This symptom is observed when you attempt to configure the **range pvc** command in a manner that exceeds the interface limit.

  Workaround: There is no workaround.

- CSCsi57207

  Symptoms: A bus error crash is seen on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen when PPPoE/PPPoA is configured with PPP idle timeout and PPP keepalive.

  Workaround: There is no workaround.

- CSCsi60103

  Symptoms: When you perform an online insertion and removal (OIR) to replace a port adapter, you may not be able to configure IPv6 on an interface of the newly inserted port adapter.

  Conditions: This symptom is observed when the newly inserted port adapter has an overlapping namespace with the port adapter that was replaced, for example, when a 1-port Fast Ethernet (FE) port adaptor is replaced by a 2-port FE port adaptor.

  Workaround: First unconfigure IPv6 on the interface of the port adapter that is to be replaced before you perform an OIR.

  Further Problem Description: The symptom is not observed when you perform an OIR to replace a port adapter with the exact same type of port adapter.

- CSCsi60125

  Symptoms: For TCP flows (typically short lived) being NATed at connection rates of about and over 100 connections per second, incorrect NetFlow translations are seen. One would see TCP RSTs generated by the TCP endpoints (e.g. server). We have noticed two NetFlow shortcuts pointing to the same adjacency.

  Conditions: Static NAT on PFC3A or PFC3B or PFC3BXL or PFC3C based systems (e.g. SUP32 or Sup720).

  Workaround: Keep the connection rate to below 100 connections per second, and if more performance is required, consider using Firewall Service Module (FWSM) to do NAT.

- CSCsi76569

  Symptoms: A Cisco router may crash during bootup or while writing or erasing the configuration during the “flow_def_master_list_lookup” process.

  Conditions: The symptom occurs during bootup or when a configuration is written to or erased from memory. The symptom may also occur when you enter the **show running-config** command.

  Workaround: There is no workaround.

- CSCsi76936

  Symptoms: A router may crash when the **debug glbp** command is enabled.

  Conditions: This symptom occurs only when GLBP receives a packet from a group that is not configured locally.

  Workaround: Do not enable GLBP debug.

- CSCsi78785

  Symptoms: A router may crash when a policy map is unconfigured.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay Traffic Shaping.

  Workaround: There is no workaround.

- CSCsi82166

  Symptoms: A router may reload during SASL authentication.

  Conditions: This symptom is observed when SASL authentication is performed while the **sasl** command is changed. For example, the symptom may occur when a BEEP session that uses SASL is performing authentication while the **sasl** command is being unconfigured.

  Workaround: Do not configure or unconfigure SASL when SASL authentication is being performed.

- CSCsi82427

  Symptoms: A ping may fail when a native Gigabit Ethernet interface functions in “speedauto,” duplex auto,” and “no neg auto” mode and when the peer interface functions in “fixed speed” and “duplex” mode.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when the interfaces are connected back-to-back via an RJ-45 cable.

  Workaround: Configure the same speed and duplex mode on both interfaces.

- CSCsi85384

  Symptoms: A flexwan may fail to boot the modules, and error messages similar to the following might be observed:

  ```
  SLOT 3/1: 00:00:19: %XDR-3-XDROOS: Received an out of sequence IPC message. Expected
  0 but got 26
  ```

  Conditions: The Cisco 7600 is running a 12.2(32)SRB2 image; this is occurring on an Enhanced flexwan with PA-MC-E3 port adapters.

  Workaround: There is no workaround.

- CSCsi85532

  Symptoms: A Cisco 851 that is running the c850-advsecurityk9-mz.124-11.T1 image is crashing with an Unexpected exception to CPU: vector 300.

  Conditions: The router crashes if not specifying pw-class in the pseudowire on interface Virtual-PPP1.

Workaround: Specify pw-class in the pseudowire.

- CSCsi90461

  Symptoms: If many L2TP sessions are brought up and down again continuously, the following error messages will be displayed on the console:

  ```
  %L2TP-3-ILLEGAL: _____:_____: ERROR: [l2tp_session_get_l2x_cfg::241], -Traceback=
  0x121FE88 0x25394E8 0x2539730 0x25558CC 0x2555FA0 0x254C0C4 0x254BB88 0x254BCD8
  0x254BDD8 0x2554040 0x2548250 0x2541E50 0x2541F6C 0x7D6510 %L2TP-3-ILLEGAL:
  _____:_____: No session config, -Traceback= 0x121FE88 0x25394E8 0x2539748 0x25558CC
  0x2555FA0 0x254C0C4 0x254BB88 0x254BCD8 0x254BDD8 0x2554040 0x2548250 0x2541E50
  0x2541F6C 0x7D6510
  ```

  Conditions: This symptom happens in both VPDN and Xconnect applications.

  Workaround: Reload the router.

- CSCsi92079

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

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

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

  - Use a prefix list for traffic class 100.1.1.0/24
  - Use an ACE for traffic class 100.1.1.0/24 DSCP af11

- CSCsi93020

  Symptoms: A router may crash when it functions as a LAC with a single PPPoE session that is locally terminated and when a service policy contains CoS marking or any other non-supported configuration.

  Conditions: This symptom is observed under the following conditions:

  1) Attach the policy to both the outbound and inbound interfaces of the virtual template.

  2) Unconfigure the policy from the outbound and inbound interfaces of the virtual template.

  3) Re-attach the policy to the outbound interface of the virtual template.

  Workaround: There is no workaround.

- CSCsj00571

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

  ```
  SPA_IPSEC-3-PWRCYCLE: SPA (<slot/subslot>) is being power-cycled (Module not
  responding to keep-alive polling) SPA_OIR-3-RECOVERY_RELOAD: subslot <slot/subslot>:
  Attempting recovery by reloading SPA ACE-6-INFO: SPA-IPSEC-2G[<slot/subslot>]: Crypto
  Engine X going DOWN
  ```

  Conditions: The conditions are as follows:

  - Large outbound packets (approx > 3500 bytes) undergo fragmentation first.
  - Followed by smaller outbound packets (approx > 1900 bytes) undergo fragmentation next.

  Workaround: Restrict the large packets going the VPNSPA by setting smaller MTUs.

- CSCsj01310

  Symptoms: With VRF configured, TCP probes turn FAILED and never become OPERATIONAL.

Conditions: Server farms & VServers are configured with access CLIs, and VRF forwarding is enabled in the client/server interfaces.

Workaround: There is no workaround.

- CSCsj05251

  Symptoms: An IOU image crashes during bootup.

  Conditions: The IOU image crashes after CSCsi64025 fix.

  Workaround: There is no workaround.

- CSCsj07189

  Symptoms: Entering the **snmpget** of an object identifier (OID) using the interface index (ifIndex) value of an interface for its index will result in an error:

  snmpget -c <community> -v1 <device> IF-MIB::ifDescr.92

  Error in packet Reason: (noSuchName) There is no such variable name in this MIB. Failed object: IF-MIB::ifDescr.92

  Conditions: This can occur after port adapters (PAs) have been swapped, such as replacing a 4-port PA with an 8-port PA.

  Workaround: Use the **snmpwalk** to retrieve the IF-MIB values.

- CSCsj07297

  Symptoms: Config sync is seen with Cisco 7600 HA routers.

  Conditions: This symptom is observed when the **no vrrp 1 preempt** interface configuration command is configured and when a switchover is done from primary to secondary.

  Workaround: There is no workaround.

- CSCsj07446

  Symptoms: When L4 Redirect is configured for a traffic class with an inbound ACL only, downstream traffic may not be translated.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: Configure both an inbound and outbound ACL for the traffic class.

- CSCsj14847

  Symptoms: The **crypto connect** command on a channelized T3 WAN card (serial interface in the non-channelized mode) is lost after a chassis reload or a WAN card reload.

  Conditions: Chassis reload with the **crypto connect** command in the startup configuration for a serial interface. WAN card reload with the **crypro connect** command configured on the serial interface.

  Workaround: Reconfigure the **crypto connect** command.

- CSCsj18688

  Symptoms: In the display of the **show l2 sess all vcid** command, the block containing “FS flash header information” is moved before the display of the counters, resulting in regression.

  Conditions: All.

  Workaround: There is no workaround.

- CSCsj19308

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

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

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

- CSCsj21066

  Symptoms: IPv4 eBGP or IPv6 eBGP session flaps when its configuration is unchanged.

  Conditions: This symptom occurs when route-target configuration is changed on another eBGP session on the same link.

  Workaround: There is no workaround.

- CSCsj21099

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

  Conditions: The symptom occurs only with images that support “vrf definition” configuration.

  Workaround: There is no workaround.

- CSCsj25562

  Symptoms: A router that functions in a BBA QoS configuration may crash when a shaper policy map is removed from a PPPoEoVLAN subinterface while QoS sessions are being established.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to a PRE-3.

  The issue is not present in any released images; it is present only in a few interim images leading up to the final 12.2(31)SB6 image.

  Workaround: There is no workaround.

- CSCsj29687

  Symptoms: An ATM VC may remain down until you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the ATM VC is configured.

  Conditions: This symptom is observed after a service policy has been added to or deleted from the ATM VC.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the ATM VC after the service policy has been added or deleted.

- CSCsj30138

  Symptoms: The standby PRE-2 may fail to boot. It may reach the standby hot state but may then reload after a “Bulk-sync failure” error is displayed on the console:

  ```
  Config Sync: Bulk-sync failure due to BEM mismatch
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB5 when SSH Version 1 (SSHv1) or SSH Version 2 (SSHv2) is configured. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsj43962

  Symptoms: ISG may send the physical MAC address in ARP reply packets when Gateway Load Balancing Protocol (GLBP) may require the virtual MAC address (VMAC) for proper operation.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, that functions as an ISG, and that connects to another ISG via an interface that is configured for GLBP.

  Workaround: There is no workaround.

- CSCsj50333

  Symptoms: An ISSU on a Cisco 7600 series may fail.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when, after you have entered the **runversion** command, the ifIndex bulk synchronization client sends infinite messages to the peer because it has entered into an endless loop.

  Workaround: There is no workaround.

- CSCsj54395

  Symptoms: A crash occurs when the IPHC **ip tcp header compression** command is configured.

  Conditions: This symptom occurs when the IPHC **ip tcp header compression** command is configured with SLIP encapsulation.

  Workaround: Use ppp/hdlc/x25/fr encapsulation.

  Further Problem Description: The crash occurs with 12.2S/12.2SR/12.2SX images, but not with 12.4/12.4T/12.0S images.

- CSCsj66522

  Symptoms: A line card crashes when running a script that adds or deletes interfaces bundles, changes encapsulation, or changes CRC.

  Conditions: Include the following:

```
top# show context slot 5

CRASH INFO: Slot 5, Index 1, Crash at 13:44:02 UTC Sun Jul 15 2007
VERSION:
GS Software (GLC1-LC-M), Version 12.0(071407A2.2007-07-14) UBUILDIT Image, CISCO
DEVELOPMENT
TEST VERSION
Compiled Sat 14-Jul-07 15:28 by xxxxxxxx
Card Type: ISE 2.5G SPA Interface Card, S/N SAD10250A6D
```

  Workaround: There is no workaround.

- CSCsj67820

  Symptoms: A virtual cem interface does not get deleted when there are no VCs configured under the interface.

  Workaround: There is no workaround.

- CSCsj85065

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsj93643

  Symptoms: In rare cases, a Cisco 12000 router with a SIP400 and one or more SPA-CT3/DS0 and SPA-T3E3 installed may display the following message:

```
SLOT 14:Jul 22 06:18:31.790 EDT: %SPA_PLIM-3-HEARTBEAT: Subslot 2 has experienced an
heart beat failure Current Sequence 1980 received Sequence 1970 Time since last keep
2952ms.
```

The SPA-CT3/DS0 and SPA-T3E3 may stay in the state, and the SPA may not recover in some cases.

Workaround: The following command may be used to disable SPA heartbeat to avoid the SPA failure.

execute-on <slot#> test hw-module subslot <subslot#> ipc keepalive disable

It is not recommended to use this command, and it may cause the SPA to become stuck in the bad state. The test command shall be used under Cisco Support supervision.

- CSCsj94561

  Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot** *slot-number* **stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

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

  Workaround: There is no workaround.

- CSCsj94583

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

  Conditions: When police cir percent conversion to cir value increases a certain range, the policy is not being accepted.

  Workaround: There is no workaround.

  Further Problem Description: Here, the cause was seen in the function af_policer_percent_to_bps. The percent value is converted to the rate, and it is compared to temp_visible_bandwidth (which is the max allowed rate). The var temp_visible_bandwidth was of type ulong, so it was not holding the right max allowable value. So the calculated rate from percent was always greater than temp_visible_bandwidth.

- CSCsj99980

  Symptoms: User is not able to configure AToM xconnects on interfaces that use PA-POS-1OC3 cards. The following error message is displayed:

  ```
  MPLS encap is not supported on this circuit
  ```

  Conditions: xconnects cannot be configured when PA-POS-1OC3 cards are used.

  Workaround: There is no workaround.

- CSCsk00054

  Symptoms: Packets requiring fragmentation going into an mGRE tunnel are dropped.

  Conditions: Symptoms are observed consistently when using mGRE.

  Workaround: It is possible to specify a large MTU on the GRE tunnel in order to avoid fragmenting going into the tunnel.

- CSCsk06279

  Symptoms: Port no calculation for pc evc egress port is missing in a few places.

  Conditions: Found during code walk-through.

  Workaround: There is no workaround.

  Further Problem Description: During the code walk-through, I found a few places where the egress port number calculation for pc evc was needed but it was not present.

- CSCsk93241

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsl17798

  Symptoms: Etherchannel membership on standby supervisor is inconsistent with the state on active supervisor. Reported in ESM-20G line card.

  Conditions: This defect may be seen with Etherchannel mode “on” and on a standby reload. Reported in Cisco 7600 series router. Could impact other platform as well.

  Etherchannel configuration and performing SSO.

  Impact: This may impact traffic forwarding. Etherchannel state inconsistent between active and standby.

  Frequency: Every time when Line card reloads.

  Workaround: Once standby supervisor has reached hot, remove etherchannel configuration and repapply. No other workaround exists.

- CSCsl33632

  Symptoms: Router crashes when VRF is unconfigured.

  Conditions: Crash is observed on Cisco 7200 router while VRF is unconfigured.

  Workaround: There is no workaround.

- CSCsl49124

  Symptoms: Observing the issue while booting the router.

  Conditions: On booting the router the issue was seen

  Workaround: There is no workaround.

- CSCsl51945

  Symptoms: The HSRP IPv6 configuration on the standby RP may lose its address. 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.

  Trigger: Standby RP on switchover stucks in standby-cold state.

  Impact: Secondary RP resets, configuration sync failure.

  Workaround: There is no workaround.

- CSCsl60107

  Symptoms: VPLS/EoMPLS traffic may be dropped at imposition when a WRED policy applied to any port on the same HW datapath on SIP600 or ES20.

Additionally, QoS may be incorrectly applied and traffic may stop on an FRR cutover of a VPLS/EoMPLS VC under similar conditions to above.

Conditions:

1. If a VPLS/EoMPLS VC egresses a port with no QoS applied and any other port on the LC has a WRED policy applied, the VC's traffic may be dropped in the imposition direction, or misqueued.
2. If a VC is FRR protected and BOTH the primary and backup paths egress ports on the second datapath on ES20 (ports 10-19), VC traffic may be dropped on tunnel switchover to the backup path.

Workaround:

1. Configure QoS on the egress interface carrying the VPLS/EoMPLS VC.
2. Configure primary and backup tunnel paths to egress interfaces on the first 10 ports of ES20.

- 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.

- CSCuk44154

  Symptoms: RPR+ mode does not work properly from a CEF perspective because the forwarding dBase is synced across from the active to redundant RP (RRP). Syncing of the forwarding dBase should happen only for SSO mode, and, consequently, Non-Stop Forwarding (NSF) should not occur in RPR+ mode.

  Conditions: Upon switchover to the RRP in RPR+ mode. The CEF forwarding dBase is already present, but should be re-created from the config.

  Workaround: There is no workaround.

- CSCuk54570

  Symptoms: IPv6 communication does not function.

  Conditions: This symptom is observed between two 6PE routers that are connected by a TE tunnel when CEFv6 does not resolve properly for these routers. The symptom does not occur for IPv4.

  Workaround: Enable an LDP session through the tunnel by entering the **interface tunnel** *te number* command followed by the **mpls ip** command.

- CSCuk61910

  Symptoms: A PE router crashes.

  Conditions: This symptom occurs while configuring MVPN.

  Workaround. There is no workaround. The bug is 100-percent reproducible.

TCP/IP Host-Mode Services

- CSCeb54456

  Symptoms: A data-link switching plus (DLSw+) circuit may not function when a TCP connection gets stuck. After about 90 seconds, the TCP connection is closed by DLSw+, and a new TCP connection is built for DLSw+. Once the new TCP connection is up, the DLSw+ circuit starts functioning again.

Conditions: This symptom is observed on a Cisco router that is configured with both a DLSw+ interface and an ATM interface.

Workaround: If this is an option, remove the ATM interface from the router. When you configure the DLSw+ interface and the ATM interface on different routers, the symptom does not occur.

- CSCec79570

  Symptoms: User Datagram Protocol (UDP) port 1985 (on which Hot Standby Router Protocol [HSRP] runs) may be opened by a port scan. This is improper behavior.

  According to the router log, the router does not generate a message that indicates that UDP port 1985 cannot be reached, as it should do.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(2)T1 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state, and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco router.

  Workaround: Identify the BGP connection that is stale by entering the **show tcp brief** command, and then clear the TCP control block.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be sent to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

- CSCsh92986

  Symptoms: The latency for the RSH command could increase when they are flowing through an FWSM module.

  Conditions: The following issue was observed on an FWSM that is running 2.2 (1) software. The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.

  Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.

- CSCsi40766

  Symptoms: H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 54,500 calls.

Conditions: This symptom is observed when H.323 uses TCP to transport signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that an unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed.

The symptom occurs for H.323 calls only when a separate TCP session is established for the H.245 session. When H.245 tunneling is enabled or no H.245 session is established, the symptom does not occur for H.323 calls.

When the **debug ip tcp transaction** command is enabled on the gateway, the "TCP: Ran out of ports for network 0" debug output is generated when the symptom occurs.

Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. At a minimum, ensure that logging to the console is changed from the default behavior of the debug level to, for example, an informational level.

Workaround: After the symptom has occurred, reload the Cisco IOS VoIP gateway. To prevent the symptom from occurring, ensure that for H.323 call processing all H.323 devices have H.245 tunneling enabled. This may not always be possible: for example, H.245 tunneling on Cisco CallManager is not supported.

- CSCsi43868

  Symptoms: TCP listening ports cease to respond to incoming SYN packets.

  Conditions: This condition occurs if a system receives the initial SYN packets but does not receive the final ACK to complete the 3-way handshake.

  Workaround: There is no workaround.

  Further Problem Description: This issue affects only images that have the fix for CSCef74037.

- CSCsi92978

  Symptoms: The "Show udp/Show ip socket" local address field may show "--any--" for port 161 and 162 because of the output of the snmp walk command showing an IP address as 0.0.0.0.

  Conditions: This problem is observed on a Cisco 7200 router with a Cisco IOS image.

  Workaround: There is no workaround.

- CSCsj62846

  Symptoms: A MIB walk of the udpTable will have extra bad entries when a UDP IPv6 connection to the box is made.

  Conditions: IPv6 must be configured, and an IPv6 UDP socket must be present.

  Workaround: There is no workaround. The symptom should not interfere with normal box operation.

Wide-Area Networking

- CSCdw04802

  Symptoms: The virtual-access counters and the RADIUS accounting data exceed the real value.

  Conditions: This symptom is observed on a Cisco 7200 PA-A3 port adapter and a Cisco 6400 NRP2-SV when a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) uses an ATM permanent virtual connection (PVC) as an ingress interface for L2TP tunnels.

  Workaround: Configure an Ethernet port as the ingress interface.

- CSCec27942

  Symptoms: A virtual-access interface is not freed when a client session is torn down.

  Conditions: This symptom is observed on a Cisco router that is configured for VPDN when the client session is momentarily disconnected and then reconnected.

  Workaround: There is no workaround.

- CSCee56988

  Symptoms: High CPU usage occurs on a Cisco 7301, and the following error message and traceback are generated:

  ```
  %TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer: 0x0 -Process= "L2X SSS manager",
  ipl= 0, pid= 69 -Traceback= 0x606E43DC 0x60B9FAC8 0x60BA11C4 0x619F502C 0x619F4A2C
  0x619F4D34 0x619F35C4 0x619F4FF4 0x619F6820 0x619F5ED8 0x619F6350 0x619CA1F4
  0x619CA6C4 0x619D2524 0x619CABB4 0x619CAFA0
  ```

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.4(5b) with PPTP/VPDN connections after, on a connected platform, rate limiting is changed to MQC policy-based limiting of the bandwidth. Note that the symptom may be release-independent.

  Workaround: There is no workaround.

- CSCef67942

  Symptoms: The amount of free processor memory slowly decreases because the “IP input” process holds increasingly more memory. This situation finally leads to MALLOC failures and a crash.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(6) or a later release, that is configured with dialer interfaces, and that is configured for large-scale dial-out (LSDO).The symptom may be release-independent.

  Workaround: When the amount of free processor memory becomes too low, reload the router when it least affects the service.

- CSCef71011

  Symptoms: Pings fail when translational bridging and ATM DXI encapsulation are configured.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S, Release 12.2S, or a release that is based on Release 12.2S.

  Workaround: Do not configure ATM DXI encapsulation. Rather, configure HDLC, PPP, or Frame Relay encapsulation.

- CSCeh25440

  Symptoms: InvARP packets on multiple MFR bundle interfaces may be dropped, causing traffic to fail after you have reloaded microcode onto a line card that processes a high load of traffic over many PVCs on MFR interfaces.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(31)S when 42 MFR bundles are configured over 336 full T1s and when egress MQC is configured on the 42 MFR bundle interfaces. However, the symptom is not platform- and release-specific.

  Workaround: There is no workaround.

- CSCeh32353

  Symptoms: An LNS intermittently routes packets to an incorrect interface in the process-switching path, preventing some applications from working properly. These applications, such as ARP, CBAC, and NAT, depend on the first packet to go to process-switching for their initialization operation. Consequently, this situation may affect user connectivity to the Internet.

Conditions: This symptom is observed when the next-hop ISP router is connected via static routes and when there is no ARP entry on the LNS.

Workaround: There is no workaround.

- CSCeh35068

  Symptoms: CEF adjacency is not established with a serial interface with Frame Relay and FR-IETF encapsulation.

  Conditions: The symptom has been observed on a Cisco 7200 router with a CE1 potent interface.

  Workaround: Enter the **shutdown** command and then the **no shutdown** command on that interface.

- CSCek54185

  Symptoms: When you add Variable Bit Rate (VBR) traffic shaping parameters to active PPPoA sessions, a Cisco 10000 series may crash and generate the following error message:

  ```
  %ERR-1-GT64120 (PCI-1)
  ```

  Conditions: This symptom is observed when PPPoA sessions without VBR are in the process of coming up while you add VBR traffic shaping parameters.

  Workaround: Wait until the sessions are completely up and then add VBR traffic shaping parameters.

- CSCek56693

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

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

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

- CSCek76406

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

  Symptom 1: A Cisco 7200 series may crash when payload compression is added to or removed from an MFR interface that has interface fragmentation configured.

  Condition 1: This symptom is observed when traffic is sent through an MFR interface that has or had interface fragmentation and payload compression configured. The symptom may not be platform-specific.

  Workaround 1: There is no workaround. Do not configure both interface fragmentation and payload compression on an MFR interface.

  Symptom 2: A Cisco 7200 series may crash when you remove interface fragmentation from an interface that is configured for Frame Relay encapsulation while traffic is running.

  Condition 2: This symptom is observed with both serial Frame Relay and MFR interfaces. The symptom may not be platform-specific.

  Workaround 2: Shut down the interface before you remove interface fragmentation.

- CSCek77555

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

  Conditions: This symptom is observed only on regular serial interfaces that use PPP encapsulation. The symptom does not occur with tunneling mechanisms such as PPP over ATM (PPPoATM) or VPDN sessions. The symptom may occur when the physical layer undergoes multiple state transitions, starting from an up state and ending in an up state, with the entire sequence occurring

over a short period of time. In such a situation, event filtering mechanisms in Cisco IOS software may prevent a notification from being sent to PPP when the link returns to an up state and, in turn, PPP from (re-)starting on the interface. The most likely time for such a situation to occur is when PPP itself resets the interface, which occurs when an existing PPP session is terminated because of a keepalive failure or LCP negotiation failure.

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

- CSCek78126

  Symptoms: A compilation error occurs.

  Conditions: This symptom occurs because vpdn ever enable variable is missing in autobahn76.

  Workaround: There is no workaround.

- CSCin86951

  Symptoms: An LNS router crashes on establishing a large number of PPPoA L2TP sessions.

  Conditions: This symptom is observed only when you establish sessions at a high rate. When you attempt to establish 8000 sessions, the router crashes shortly after 5000 sessions are established.

  Workaround: Establish sessions at a low rate.

- CSCsb11520

  Symptoms: A Cisco 7204 series will display "%SYS-2-LINKED: Bad enqueue of 6318AECC in queue 6313B39C" when attempting to dial out over ISDN.

  Conditions: This symptom is observed on a Cisco 7204VXR that runs Cisco IOS Release 12.2(29) and that is configured with an NPE-400 processor. The dial out attempt fails to connect to the remote end. Connections dialing in to the same interface will establish okay.

  Workaround: There is no workaround.

- CSCse81327

  Symptoms: When a main interface has subinterfaces and is configured for Frame Relay encapsulation and when a subinterface is deleted and then re-added, the DLCI information is not re-added to the running configuration, and no error message is generated to indicate an error.

  Conditions: This symptom is observed on a Cisco router only when the main interface is shut down. If the main interface is administratively up, the symptom does not occur.

  Workaround: Do not provision and rollback subinterfaces on main interfaces that are shut down.

- CSCsf30411

  Symptoms: In an L2TP dialout configuration, when a failover occurs and when limit and priority options are specified, the output of the **show vpdn** command may be incorrect. This situation causes the limit option to be unusable.

  Conditions: This symptom is observed when limit and priority options are enabled on the LNS and when a ping is made from the LNS to two LACs to check if the limit option functions. The session should be the same as that of the limit, but is more than the specified limit.

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *hostname* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is both platform- and release-independent.

  Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

  After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.

- CSCsg89222

  Symptoms: A PPP session that is initiated from a client may not be forwarded to an LNS.

  Conditions: This symptom is observed on a Cisco router after the PPP session has been established.

  Workaround: Enter the **vpdn source-ip** global configuration command.

- CSCsh02500

  Symptoms: L2TP sessions fail when the L2TP peer (that is, the LAC if Cisco IOS software is acting as an LNS) is sending L2TP AVPs that are hidden. “Debug vpdn error” will show the following error message:

  ```
  Error unhiding AVP <x>, no shared secret configured
  ```

  Conditions: This symptom occurs when the L2TPv2 tunnel protocol is used and when the L2TP peer is sending L2TP AVPs hidden according to RFC 1661, section 4.3.

  Workaround: There is no workaround.

- CSCsh06841

  Symptoms: A router may crash while establishing a PPP session.

  Conditions: This symptom is observed when the **ppp reliable-link** interface configuration command is enabled on an interface that is bound to a dialer profile.

  Workaround: Disable the **ppp reliable-link** interface configuration command, save the configuration, and reload the router. Disabling the command without reloading the router is not sufficient.

- CSCsh27457

  Symptoms: On an HA BBA, the standby RP disconnects PPPoE sessions when the **ppp lcp echo mru verify** command is configured under the Virtual-Template.

  Conditions: This symptom occurs when the **ppp lcp echo mru verify** command is configured under the Virtual-Template.

  Workaround: Do not configure the **ppp lcp echo mru verify** command.

- CSCsh49699

  Symptoms: A router may crash when you configure Frame Relay fragmentation on a Frame Relay main interface after the following error message has been generated:

  ```
  Leased-line fragmentation works with main interface service-policy only, please
  remove policy under subinterface/PVC and re-enter the command.
  ```

Conditions: This symptom is observed on a Cisco router after you first attempt to configure Frame Relay fragmentation on a Frame Relay main interface that has a service policy on a subinterface, when you then remove the service policy from the subinterface, and when you then again attempt to configure Frame Relay fragmentation.

Workaround: After the error message has been generated, immediately remove the Frame Relay fragmentation before you remove the service policy.

- CSCsh62833

  Symptoms: The **sessions per-mac throttle** command functions as expected, but when you enter the **show pppoe throttled mac** command, no output is displayed, and a warning message and traceback are generated:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 70A48450
  chunkmagic 0 chunk_freema0 -Process= "Exec", ipl= 0, pid= 234 -Traceback= 6053AADC
  606167A8 6158DB78 61578A28 61578B4C 604E4BF4 601C01E8 604FE6F8 60617B54 60617B40
  604FE6F8 60617B54 60617B40
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has an PRE-2, that runs Cisco IOS Release 12.2(28)SB4, and that is configured for PPPoE connection throttling. Note, however, that the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCsh72559

  Symptoms: The **show pppoe throttled mac** command may display no or invalid output.

  Conditions: The problem may be seen when the **show pppoe throttled mac** command is issued.

  Workaround: There is now workaround.

- CSCsi00004

  Symptoms: The following errors are displayed:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=657A5740, count=0
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61A716DC reading 0x22
  ```

  The line protocol may also go down.

  Conditions: These errors may be seen when removing frame-relay payload-compression configuration when frame-relay interface fragmentation is configured.

  Workaround: Remove the frame-relay interface fragmentation configuration before removing frame-relay payload-compression.

- CSCsi02669

  Symptoms: A router may reload while displaying the output of the **show ppp multilink** command.

  Conditions: This symptom is observed when the multilink bundle goes down while the output is being displayed.

  Workaround: There is no workaround.

- CSCsi51530

  Symptoms: If a non-Cisco PPPoA client is dialing in to a Cisco router, the call may fail at the PPP authentication phase. When this situation occurs, the following error message is generated:

  ```
  Failed to send an authentication request x
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB5.

  Workaround: There is no workaround.

- CSCsi57143

  Symptoms: After an SSO switchover has occurred, some serial interfaces may remain down on the newly active RP.

  Conditions: This symptom is observed on a Cisco router that has several serial interfaces with PPP encapsulation up and running on the active RP before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsi60136

  Symptoms: The standby processor on a router that is configured for PPP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the **debug ppp redundancy** command is enabled on the standby processor.

  Workaround: Do not enable the **debug ppp redundancy** command on the standby processor.

- CSCsi69009

  Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

  Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase "cloned from: AAA, AAA, ..." (that is, multiple instances of AAA) as identification.

  Workaround: There is no workaround.

  Further Problem Description: You can alleviate the situation somewhat by configuring the NCP timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

  - Increase the hello timers for L2TP and for the receive windows.
  - Configure the timers under the virtual template.
  - Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
  - Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- CSCsi72045

  Symptoms: A bus error crash occurs on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen with AAA and PPPoE configured.

  Workaround: There is no workaround.

- CSCsi78968

  Symptoms: When a multilink bundle comes up, the following error message may be generated:

  ```
  SYS-2-INTSCHED: 'idle' at level 2 -Process= "PPP Events"
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3.

  Workaround: There is no workaround.

- CSCsi82832

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

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

  Workaround: There is no workaround.

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

- CSCsi94498

  Symptoms: Alternate packets may be dropped during a ping test.

  Conditions: This symptom is observed when you initiate a ping over a Frame Relay PVC bundle.

  Workaround: There is no workaround.

- CSCsj05288

  Symptoms: When you delete a Frame Relay subinterface, the following error message and a traceback may be generated continuously:

  ```
  SYS-2-BADSHARE: Bad refcount in retparticle
  ```

  Conditions: This symptom is observed on a Cisco router when a Frame Relay subinterface with a service policy is applied inside a VRF.

  Workaround: Recreate and then delete the interface. When you do so, the error message and a traceback are no longer generated.

- CSCsj10933

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

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

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

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

- CSCsj12579

  Symptoms: The router can reload if using the vpdn-group command **lt2p ignore tx-speed** on a router acting as a LAC. This command is expected to be used on an LNS, but if it is used on the LAC, a reload can occur.

  Conditions: This symptom occurs on a router acting as a LAC. This command is expected to be used on an LNS, but if it is used on the LAC, a reload can occur.

  Workaround: There is no workaround.

- CSCsj36201

  Symptoms: The traffic flow stops and tracebacks are generated when the fragmentation size is changed by using an MQC shaped policy on a PVC. When the fragmentation size is set to a value equal to or larger than 700, the router hangs.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(31)SB4.

  Workaround: When the symptom occurs, you must power-cycle the router. To prevent the symptom from occurring, first remove fragmentation, change the size, and then reapply the map class. To prevent the router from hanging, use FRTS.

- CSCsj51280

  Symptoms: No debugs are displayed on the console. VPDN debugs are not displayed when conditional debugging like the **debug condition domain cisco.com** command or any other conditional debugging commands are enabled.

  Conditions: This symptom occurs only when conditional debugging is enabled (for example, the command above).

  Workaround: Do not enable the above conditional debugging to display the messages.

- CSCsj60578

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

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

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

- CSCsj75575

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

  Conditions: This issue arises only when DBS is configured.

  Workaround: Disable DBS.

- CSCsj75811

  Symptoms: MIB: cvpdnSessionAttrUserName is limited to 31 CHAR.

  Conditions: This symptom occurs on a Cisco IOS router acting as VPDN LNS and running Cisco IOS Release 12.4(15)T.

  Workaround: There is no workaround.

- CSCsj76378

  Symptoms: A router crashes when a vc-group is configured using an MFR bundle link interface.

Conditions: This symptom occurs when an invalid FRF.5 configuration is attempted.

Workaround: This is an invalid configuration. Use the MFR bundle interface instead of the bundle link.