Caveats for Cisco IOS Release 15.1(2)S

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.

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 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:

Resolved Caveats—Cisco IOS Release 15.1(2)S2

Cisco IOS Release 15.1(2)S2 is a rebuild release for Cisco IOS Release 15.1(2)S. The caveats in this section are resolved in Cisco IOS Release 15.1(2)S2 but may be open in previous Cisco IOS releases.

- CSCti42671

  Symptoms: The state of MLP bundles on active RP and standby RP is not in sync. Some of the bundles that are active on active RP, show up as inactive on standby RP. This may result in the bundles going to down state after switchover.

  Conditions: This symptom occurs under the following conditions:

  1. Configure scaled number of MLP bundles on 1xCHOC12 SPA.
  2. Reload the SPA.

  Workaround: Reload the standby RP.

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCti83542

  Symptoms: MPLS LDP flapping is seen with T3 SATOP CEM interface configurations.

  Conditions: This issue is seen with T3/E3 SATOP TDM configurations.

  Workaround: There is no workaround.

- CSCti98219

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj04672

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtj14525

  Symptoms: Standby is not synced to active after attaching a new policy.

  Conditions: This symptom happens when dynamic policy is used such as RADIUS CoA.

  Workaround: There is no workaround.

- CSCtk67768

  Symptoms: RP crash is observed in DHCPD receive process.

  Conditions: This symptom occurs on the DHCP server that is used on Cisco ASR routers and acting as ISG.

  Workaround: There is no workaround.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

Workaround: There is no workaround.

- CSCtl00995

  Symptoms: Cisco ASR 1000 series routers with 1000 or more DVTIs may reboot when a shut/no shut operation is performed on the tunnel interfaces or the tunnel source interfaces.

  Conditions: This symptom occurs when all the DVTIs have a single physical interface as tunnel source.

  Workaround: Use different tunnel source for each of the DVTIs. You can configure multiple loopback interfaces and use them as tunnel source.

- CSCtl49917

  Symptoms: Minor diagnostic error is seen on SIP-400.

  Conditions: This symptom occurs when scaled configurations are applied to ES+ and SIP-400. The BusConnectivity test fails on SIP-400 during boot-up.

  Workaround: Power enable SIP-400 after all the line cards have come up in the test bed. Or, after a couple of retries, reload SIP-400, and it automatically comes up.

- CSCtn15317

  Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on the P router, the entry has an instruction to TAG all packets that are destined to the PE router instead of a POP instruction which is expected on a directly connected P.

  Conditions: This symptom occurs with the following conditions:

  - The ISIS protocol is running as IGP on MPLS infrastructure.
  - ISIS on the PE router is summarizing network that includes BGP vpnv4 update-source.
  - The P router is running an MFI-based image.

  Workaround 1: Remove the **summary-address** command in ISIS on PE.

  Workaround 2: Change the BGP update source.

- CSCtn18784

  Symptoms: Interface Tunnel 0 constantly sends high-bandwidth alarms.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn19027

  Symptoms: The **show mediatrace responder sessions brief** command crashes the router.

  Conditions: This symptom is observed on Mediatrace Responder when showing a stale session.

  Workaround: There is no workaround. Avoid issuing this impacted **show** command.

- CSCtn40571

  Symptoms: Issuing the **crypto pki server** *name* **rollover cancel** command can result in multiple rollover certificates installed on Sub-CA router.

  Conditions: This symptom is seen when the rollover certificate is already installed.

  Workaround:

  - Copy startup-configuration from router.

  - Remove the older rollover certificate from configuration under the **crypto pki cert chain** *ca* command.
  - Copy the new configuration back to startup-configuration and reload the router.

- CSCtn44232

  Symptoms: With multiple RP switchovers, both RPs become unusable.

  Conditions: This symptom is observed with multiple RP switchovers.

  Workaround: There is no workaround.

- CSCtn58128

  Symptoms: BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: The issue may be triggered by route-flaps in scaled scenario where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure "no logging console" is configured.

- CSCtn64879

  Symptoms: After configuring service group, traffic will go through both of the memberlinks of Ethernet Virtual Connection (EVC) point of contact (PoC) with xconnect.

  Conditions: This symptom is seen when defaulting the PoC configuration and adding it back.

  Workaround: Reset line card.

- CSCtn67637

  Symptoms: Traffic is not forwarded from the DECAP PE in the egress replication mode.

  Conditions: This symptom occurs when the ingress LC on the DECAP PE is a CFC LC like 6748/SIP400 and the egress replication mode is used on the DECAP PE in a mVPN setup.

  Workaround: Switch to the ingress replication mode on the DECAP PE. Then, the traffic will start flowing.

- CSCtn68117

  Symptoms: The **session** command does not work on Cisco 3000 series routers that have become the master after a mastership change.

  Conditions: This symptom is seen when fail-over to slave occurs.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

  Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The BGP peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

  Router3 ---ebgp--- Router1 ---ibgp--- Router2

Router1:

```
--------
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-mode
!

router ospf 100
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 10.1.1.2 remote-as 1
 neighbor 10.1.1.3 remote-as 11
!
```

Router 2:

```
--------
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip pim sparse-mode
!
router ospf 100
 redistribute static
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
 bgp log-neighbor-changes
 network 0.0.0.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Router 3:

```
-------
interface Ethernet0/0
 ip address 10.1.1.3 255.255.255.0
 ip pim sparse-mode
!

router bgp 11
bgp log-neighbor-changes
 network 0.0.0.0
 network 0.0.0.0 mask 255.255.255.0
 redistribute static
 neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

Reproduce crash with the following steps:

1. Traffic travel from router 3 to router 2.
2. “clear bgp ipv4 unicast 10.1.1.1” on router 2.

Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a vrf and the configuration such that the connected routes are redistributed in the vrf. This redistributed route fails to tag itself with the RT when it reaches the peering PE(+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  - Create an IOS image that does not IPV6 enabled.
  - Enable BFD on an interface.
  - Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.

  Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCto11957

  Symptoms: PPPoE is terminated on port-channel with ES+ session limit error occurring incorrectly.

```
%CWAN_RP-6-SESS_LIMITS_PORT_GROUP: Exceeded max number of sessions supported
on
```

```
port-group
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:PPPoE:5789] - hardware platform error.

Mismatch in sessions on RP and ES+:
BRAS#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                              57      56       0       1
Port-channel100                    57      56       0       1

BRAS#show platform isg session-count 4
 ES+ line card
 Sessions on a port-channel are instantiated on all member ports
 Port-group          Sess-instance   Max Sess-instance
 ----------          -------------   -----------------
 Gig4/11-Gig4/15              2936                4000 <<<<<<< INCORRECT
```

Conditions: This symptom is seen when scaled PPPoE sessions are terminated on port-channel with ES+ ports. Sessions negotiate, disconnect and attempt to renegotiate port-channel number other than port-channel 2.

Workaround: Change port-channel number to port-channel 2. Configure sessions to terminate on stand-alone ports.

- CSCto16106

  Symptoms: Address not assigned when “ip dhcp use class aaa” is configured.

  Conditions: When the DHCP server is configured to download a class name from the radius using “ip dhcp use class aaa” and lease an IP address from that class, the IP address is not assigned to the client.

  Workaround: There is no workaround.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/re-add the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto35160

  Symptoms: After switchover, traffic drops are seen in CARRIER-Ethernet testcase for about 15 seconds. This issue is not seen consistently.

  Conditions: This symptom is seen after switchover.

Workaround: Will auto restore after 15 seconds.

- CSCto41165

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command.

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto41223

  Symptoms: Standby IOSD crashes when standby RP reload is executed.

  Conditions: This symptom is observed in a scaled configuration with 8000 EoMPLS and 8000 EVC sessions while the traffic is flowing. On issuing standby RP reload, IOSd crashes at the process "Standby service handler".

  Workaround: There is no workaround.

- CSCto46716

  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In "debug ip ospf spf", when the SPF process link for the TE tunnel is in its own RTR LSA, the "Add path fails: no output interface" message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto55643

  Symptoms: High CPU loading conditions can result in delayed download of multicast routes to line cards, resulting in multicast forwarding (MFIB) state on line cards out of sync with the RP. The **show mfib linecard** command shows line cards in sync fail state with many in LOADED state.

  Conditions: This symptom occurs during high CPU loading due to router reload or line card OIR events in a highly scaled multicast environment with high line rates of multicast traffic and unrestricted processed switched packets, before HW forwarding can be programmed.

  Workaround: There is no workaround. Ensure that mls rate limits are properly configured.

  Further Problem Description: IPC errors may be reported in the MRIB Proxy communications channel that downloads multicast routes to line cards.

- CSCto55983

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the high CPU rate, line cards are stuck in a continual loop of failing to complete MFIB download and retrying.

  Conditions: This symptom occurs during high CPU utilization caused by multicast traffic. The **show mfib line summary** command does not show cards in sync.

  Workaround: There is no workaround.

- CSCto63720

  Symptoms: No traffic passes after a link flap if port-security is configured on the Gigabit Ethernet interface on 6748 LC.

Conditions: This symptom occurs when the Cisco IOS version running is Cisco IOS Release 12.2(33)SRE2. This issue is seen when port-security is configured on a 6748 port and the link flap occurs on this interface.

Workaround: Reconfiguring port-security fixes the problem.

- CSCto69071

  Symptoms: Metrics collection fails due to invalid DVMC runtime object handle.

  Conditions: This symptom occurs when the transport layer is not passing up an interface type that is acceptable to DVMC.

  Workaround: There is no workaround.

- CSCto71004

  Symptoms: Router crashes with high scale and a lot of BGP routes. This crash is seen in the box when core links flap.

  Conditions: This symptom is seen when scaled box with a lot of BGP routes crashes the box when some of the core links flap.

  Workaround: There is no workaround.

- CSCto72480

  Symptoms: The output of the **show mfib linecard** command shows that line cards are in “sync fail” state.

  Conditions: This symptom occurs usually when the last reload context displayed in the **show mfib linecard internal** command output is “epoch change”. This indicates that an IPC timeout error has occurred in the MRIB communications channel that downloads multicast routing entries to the multicast forwarding information base (MFIB). In this condition, multicast routing changes are not communicated to the failed line cards and they are not in sync with the RP.

  Workaround: If this issue is seen, using the **clear mfib linecard** *slot* command may clear the problem. If the problem occurs on a Cisco 7600 SP, an RP switchover is required after clearing the problem on any affected line cards. The workaround may not completely work if high CPU loading continues to be present and IPC errors are reported.

  Further Problem Description: The IPC timeout errors could result from high CPU loading conditions caused by high rates of processed switched packets. High rates of multicast processed switched packets can be avoided if rate limits are applied after each router boot, especially after using the **mls rate-limit multicast ipv4 fib-miss** command.

- CSCto75643

  Symptoms: Few ISIS packets get subjected to QoS. In case of congestion, this may cause ISIS protocol flaps.

  Conditions: This symptom occurs only when “isis network point-to-point” is configured.

  Workaround: Add a class-map to classify ISIS control packets and allot bandwidth for it.

- CSCto76018

  Symptoms: Cisco ASR1000-WATCHDOG process crashes on DVTI Server after clearing crypto session on DVTI Client.

  Conditions: This symptom occurs for sessions with the configuration of 1000 vrf, 1 IKE session per vrf, and 4 IPSec SA dual per session. The ASR1000- WATCHDOG process crashes on DVTI Server during clear crypto session on DVTI client, after all the SAs have been established.

  Workaround: There is no workaround.

- CSCto77504

  Symptoms: With shape configured on port-shaper and bandwidth-percent configured on groups in the EVC, on dynamic configuration of port-shaper value, the groups do not get the updated shape values based on bandwidth percent.

  Conditions: This symptom is seen when bandwidth-percent is configured on group or EVC with port-shaper.

  Workaround: There is no workaround.

- CSCto80714

  Symptoms: Prowler SPA goes out of service with heartbeat failures when traffic flows through the MLPPP (multilink) interface. This issue is seen only in the Cisco IOS Release 12.2SRE throttle and not in mcp_dev. Some optimizations and a microcode reload-related fix is also included as part of this DDTS.

  Conditions: This symptom is observed when traffic flows through the MLPPP interface on Prowler. Microcode and SPA reload is required to recover.

  Workaround: There is no workaround.

- CSCto88581

  Symptoms: The standby RP crashes following an interface configuration change.

  Conditions: This symptom is observed only when “ospf non-stop routing” is configured.

  Workaround: There is no workaround.

- CSCto88660

  Symptoms: Command failure on RP is causing both protecting and working APS to go to active.

  Conditions: This symptom may be caused by switchover during scaled conditions.

  Workaround: There is no workaround.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

- This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.
  CSCto90252

  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.

  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.

  Workaround: Disable NSR.

- CSCto98212

  Symptoms: The IPv6 address and prefix 2001:DB8:1:104::/64 at 25 Aug 2011 00:01 25 Jul 2011 00:01 are lost after a router reload.

  Conditions: This command checks for the clock validity. When the router reloads the clock validity is displayed as “not yet valid”. This causes the command to not be applied.

Workaround: There is no workaround.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loop back. OSPF provides reachability to BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x *** command.

- CSCtq06538

  Symptoms: RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF
        Header
          AttributeFlags
            Optional: 0b0
            Transitive: 0b1
            Partial: 0b0
            ExtendedLength: 0b0
            Unused: 0b0 0b0 0b0 0b0
          TypeCode: 0x05
          Length: 0x01    <----- should be 0x04 instead
        Value: 0xff 0xff 0xff 0xff
    NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
```

  Workaround: There is no workaround.

- CSCtq10019

  Symptoms: After router reload, rate-limiters for multicast do not come into effect and packets are punted.

  Conditions: This symptom occurs during high CPU load when mfib is unable to distribute into lc and SP.

  Workaround: There is no workaround.

- CSCtq21785

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(2)S may crash upon performing a CRL check on an invalid certificate.

  Conditions: The conditions are unknown.

  Workaround: Turning off CRL check should stop the crash. It should be configured as:

  “revocation-check none”

  This will stop the CRL check of the peer certificate but should not be a long term solution.

- CSCtq22873

  Symptoms: Router may show the following traceback (error message) after receiving certain IPv6 packets:

  ```
  TB:%SCHED-2-EDISMSCRIT:process=PuntInject Keepalive Process
  ```

  Conditions: This symptom is seen when router is configured for IPv6 routing.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtq23038

  Symptoms: With “platform control-packets use-priority-q disable” configured on the port-channel main interface, after shut/no shut on the port-channel or member-link, port-channel subinterfaces do not inherit the “platform control-packets use-priority-q disable” feature.

  Conditions: This symptom occurs when you perform shut/no shut on a member-link or link flaps with port-channel subinterfaces and “platform control-packets use-priority-q disable” configured on the port-channel.

  Workaround: A possible workaround is to remove and reconfigure the subinterfaces.

- CSCtq23158

  Symptoms: The dlfi o atm fails to come up on sip400 with Cisco IOS Release 15.0(1)S images onwards if an ES+ card is present.

  Conditions: This symptom occurs when you cannot bring up dlfi o atm.

  Workaround: A possible workaround is to power down all ES+ cards.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add MDT configuration.

- CSCtq30686

  Symptoms: A Cisco router crashes in a Secure Device Provisioning (SDP) environment.

Conditions: This symptom is seen when the Registrar router crashes when a client router submits an enrollment request that was previously stuck in “granted” status with the same fingerprint.

Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq34807

  Symptoms: Service group does not take effect on EVC Xconnect on a port channel.

  Conditions: This symptom is observed with a service group configuration on EVC Xconnect existing on a port channel. This issue is seen when EVC is removed and the configuration is reapplied.

  Workaround: Remove and reapply the service group.

- CSCtq43480

  Symptoms: A Cisco router crashes.

  Conditions: This symptom occurs when a session starts with PBHK and accounting features while the method list is not provisioned for the accounting features.

  Workaround: There is no workaround.

- CSCtq46745

  Symptoms: Custom configured default sip profiles (option/method/header) are lost during a router reload.

  Conditions: This symptom occurs during reload.

  Workaround: Use non-default profiles for each adjacency.

- CSCtq46760

  Symptoms: When doing ISSU subpackage upgrade from Cisco IOS XE Release 3.2.2 to Cisco IOS XE Release 3.4.0 with the Cisco IOS XE Release 2.3 feature set, both FPs crash and multiple core files are seen after the last ISSU step, active RP loadversion.

  Conditions: This symptom only occurs on Cisco ASR1006 subpackage upgrade with dual RPs.

  Workaround: Reload the standby RP before switchover.

- CSCtq50674

  Symptoms: Total traffic drop is seen for 6PE/6VPE when IPFRR is configured in the core.

  Conditions: This symptom occurs when BGP/6PE peer is protected by IPFRR in core.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: CLNS routing table is not updated when LAN interface with CLNS router isis configured shuts down because ISIS LSP is not regenerated. CLNS route will be cleared after 10 minutes when isis ages out the stale routes.

  Conditions: This symptom is seen when only CLNS router ISIS is enabled on LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq63744

  Symptoms: MAC withdrawal is not sent to the core VCs on reception of STP TCN for MST.

  Conditions: This symptom is seen when access has switchport only.

  Workaround: There is no workaround.

- CSCtq67680

  Symptoms: An SPA reload triggers silent LC reload under the following steps:

  1. Configure policy-maps as shown below:

     ```
     policy-map mul1
     class GOLD
     priority 1000
     class SILVER
     bandwidth 1000
     policy-map mul2
     class GOLD
     priority 7000
     class SILVER
     bandwidth 7000
     class class-default
     random-detect
     ```

  2. Apply it on multilink interfaces - multilink1 and multilink2.
  3. Reload the SPA.

  Conditions: This issue is seen only with QoS policy applied on multilink bundle on serial SPA.

  Workaround: There is no workaround.

- CSCtq67970

  Symptoms: Inter-AS IPv4 multicast streams do not resume if the source of the multicast stream is stopped. The s,g state expires in the transit AS, and traffic source is started again.

  Conditions: This symptom occurs when BGP PIC CORE/EDGE is configured in the system.

  Workaround: There is no workaround.

- CSCtq77363

  Symptoms: License images are not working properly.

  Conditions: This symptom is seen when the license image is loaded. There is a traceback due to access of uninitialized variables.

  Workaround: There are no workarounds.

- CSCtq83629

  Symptoms: The error message is associated with a loss in multicast forwarding state on line cards under scaled conditions when an IPC error has occurred.

  Conditions: This symptom is observed during router boot or high CPU loading, which can cause IPC timeout errors. This issue is seen on line cards during recovery from an IPC error in the MRIB channel.

  Workaround: Line card reload is required to resolve the problem.

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtq93823

  Symptoms: Ping drops with fragment size of 256.

  Conditions: This symptom occurs when doing a sweep ping with sizes 500 to 1000.

  Workaround: Flap the interfaces.

- CSCtq94418

  Symptoms: Adding, deleting, and re-adding an access subinterface may sometimes lead to loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create dummy access subinterfaces belonging to a new vrf. Do not remove the interface.

- CSCtq96329

  Symptoms: Router fails to send withdraws for prefixes when bgp deterministic-med is configured. This could lead to traffic blackholing and routing loops. Could also result in memory corruption/crash in rare conditions.

  Conditions: This symptom can happen only when bgp deterministic-med is configured.

  The following releases are impacted:

  - Cisco IOS Release 15.0(1)S4
  - Cisco IOS Release 15.1(2)T4
  - Cisco IOS Release 15.1(3)S
  - Cisco IOS Release 15.2(1)T

  Workaround: Disable deterministic med in the network/AS by issuing the **no bgp deterministic-med** command and then the **clear ip bgp *** command or hardreset of BGP session to remove any stale prefixes.

  It is further recommended to do a SSO on routers that are running impacted software to eliminate any potential corruption that might have already existed on routers that are running impacted software.

  Further Problem Description: If deterministic med is enabled, withdraws are not sent.

- CSCtq97646

  Symptoms: A Cisco 7600 ES+ and SIP-400 card may crash when Dynamic Ethernet Services Activation (DESA) is configured, and certain attributes are downloaded from a radius server.

  Conditions: This symptom is seen when DESA is configured, and the radius profile that it downloads for an EVC contains an idle-timeout and dot1q range for the “stag-vlan-id” attribute. The card will crash.

  The ES+ card will crash as soon as the attributes are downloaded while a SIP- 400 may crash when the idle-timer expires.

  Radius Example:

```
simulator radius subscriber 25029
 <b># [28] idle-timeout
 attribute 28 numeric 60</b>
 vsa cisco generic 1 string "subscriber:sss-service=vpws"
 vsa cisco generic 1 string "l2vpn:service-
id=atom_from_agg22_to_dist2_int1_cfg1_1_of_1000"
 vsa cisco generic 1 string "l2vpn:redundancy-group=2"
 vsa cisco generic 1 string "ethernet-service-instance:service-instance-
description=... Dynamic EFP on Po2, stag:2000-2009, CFG_SEQ:1306963076"
 vsa cisco generic 1 string "l2vpn:redundancy-priority=2"
 vsa cisco generic 1 string "cdp:l2protocol-pdu-action=forward"
 vsa cisco generic 1 string "accounting-list=ACCT11"
 vsa cisco generic 1 string "ethernet-service-instance:stag-vlan-id=<b>2000-
2009</b>"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress=1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-tag-
operation=Push1"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
type=0x8100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-stag-
vlanid=1100"
 vsa cisco generic 1 string "ethernet-service-instance:rewrite-ingress-
symmetric=TRUE"
!
```

The card will not crash if either dot1q range or IDLE-Timeout is absent from the downloaded configuration.

Workaround: Configure radius to either not send an idle-timeout value or to not send a dot1q range.

- CSCtr07704

  Symptoms: While using scripts to delete non-existent class map filter from a class, the router sometimes crashes (c2600XM) or returns traceback spurious memory access (c2801nm).

  Conditions: This symptom occurs when trying to delete a non-existent classmap filter, the classmap will be NULL, and passed to match_class_params_same. This results in referencing a null pointer.

  Workaround: Do null check in match_class_command and match_class_params_same. To keep existing behavior, do not print out a message like “the class does not exist” when deleting a non-existent class map from a class.

- CSCtr22007

  Symptoms: A Cisco 7600 router that is configured with RSVP crashes.

  Conditions: The condition is unknown.

  Workaround: There is no workaround.

- CSCtr30820

  Symptoms: IP address is not assigned to the client after a DHCP request.

  Conditions: The problem is observed while verifying the VRF-aware-DHCP functionality in Cisco IOS relay and server in an MPLS setup.

Workaround: There is no work around.

Resolved Caveats—Cisco IOS Release 15.1(2)S1

Cisco IOS Release 15.1(2)S1 is a rebuild release for Cisco IOS Release 15.1(2)S. The caveats in this section are resolved in Cisco IOS Release 15.1(2)S1 but may be open in previous Cisco IOS releases.

- CSCtd10712

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd23069

  Symptoms: A crash occurs because of a SegV exception after configuring the **ip virtual-reassembly** command.

  Conditions: This symptom is observed on a Cisco 7206VXR router that is configured as an LNS and that is running Cisco IOS Release 12.4(15)T7 and Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCth52252

  Symptoms: Two EzVPN clients behind the same NAT device initiate sessions to dVTI EzVPN Server. When the first client connects, traffic is successful. When the second client also connects, traffic is successful for the second client, but fails for the first client.

  Conditions: This symptom is observed when two EzVPN clients behind the same NAT device initiate sessions to dVTI EzVPN Server.

  The drop reason is

  ```
  sh pl ha qf ac fe ipsec data drop

  ----------------------------------------------------------------------

  Drop Type  Name                              Packets

  ----------------------------------------------------------------------

      30  IN_V4_POST_INPUT_POLICY_FAIL                         8
  ```

  The same scenario is supported with dynamic crypto map configuration.

  Workaround: Use legacy EZVPN and RRI. Only partial functionality of DVTI is achieved.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCti64685

  Symptoms: User may not be able to configure SLA MPLS configuration.

  Conditions: This symptom occurs when the router is booted up and may be random.

  Workaround: There is no workaround.

- CSCti92812

  Symptoms: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Conditions: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtj46670

  Symptoms:

  IPCP cannot complete after dialer interface is moved out of Standby mode CONFREJ is seen while negotiating IPCP

  Conditions: The symptom is observed when a dialer interface has moved out from standby mode.

  Workaround: Reload the router.

- CSCtj55624

  Symptoms: A router crashes upon entering the **show crypto ruleset** command.

  Conditions: This symptom is seen when version 6 crypto maps are configured.

  Workaround: Do not run the **show** command.

- CSCtj65692

  Symptoms: The service policy applied to a service instance stops forwarding any traffic. The output of the **show policy-map interface** *x/y* command indicates that all packets are hitting the violation queue. The conform counter does not increase at all and all traffic is dropped.

  Conditions: This symptom is observed in Cisco 7600 running Cisco IOS Release 12.2SRD. This issue is applicable for the service policy applied for ingress or egress traffic.

  Workaround: There is no workaround. To restore the services, the service policy has to be removed from the service instance, and then the condition clears. The service policy can then be reapplied and will work normally.

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtj91149

  Symptoms: A delay of approximately 30 seconds is observed in dynamic xconnect- based ISG session that comes up on standby, after it is up on active.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj94510

  Symptoms: When sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and 4 SA dual per session, a crash happens on Crypto_SS_process.

  Conditions: This symptom occurs when sessions are setting up with the configuration of 1000 VRFs (fvrf!=ivrf), one IKE session per VRF, and four SA dual per session.

  Workaround: There is no workaround.

- CSCtk12122

  Symptoms: A Cisco 7200 router may crash after clearing the SAs while using the IKE keepalive feature.

  Conditions: This symptom occurs when the IKE keepalive feature is turned on, and the user executes a **clear crypto session** command or a **clear crypto sa** command.

  Workaround: There is no workaround.

- CSCtk46381

  Symptoms: Service Policy installation on L2transport PVP fails when shaping rate is changed.

  Conditions: This symptom is seen when the PVP shape rate is changed.

  Workaround: Remove the service-policy and add again.

- CSCtk76697

  Symptoms: Service instances on the line card go to the down state for the approximately first 100 service instances of 4000 service instances after a test crash on the line card, resulting in a complete traffic drop on these service instances.

  Conditions: This symptom occurs only during the first test crash on the LC after booting up the router.

  Workaround: A shut/no shut on the service instance/interface will resolve this issue.

- CSCtk83638

  Symptoms: Client gets assigned an IP address from an incorrect pool when it reconnects with a different profile.

  Conditions: This symptom is been observed in a setup where two clients are behind a NAT router. When one client connection is broken and the server is not made aware of this, and the client reconnects with a different group, the IP address assigned is not from the correct pool.

  Workaround: There is no workaround.

- CSCtk95106

  Symptoms: CPU 1 of SPA 8XT1E1 goes into a forced reload followed by a software forced reload of line card SIP-200 when a multilink PPP with interleave enabled having fragment size 42 is disabled and enabled. One member of the link is removed.

  Conditions: This issue is noticed when traffic is pumped onto the DUT from remote end. Size could be as low as 800 bytes. Interleave is disabled and enabled on the mulilink interface, and one of the members of the MP is detached from the bundle using the **no ppp multlink group** <> command.

Workaround: There is no workaround.

- CSCtl70143

  Symptoms: LAC does not forward a PPP CHAP-SUCCESS message from LNS to client sometimes.

  Condition: This symptom is seen when T1/PRI is used between the client and LAC.

  Workaround: There is no workaround.

- CSCtl78285

  Symptoms: In VRF configuration, we are not able to add rd after deleting rd configuration once:

```
A-SUP5-6509E#sho run | be vrf
ip vrf CUST1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 239.39.39.39



A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#no rd 1:1
% "rd 1:1" for VRF CUST1 scheduled for deletion

wait for some time and try to add rd again (waited for more than 2 hrs)

A-SUP5-6509E(config)#ip vrf CUST1
A-SUP5-6509E(config-vrf)#rd 1:1
% Deletion of "rd" in progress; wait for it to complete
A-SUP5-6509E(config-vrf)#
```

  Conditions: This symptom is seen in a VRF configuration with rd.

  Workaround: Remove VRF configuration and add again.

- CSCtl82517

  Symptoms: For the Cisco ME3600 and Cisco ME3800, the following licensing errors are seen, leading to license manager failure at bootup:

```
%SCHED-7-WATCH: Attempt to lock uninitialized watched semaphore (address 0).
-Process= "Init", ipl= 4, pid=
```

  Conditions: This symptom is seen when a Cisco ME3600 or Cisco ME3800 license-based image is loaded off mcp_dev_nile.

  Workaround: Use whales-universal-mz.

- CSCtl84797

  Symptoms: SBC traceback occurs.

  Conditions: This issue is observed when LI is enabled and there are multiple media sessions in a single call (that is, SDP contains information about multiple media sessions).

  Workaround: There is no workaround.

- CSCtl92210

  Symptoms: A router may crash when trying to show the sessions on responder while the session queue is being managed (removal).

  Conditions: This symptom occurs while new sessions are being provisioned or removed from Mediatrace initiator side. The router can crash when trying to show the session objects on the responder while the session queue is being managed (removal) by first disabling the initiator using the **no mediatrace initiator force** command and then disabling responder with the **no mediatrace responder** command.

  Workaround: Do not disable initiator with the **no mediatrace initiator force** command and responder with the **no mediatrace responder** command in quick succession while the **show mediatrace responder session [brief | details]** command is not finished with output or in pause mode.

- CSCtl99266

  Symptoms:

  1. CoA service logon is not synced to standby.
  2. CoA multiservice logon/logoff is not synced to standby.

  Conditions:

  For issue 1:

  - Do CoA service logoff of a service that was not installed via CoA service logon (i.e. installed through a rule or as an auto service). This gets synced to standby.
  - Do CoA service logon of the same service. This is not synced.

  For issue 2:

  - Do CoA multiservice logon/logoff of more than 1 service. The services are applied/unapplied on active, but not on standby.

  Workaround:

  For issue 1:

  - After the CoA service logon is not synced, reboot the standby.
  - After the standby comes up, a bulk sync from the active is initiated, which will sync the service logon.

  For issue 2: There is no workaround.

- CSCtn11326

  Symptoms: The Structure-agnostic TDM over Packet (SAToP) PW remains down when the AC is down.

  Conditions: This problem is seen if the xconnect configuration is applied on a CEM AC, which is in down state.

  Workaround: There is no workaround.

- CSCtn16840

  Symptoms: VPLS imposition traffic does not go through for some of the VCs when the core is a port channel on ES20.

  Conditions: This symptom is observed when core facing is a port channel on ES20.

  Workaround: Do a shut/no shut on the port channel.

- CSCtn17680

  Symptoms: When performing an OIR on a Cisco WS-X6708 module, the router may crash. When inserting the card, the following message is displayed:

  ```
  %EARL_L2_ASIC-SP-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. Error occurred. Ctrl1 
  0xB88D0E3D
  ```

  Then, the following message is displayed:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 60 seconds 
  [*Sched* 41%/0% (00:01:00.244 99%/99%)]
  ```

  Finally, a timeout occurs, followed by the crash:

  ```
  %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR messages have failed, resetting system 
  (self) [5/0]
  ```

  Conditions: This symptom is observed on Cisco IOS 7600 series routers with either a single or dual RSP720 supervisor. In the case of dual supervisors, both supervisors crash. The cause of the crash is unknown. However, after the router reloads, the affected module has been installed again without further issue in a couple of instances.

  Workaround: There is no workaround.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working VRF "A" and a new local label will not be reassigned.

  Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused VRF "B", including:

  - The VRF interface, for example, **no interface Gi1/0/1.430**
  - The same VRF process, for example, **no router ospf** *process id* **vrf** *vrf name*

  Run the following commands to verify whether you are facing this issue:

  - **show ip bgp vpnv4 vrf A** *subnet* (this is for the working VRF)
  - **show mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

  - **clear ip bgp** *mp-bgp neighbor* **soft in**
  - **clear ip bgp** *mp-bgp neighbor* **soft out**

- CSCtn19444

  Symptoms: mLACP memberlinks may be bundled on an isolated PoA with a core failure, resulting in both PoAs becoming active.

  Conditions: This symptom occurs when running mLACP. The ICRM connection between the PoAs is lost. The PoAs are in a split brain situation and both PoAs attempt to become active. If the interface configured as "backbone interface" goes down on one of the PoAs, that PoA may keep the port-channel memberlinks bundled. The end result is that both PoAs are in mLACP active state, and both have their port-channel memberlinks bundled. After the fix the PoA with the backbone interface failure will unbundle its port-channel memberlinks, leaving only one PoA as active.

  Workaround: Configure shared control by configuring "lacp max-bundle" on the Dual Homed Device (DHD) if the device supports it. This would prevent the DHD from bundling the memberlinks to both PoAs at the same time.

- CSCtn37743

  Symptoms: Egress interface is not correct as observed by Mediatrace responder. This can impact monitoring on perf-traffic and system profiles.

  Conditions: This symptom is seen on a node where it has both initiator and responder. When the responder has both high and low cost routes and when the interface is changed, the change is detected, but the egress is not reflected.

  Workaround: Remove the original session and add it again.

- CSCtn38996

  Symptoms: All MVPN traffic is getting blackholed when peer is reachable using a TE Tunnel, and an interface flap is done so that secondary path can be selected. The multicast route does not contain a native path using the physical interface.

  Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn39632

  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.

  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn41653

  Symptoms: When a user attempts to configure CFMoXC dynamic sessions, the standby router will reload.

  Conditions: This symptom is seen when setting up CFMoXC PEI dynamic sessions. It is observed during a large number of dynamic sessions.

  Workaround: There is no workaround.

- CSCtn42601

  Symptoms: A Cisco router may unexpectedly reload when OSPF event debugging is enabled.

  Conditions: This symptom occurs under the following conditions:

  1. OSPF router configured to redistribute another protocol and redistribution is being controlled by a route-map.
  2. The **debug ip ospf events** command is enabled.

  Workaround: Do not reconfigure route maps while OSPF event debugging is on. Disable OSPF event debugging before making route-map configuration changes.

- CSCtn43223

  Symptoms: The idle timer is not working with traffic flowing with backup PW.

  Conditions: This symptom is seen when primary VC is down in PW redundancy setup.

  Workaround: There is no workaround.

- CSCtn45777

  Symptoms: Align messages are seen when enabling the **debug cwan atom** debug command.

Conditions: This symptom is observed when the **cwan atom** debug command is enabled. Spurious memory access messages are seen on the router console.

Workaround: There is no workaround.

- CSCtn46263

  Symptoms: Memory leaks are seen in ikev2_packet_enqueue and ikev2_hash.

  Conditions: This symptom is observed during retransmissions and window throttling of requests.

  Workaround: There is no workaround.

- CSCtn48744

  Symptoms: Memory leaks on OER border router while running PfR-IPSLA configuration.

  Conditions: This symptom is seen on a Cisco 7200 router that is running Cisco IOS Release 15.1(4)M.

  Workaround: There is no workaround.

- CSCtn51058

  Symptoms: Traffic drops cause long multicast reconvergence times.

  Conditions: This symptom occurs when performing Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in EzVPN process.

  Conditions: This symptom is seen when EzVPN connection is configured with split tunnel attributes.

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350.
  -Process= "Mwheel Process", ipl= 2, pid= 315
  ```

  Conditions: This symptom is observed when toggling very fast between the **ip pim** *mode* and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

  Workaround: Avoid fast toggling of the **ip pim** *mode* command if possible when it is only present on a single interface.

- CSCtn53222

  Symptoms: The REALs are stuck in READY_TO_TEST state, and they never come to OPERATIONAL state. The only way to make them operational is to make them OUTOFSERVICE and INSERVICE again.

  Conditions: This symptom occurs when the REAL moves to FAILED state because of real failure that is detected by the inband failure mechanism. After the retry timeout, the REAL will be moved to READY_TO_TEST state.

  Workaround: There is no workaround.

- CSCtn54985

  Symptoms: The status of a LSP health monitor with LSP discovery is shown as unknown.

Conditions: This symptom is observed when PE routers in an MPLS VPN scenario are configured with LSP health monitors.

Workaround: There is no workaround.

- CSCtn55187

  Symptoms: Memory leaks are seen at ikev2_ipsec_add_proxy_to_list, ikev2_skeyseed_create, and ikev2_ios_get_ipv6_pak on the Cisco 2900 and Cisco 3900 platform routers respectively.

  Conditions: This symptom is seen after the test has been completed and while trying to check for the memory leaks when testing the Tunnel Protection for IPv6 feature.

  Workaround: There is no workaround.

- CSCtn59698

  Symptoms: When MLP bundle comes up on LNS with conditional debugging based on username enabled, certain attributes like IDB description and IP-VRF are not applied on the MLP bundle Virtual-Access.

  Conditions: This symptom is observed with the following conditions:

  1. Only for MLP sessions on LNS.
  2. When you configure per-user attributes in the user Radius profile such as “ip:vrf-id” and “ip:description”.
  3. When you bring up the session.
  4. When you run **show interfaces virtual-access** *intf* configuration for both the member-link VA and bundle VA.
  5. When the VRF and IDB description sent by Radius is applied only on member link VA and not on bundle VA.

  Workaround: Do not enable conditional debugs like **debug condition username** *user-name*.

- CSCtn61834

  Symptoms: NAT-T keepalive cannot send out cause NAT translation timeout.

  Conditions: This symptom is seen when the NAT translation table is getting timeout since no NAT keep alive message is received.

  Workaround: There is no workaround.

- CSCtn62250

  Symptoms: After upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3, there may be a problem with pim mdt neighbors, which do not get brought up, though the configuration is not changed. Conditions: This symptom is observed after upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3. Workaround: Remove/reinsert the **mdt default** command in ip vrf configuration mode.

- CSCtn64500

  Symptoms: Multicast traffic does not pass through an ATM point to a multipoint subinterface.

  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the **show adjacency ATM interface detail** command shows that the Inject P2MP multicast adjacency is in incomplete state.

  Workaround: Run the **clear adjacency** command to force repopulating the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn73941

  Symptoms: After doing an OIR for an ES+ card having EVC configuration with the **module clear-config** command enabled, restoring the old configuration does not work anymore, indicating that traffic will not be forwarded over those service instances. The VLANS used in the previous config cannot be effectively used on those ports, not even by changing the service instance numbers. It is observed that the IOS still believes that the port is configured though there is no configuration yet.

  ```
  Router#sh bridge-domain 10
  Bridge-domain 10 (3 ports in all)
  State: UP                    Mac learning: Enabled
      TenGigabitEthernet4/1 service instance 10

  Router#sh run int ten4/1
  Building configuration...

  Current configuration : 64 bytes
  !
  interface TenGigabitEthernet4/1
   no ip address
   shutdown
  end
  ```

  Conditions: This symptom occurs only with **module clear-config** configured.

  Workaround: There is no workaround. A complete reload would probably resolve this issue.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process

  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept

  Workaround: Do not use long banner in HTTP intercept.

- CSCtn74673

  Symptoms: After reload, incoming mcast traffic is punted into the CPU before MFIB is downloaded into line cards. Due to the CPU rate being high, the line cards are stuck in a continual loop of failing to complete MFIB download.

  Conditions: This symptom is observed when high CPU utilization is caused by multicast traffic and the **show mfib linecard** does not show cards in sync and tables are in “connecting” state. The **clear mfib linecard** command does not correct the line card table states.

  Workaround: There is no workaround other than line card reload.

- CSCtn80120

  Symptoms: VLAN translation in ES+ line cards is not working when ports are configured as Layer 2 switch ports (as in LAN cards).

  Conditions: This symptom is observed when you configure VLAN translation in ES+ line cards.

  Workaround: There is no workaround

- CSCtn80993

  Symptoms: An IOSD crash is found when doing two SPA IORs back-to-back on the same SPA.

Conditions: This symptom is observed on a router that has scaled L2VPN configuration, for example, Cisco 7000 EoMPLS, 1500 TE tunnels, 6000 EVCs, and 3000 L2TPv3 sessions. IOSD crash is seen consistently on the second SPA OIR when there is traffic through the sessions, and when the second SPA OIR is attempted immediately after the first SPA OIR of the same SPA.

Workaround: Once the SPA comes up after the first OIR, wait about one minute before issuing the second SPA OIR.

- CSCtn81186

  Symptoms: BFD hardware offload subsystem has some memory leaks in the error paths.

  Conditions: This symptom is seen when BFD sessions are offloaded to ES+ line cards in bulk and when some errors occur.

  Workaround: There is no workaround.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out of the RBE interface due to incomplete multicast adjacency.

  Conditions: This symptom is seen on an ATM DCHP host that is running IGMPv2 is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and therefore cannot forward multicast traffic.

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

- CSCtn87155

  Symptoms: CoA sessions are not coming up.

  Conditions: This symptom is observed when some CLI commands that are called within shell function might fail if the shell programmatic APIs are used.

  Workaround: Manually use shell functions on the console.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS 12.2(33)SRD or later releases, c7600rsp72043-adventerprisek9-mz.

  Workaround:

  1. Apply a service policy similar to below:

     ```
     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth(in kbps)*1000 / (8
     * 250 * 2) value for the correct behavior.)
     ```

  2. Or reload the line card.

- CSCtn93158

  Symptoms: When per flow load balancing is configured on a port-channel with EVC connect and Xconnect, sometimes egress traffic on EVC connect or Xconnect may get dropped.

Conditions: This symptom occurs when one of the port channel member links is shut.

Workaround: Use the **shutdown** command followed by the **no shutdown** command on the port channel.

- CSCtn95344

  Symptoms: After RPR downgrade from Cisco IOS Release 12.2(33)SRE2 to Cisco IOS Release 12.2(33)SRE1, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from Cisco IOS Release 12.2(33)SRE2 to Cisco IOS Release 12.2(33)SRE1.

  Workaround: Perform reload on the router.

- CSCtn98521

  Symptoms: After the CLI is enabled on ES+ for the control packets hitting on ES+ to not go into special queue, CLI does not reflect in the running configuration on RP sometimes.

  Conditions: This symptom occurs after enabling the **platform control- packet use-priority-q disable** command on ES+ for the control packets hitting on ES+ to not go into special queue. CLI does not reflect in the running configuration on RP.

  Workaround: There is no workaround.

- CSCtn98966

  Symptoms: In the following topology, the port-channel link on the standby PoA may forward packets unexpected to DHD. The issue is observed in both Cu’s environment and the test lab:

  ```
  Topology:
   ------------------POA-1(active)
  |                          |
  DHD                  |(L3  ICC link and L2 Trunk)
  |                          |
   ------------------POA-2(standby)
  ```

  In Cu’s environment: When DHD sends an arp request to ask for MAC of an HSRP virtual IP, it will receive the arp reply from the standby PoA, causing MAC flapping on DHD.

  In the lab test environment: When you configure static arp on PoAs to bind an IP address with a nonexistent MAC address, ping this IP, so it will do unicast flooding within vlan. When you ping, POA-2(standby) also sends out the unicast packet to DHD via its port-channel link.

  Conditions: This symptom occurs both on Cisco IOS Release 12.2(33)SRE2 and Cisco IOS Release 12.2(33)SRE3 with MLACP deployment.

  Workaround: There is no workaround.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

- CSCto02448

  Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

Conditions: This symptom is observed with the following conditions:

1. The neighbor is configured with soft-reconfiguration inbound.
2. The inbound routemap is not configured for the neighbor
3. The non-routemap inbound policy (filter-list) allows the path.

Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto04593

  Symptoms: Statid leak in line card is observed while churning PPPoE sessions when using "show plat npc xlif 0 statid-usage". The statid leak results in high LC CPU, when it runs out of stat ids.

  Conditions: This symptom is seen only with scale.

  Workaround: There is no workaround.

- CSCto10958

  Symptoms: One of the OIFS starts dropping traffic in MLDP/LSM scenario.

  Conditions: This symptom is seen within MLDP/LSM configuration on a midpoint node or bud node.

  Workaround: Flap the interface where the OIF is going.

- CSCto11076

  Symptoms: Flood traffic does not work post TE FRR cutover for VPLS VCs.

  Conditions: This symptom is seen when VPLS VCs are going over TE/FRR and FRR cutover.

  Workaround: Have bidirectional traffic.

- CSCto13029

  Symptoms: When the Cisco 7600 router is running Cisco IOS Release 15.1(3)S, under rare conditions, the service instance configuration may not be downloaded to SP.

  Conditions: This symptom occurs if a large number of service instances are configured on the router.

  Workaround: There is no workaround.

- CSCto43154

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

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

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

  Workaround: There is no workaround.

- CSCto44396

  Symptoms: If flow is learned as ip-cbr flow and later MDI metric configuration is added to the class-map, and when the flow is updated as MDI, the MDI metrics will not be updated to SNMP.

  Conditions: This symptom occurs only if the flow is learned as ip-cbr and then later updated as MDI flow also.

  Workaround: Removing and reattaching the policy-map.

- CSCto44585

  Symptoms: Packets with DF-bit set across the l2tpv3 tunnel are punted/dropped on the CPU.

Conditions: This symptom occurs when PMTU in pseudowire-class configuration is enabled.

Workaround: Reduce MTU on client side.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs responder.

  A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  one may start to see process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80mb per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on affected router, if possible.

- CSCto48592

  Symptoms: With IPFRR/MPLS-TE FRR enable, IOSd crashes during a switchover.

  Conditions: This symptom occurs under the following conditions:

  1. Enable IPFRR/MPLS-TE FRR
  2. . Enable BFD on the protected interface
  3. Switchover
  4. Independent with protocol being used, whether OSPF or ISIS

  Workaround: There is no workaround.

- CSCto50204

  Symptoms: Selective traffic denied by an inbound WCCP redirect list is being software switched due to incorrect TCAM programming. This issue is seen on the Cisco 7600/RSP720 that is running Cisco IOS Release 15.1(1)S1.

  Conditions: This symptom is seen under the following conditions:

  - WCCP redirect list should be applied inbound.
  - Only certain traffic may be software switched.
  - Cisco 7600/RSP720 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: There is no workaround.

- CSCto50255

  Symptoms: Memory leak occurs while running UDP echo operation.

  Conditions: This symptom is observed when an UDP echo operation successfully runs. Leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

Conditions: This symptom is seen with GETVPN related configurations with fail-close feature activated.

Workaround: There is no workaround.

- CSCto64240

  Symptoms: Unable to configure port-channel access sub-interface with three memberlinks.

  Conditions: This symptom occurs when the port-channel has more than two members.

  Workaround: There is no workaround.

- CSCto70972

  Symptoms: Multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Conditions: This symptom occurs when multicast traffic drops and does not reach the corresponding entries like (*,G/m) or (*,G).

  Workaround: There is no workaround.

- CSCto80174

  Symptoms: A chunk memory leak may be observed when PTP configuration is applied, changed, or removed with multicast mode.

  Conditions: This symptom is occurs when the PTP clock configuration is on the Cisco 7600 router with spa-2x1GE-SYNC SPA.

  Workaround: There is no workaround.

  Further Problem Description: The chunk memory leak is observed when a few multicast related configurations of PTP are configured on the Cisco 7600 router.

- CSCto90096

  Symptoms: A router crashes while unconfiguring recovered clock configuration.

  Conditions: This symptom occurs when applying “no recovered-clock” to the router.

  Workaround: There is no workaround.

- CSCtq01136

  Symptoms: There is a ping failure over tunnel interface.

  Conditions: This symptom is seen during 6VPE basic configuration.

  Workaround: There is no workaround.

- CSCtq12230

  Symptoms: When overhead accounting command “hw-module slot 1 account np 0 out 4” is configured on the ES+ LC, show policy-map interface counters do not get updated.

  Conditions: This symptom is seen with QoS on any ES+ interface with overhead accounting feature enabled.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.1(2)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(2)S. All the caveats listed in this section are open in Cisco IOS Release 15.1(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCti92812

  Symptom: After physical interface flap, GRE tunnel for VRF does not come up correctly.

  Condition: This symptom occurs when GRE tunnel is configured for default (global) routing table.

  Workaround: There is no workaround.

- CSCtk97082

  Symptoms: IPv6 addresses are not cleared from an interface when **vrf forwarding** is applied for an IPv4-only VRF defined with the **vrf definition** command.

  Conditions: The following must be true:

  - The VRF is defined using the **vrf definition** command.
  - **address-family ipv4** is configured.
  - **address-family ipv6** is not configured.
  - An IPv6 address is present on the interface.
  - **vrf forwarding** is then configured on the interface.

  Under these conditions the IPv6 address will not be removed from the interface when **vrf forwarding** is applied.

  Workaround: Clear IPv6 addresses from the interface before applying **vrf forwarding**.

- CSCtk99836

  Symptoms: In scale environment with 4000 udp-jitter probes, responder crashes.

  Conditions: This symptom occurs when source starts running all 4000 probes with group schedule and aggressive frequency. Responder crashes.

  Workaround: There is no workaround.

- CSCtl44112

  Symptoms: MLS adjacencies for few labels are getting corrupted.

  Conditions: This symptom occurs during redundancy switchover.

  Workaround: Associated tunnel shut/no shut.

- CSCtl99266

  Symptoms: CoA service logon is not synced to standby.

  Conditions:

  - Do CoA service logoff of a service that was not installed via CoA service logon (i.e. installed through a rule or as an auto service). This gets synced to standby.
  - Do CoA service logon of the same service. This is not synced.

  Workaround:

  - After the CoA service logon is not synced, reboot the standby.
  - After the standby comes up, a bulk sync from the active is initiated, which will sync the service logon.

- CSCtn15317

  Symptoms: Traffic on MPLS VPN is dropped. When you check LFIB information on P router, you notice that entry has an instruction to TAG all packets that are destined to PE router instead of a POP instruction which is expected on a directly connected P.

  Conditions:

  - ISIS protocol is running as IGP on MPLS infrastructure.
  - ISIS on PE router is summarizing network that includes BGP VPNv4 update-source.
  - P router is running MFI based image.

  Workaround:

  - Remove **summary-address** command in ISIS on PE.
  - Change BGP update source.

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, you may experience a situation where the local label for working VRF "A" clears and a new label never is reassigned.

  Conditions: To trigger this issue on the MPLS Edge LSR, remove the configuration of an unused VRF "B", this includes:

  - The vrf interface, for example "no int Gi1/0/1.430".
  - The same vrf process, for example "no router ospf *process id* vrf *vrf name.*

  Run the following command to verify if you are hitting this issue:

  - **sh ip bgp vpnv4 vrf A** *subnet*; this is for the working VRF.
  - **sh mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router you should clear the mp-bgp session:

  clear ip bgp *mp-bgp neigh* soft in, or **clear ip bgp** *mp-bgp neigh* soft out

- CSCtn26307

  Symptoms: In a scaled setup, a new subinterface will behave as expected during the first 20 minutes, and then will stop working.

  Conditions: This behavior is observed in a scaled setup after deleting and recreating subinterfaces. Though the sequence of commands to reproduce this is not yet clearly identified. It seems to be triggered by deleting interfaces and some timing issues. There should be a entry for the interface/vlan in the hidden vlans section of "show platform vlan". If that entry is missing, then this is probably the defect that is being encountered. There will probably be a entry in the recycled vlans for that interface instead.

  Workaround: Observe the output of "show platform vlan". In the recycled vlans section, those vlans should not stay there more than 20 minutes after a interface is deleted. If it does, then it might be possible to restore service, by following these steps:

  1. deleting the sub-interface that is having problems
  2. creating new temporary subinterfaces until the output of "show platform vlan" no longer has entries stuck in the recycled state.
  3. Add the sub-interface that was broken back into the configuration.
  4. . Observe the output of "show platform vlan" for 20 minutes to ensure that a entry stays in the hidden vlan section.
  5. Delete the temporary sub-interfaces.

  A reboot will also resolve this.

- CSCtn53834

  Symptom: When configuring HvPLS for a new circuit/VFI traffic does not pass. Mac addresses are not assigned to the VFI and traffic is blackholed.

Conditions: This symptom occurs on a Cisco 7600 series router with ES/ES+ module configured for HvPLS that is running Cisco IOS Releases SRD and SRE.

Workaround: Disable Mac Learning on the X-connect VLAN:

no mac address-table learning vlan *vlan-ID*

- CSCtn62287

  Symptoms: Standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flowing across the multilink.

  Workaround: No work around

- CSCtn67637

  Symptoms: Traffic is not forwarded out of DECAP PE for egress replication mode.

  Conditions: The ingtress LC on the DECAP PE must be a CFC LC like 6748/SIP400 and egress replication mode should be used on the DECAP PE in a mVPN setup.

  Workaround: Switch to ingress replication mode on the DECAP PE and the traffic starts flowing.

- CSCtn73941

  Symptoms: After doing an OIR for an ES+ card having EVC configuration with the **module clear-config** command enabled, putting back the old configuration does not work anymore, meaning the traffic will not be forwarded over those service instances. The VLANs used in the previous configuration cannot be effectively used on those ports, not even changing the service instance numbers. It looks like Cisco IOS still believes that port is configured though there is no configuration yet:

  ```
  Router#sh bridge-domain 10
  Bridge-domain 10 (3 ports in all)
  State: UP                    Mac learning: Enabled
      TenGigabitEthernet4/1 service instance 10

  Router#sh run int ten4/1
  Building configuration...

  Current configuration : 64 bytes
  !
  interface TenGigabitEthernet4/1
   no ip address
   shutdown
  end
  ```

  Conditions: This symptom only happens with **module clear-config** configured.

  Workaround: There is no workaround.

- CSCtn80120

  Symptoms: VLAN translation in ES+ line cards is not working.

  Conditions: This symptom occurs when configuring VLAN translation in ES+ line card.

  Workaround: There is no workaround.

- CSCtn81231

  Symptoms: Multicast traffic is not forwarded out the RBE interface due to incomplete multicast adjacency.

Conditions: This symptom is seen when ATM DCHP host that is running IGMPv2 is established over RBE interface to router. Multicast group join is successful. However, multicast adjacency is incomplete and hence cannot forward multicast traffic.

Workaround: Shut/no shut the ATM main interface.

- CSCtn89179

  Symptoms: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA S

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later.

  Workaround:

  1. Apply a service policy similar to below:

     policy-map test1
     class class-default
     queue-limit 496 --> (this number is a interface bandwidth (in kbps)*1000 / (8 * 250 * 2) value for the correct behavior.)

  2. Reload line card.

- CSCtn90664

  Symptoms: On a Cisco 7600 router which has globally configured **mls qos protocol arp police** *value* packets, which are received on an ES+ switchport/SVI interface, bypasses the policer and causes high CPU.

  Conditions: This symptom occurs when ES+ switchport/SVI interface with **mls qos protocol arp police** <> is enabled on the router.

  Workaround: Broadcast storm control could be used to rate-limit arp broadcast packets, or the following policy can be configured on the interfaces:

```
Policy-map ingress_policy-map
    Class cos0
      Set cos 0
    Class cos1
     Set cos 1
    Class cos2
       Set cos 2
    Class cos3
         Set cos 3
    Class cos4
      Set cos 4
    Class cos5
     Set cos 5
    Class cos6
       Set cos 6
    Class cos7
         Set cos 7



class-map cos0
   match cos 0
class-map cos1
   match cos 1
class-map cos2
```

```
   match cos 2
class-map cos3
   match cos 3
class-map cos4
   match cos 4
class-map cos5
   match cos 5
class-map cos6
   match cos 6
class-map cos7
   match cos 7
```

and then dscp-transparency is enabled using the CLI:

no mls qos ip rewrite dscp slot *module*

- CSCtn98966

  Symptoms: Topology:

  Topology:

  ```
   ------------------POA-1(active)
  |                  |
  DHD                |(L3  ICC link and L2 Trunk)
  |                  |
   ------------------POA-2(standby)
  ```

  In the above topology, the port-channel link on standby POA may forward packets unexpected to DHD. The problem is observed at both the customer environment and test lab:

  In the customer environment: When DHD sends arp request to ask for MAC of a HSRP virtual IP, it will receive the arp reply from the standby POA, causing MAC flapping on DHD.

  In the lab test environment: Static arp is configured on POAs to bind an IP address with a non-existed MAC address, then ping this IP, so it will do unicast flooding within vlan. When doing the ping, it is observed that POA-2 (standby) also sends out the unicast packet to DHD via its port-channel link.

  Conditions: This problem happens both on Cisco IOS Releases SRE2 and SRE3 with MLACP deployment.

  Workaround: There is no workaround.

- CSCto04744

  Symptoms: A new subinterface will disappear from the list of the "sh platform vlan" hidden VLAN.

  Conditions: This behavior is observed in a scaled setup after a switchover. After deleting and recreating subinterfaces, there should be an entry for the interface/vlan in the hidden vlans section of "show platform vlan", but that entry is missing. The steps to reproduce are not clearly identified but when the repro succeeds, the steps that lead to the issue are basically:

  1. A switchover.
  2. Removal of 4 subifs.
  3. Recreation of 2 subifs among the 4 removed in 2.
  4. The issue is triggered for one of the 2 recreated subifs.

  Workaround: There is no workaround except to delete the interface and to recreate a new one.

- CSCto15040

  Symptoms: When configuring a service-instance, the service instance may not be programmed properly on the Switch Processor leading to a loss of connectivity

  Conditions: This problem is observed when configuring the service instance under the physical interface of an ES+ card. You also need to run 12.2(33)SRE or above.

  Workaround: Configure the port in a channel-group and move the service instance configuration under the port-channel interface.

Resolved Caveats—Cisco IOS Release 15.1(2)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(2)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsh36203

  Symptoms: A Cisco router is crashing at p_dequeue.

  Conditions: This symptom is observed when testing the Echo cancelling feature in the Cisco 1700 platform but is not platform dependent.

  Workaround: There is no workaround.

- CSCsl18054

  Symptoms: A local user created with a one-time keyword is removed after unsuccessful login attempts. A one-time user should be removed automatically after the first successful login, not after failed logins.

  Symptoms: This symptom occurs on a router that is running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsm26063

  Symptoms: Router crashes following a **shut/no shut** on the main interface.

  Conditions: Occurs on a router running Cisco IOS Release 12.2SXH2a. IPv6 traffic must be flowing over the WAN interface for multiple IPv6 prefixes. The crash occurs when a **shut/no shut** is done on the main interface on which multiple subinterfaces have been configured and IPv6 routing is enabled.

  Workaround: There is no workaround.

- CSCsq02771

  Symptoms: DHCP relay may hang when request for IP address is received from a DHCP client on an unnumbered in an MPLS and VPN setup.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(19.16)T1.

  Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv97424

  Symptoms: A router will reload due to memory corruption in the I/O pool. As an indication for this bug, we will see the same caller PC in the output of the show buffer pool Serial0/0/0 command.

  Conditions: This symptom is observed on Cisco routers that are running the adventerprisek9_ivs-mz feature set and when packets are being processed by an ATM interface.

  Frequency: Always.

  Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: “no crypto engine accelerator”.

  Note: When hardware crypto is turned off, encryption and de-cryption will be done by software and not by hardware. This can slightly hike CPU utilization, and this should not be an issue as long as we are not hit with pretty huge volume of traffic.

- CSCsy33068

  Symptoms: A big SDP HTML template causes an abrupt termination of the SDP process.

  Conditions: The HTTP post to the HTTP server in an IOS router is size-limited. The limit is set to 32KiB by default. In the SDP process, the transition from introduction page to the completion page involves an HTTP post. The post contains information including the SDP bootstrap configuration and the completion template together with the overhead of HTTP post communication. The size limit might be reached with moderate usage of HTML elements. The HTTP post in SDP is base-64 encoded. The total size limit of the SDP bootstrap and the completion template is roughly (32KiB - 2KiB(overhead)) * 3/4(base-64 encoding) = 22.5KB.

  Workaround: Reduce the size of the HTML template, and abridge the configuration. The total size of the two cannot exceed ~22.5KB. Example of abridged configuration:

  ```
  configure terminal => config t
  Interface FastEthernet 1 => int Fa 1
  ```

- CSCsy54233

  Symptoms: exception_reserve_memory is invalid in UNIX image.

  Conditions: UNIX images do not support exception_reserve_memory.

  Workaround: There is no workaround.

- CSCsy61302

  Symptoms: A chunk header corruption and a router crash with BADMAGIC error message is seen for either a free or in-use chunk.

  Conditions: The symptom is observed when the following SNMP commands are configured:

  snmp-server community public ro snmp-server packetsize 17940

  The crash is seen upon doing a **show run** and doing a grep for some keyword (e.g.: **show run | inc mem**). Memory checks need to be enabled. To see this issue reasonably fast, the interval of memory checks needs to be in the order of 3-4 seconds.

  Workaround: Do not configure “snmp-server packetsize more than 2048”.

  Further Problem Description: This crash is seen because of the snmp-server packetsize 17940. There is a local variable in one of SNMP functions with the configured packet size and when we run the CLI **show run**, the exec process stack overflows and corrupts the subsequent malloced block. This causes the memory corruption.

- CSCsy82679

  Symptoms: A Cisco IOS device may leak memory when using commands that generate a configuration.

  Conditions: This symptom occurs with the Embedded Event Manager version 3.1 where a policy description was introduced. If a policy description is applied to an applet, Cisco IOS will leak memory each time that the configuration is generated.

  Workaround: Do not use the policy description for applets.

- CSCsz18634

  Symptoms: An input/output rate is always displayed with "0" in interface status, even though packets are flowing on the ports normally.

```
show int gig 4/1 output
GigabitEthernet4/1 is up, line protocol is up (connected)
......
  Output queue: 0/40 (size/max)
  30 second input rate 0 bits/sec, 0 packets/sec  <<<<<<<<<<<
  30 second output rate 0 bits/sec, 0 packets/sec  <<<<<<<<<<<
     3411001 packets input, 567007874 bytes, 0 no buffer
     Received 818876 broadcasts (725328 multicasts)
```

  Conditions: This issue has been seen on a Cisco 3750 that is running Cisco IOS Release 12.2(46)SE, as well as a Cisco 4500 and Cisco 4900M that are running Cisco IOS Release 12.2(46)SG and Cisco IOS Release 12.2(53)SG1.

  Workaround: This issue is a cosmetic issue and does not affect the functionality of the switch or the traffic flow.

  Use the value of the **show int gigx/y count detail** command to see the raw statistics.

  The rate shown in the **sh int** command uses a complex convergence algorithm. If the rate changes from X to Y, it could take several minutes (15-30) for the rate to converge from X to Y. The rate must be steady and should be sent from a tester to confirm that the convergence is happening correctly.

  Or, execute reload.

  Further Problem Description: On the Cisco 3570 platform, the fix is in Cisco IOS Release 12.2(53)SE. On the Cisco 4500/4900M, the fix for this bug is scheduled to be in Cisco IOS Release 12.2(53)SG2 and Cisco IOS Release 12.2 (50)SG7.

- CSCsz35913

  Symptoms: Interface goes down in spite of carrier-delay configuration.

  Conditions: The symptom is observed on a PA-E3, when the serial interface carrier-delay is configured for one second and any of the alarms (AIS, LOF) are generated for less than or equal to one second.

  Workaround: Increase the carrier-delay.

- CSCsz90894

  Symptoms: L2 broadcast traffic can be leaked through blocked promiscuous port, which will cause SMAC to flap between the ports. As a result the return traffic to SMAC can get black hole until L2 forwarding is correct to show the right port.

  Conditions: This symptom will only happen multiple (at least two) L2 promiscuous ports are connected to other L2 switches, which participate in spanning tree.

  Workaround: Do not connect multiple L2 promiscuous port to other L2 devices in same VLAN.

- CSCta10402

  Symptoms: Continuous packet send by BFD causes a CPU hog.

  Conditions: The symptom is observed when BFD is enabled in the router.

  Workaround: Disable BFD.

- CSCta11223

  Symptoms: A Cisco router may crash when the **show dmvpn** or **show dmvpn detail** commands are entered.

  Conditions: This symptom is observed when the device is running Cisco IOS and configured with DMVPN. The crash occurs when the **show dmvpn** or **show dmvpn detail** commands are entered two or more times.

  Workaround: There is no known workaround.

- CSCta26520

  Symptoms: The following traceback is seen:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_LINK: Driver for IDB type 0 changed the Identity of
  interface "Tunnel1" without deleting the old Identity first
  ```

  Conditions: This symptom is observed when numerous tunnel interfaces are rapidly added and removed.

  Workaround: There is no workaround

- CSCta43825

  Symptoms: A CMTS walk of the ARP table causes high CPU usage. This symptom is also seen with an SNMP walk of the ARP table.

  Conditions: This symptom is observed in the Cisco IOS 12.2S train.

  Workaround: To prevent high CPU usage due to SNMP walk, implement SNMP view to prevent SNMP walk of the ARP table:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown at excluded
  snmp-server view cutdown ip.21 excluded
  snmp-server community public view cutdown ro
  snmp-server community private view cutdown rw
  ```

  Further Problem Description: This symptom is widely observed in Cisco IOS 12.2S train since the arp redesign in 2004. It is not an efficient way to do next search/tree walk. When there are a lot of arp entries, the CPU utilization can reach as high as 99% when polling ipNetToMediaTable or atTable (they share the same logic).

- CSCta53372

  Symptoms: A VPN static route is not seen in the RIB after an interface is shut down and brought back up (shut/no shut).

  Conditions: Configure the crypto client and server routers in such a way that the session is up and RRI installs a static route on the server that is pointing to the client IP address. Now shut down the interface on the server router that is facing the client. The RRI static route disappears from the RIB and never reappears.

  Workaround: Reset the RRI session.

- CSCta78759

  Symptom: Traceback is seen in the new active when switchover is forced from RPR mode.

Conditions: This symptom is seen when the configured redundancy state is SSO and operational state is RPR due to image mismatch in active and standby.

Workaround: There is no workaround.

- CSCta79410

  Symptom: In a closed REP ring topology, where the uplink is VPLS using ES40 card, if one of the REP ports is Open and the other is Alt, then the convergence time is high when the Open port goes down.

  Conditions: The issue is only seen when the Alt port also resides on the same switch where there is a failure, and also if the Uplink happens to be VPLS.

  Workaround: There is no workaround. Reducing the number of VCs to 500 or less reduces the convergence time significantly. Moving the Alt port to some other device also reduces the convergence time significantly.

- CSCtb17152

  Symptoms: A large packet drop may occur when FRF.12 is enabled.

  Conditions: This symptom is observed when FRF.12 is enabled.

  Workaround: There is no workaround.

- CSCtb42862

  Symptoms: A Cisco 3845 router crashes due to illegal memory access.

  Conditions: The symptom is observed in a scale testing environment which has eight key servers and 20 GM routers (simulating 2000 group members) and when there is unicast rekeying. The GM router crashes in steady state (no traffic). This seems to be intermittent.

  Workaround: There is no workaround.

- CSCtb66391

  Symptoms: The following error message is displayed:

  ```
  Unable to operate on vc class. Possibly multiple users configuring IOS
  simultaneously.mapclass name class_vc1 process 374
  ```

  Conditions: This symptom happens when unconfiguring/reconfiguring scaling configuration with VC class.

  Workaround: There is no workaround.

- CSCtb87856

  Symptoms: Router can crash with a "%SYS-3-CPUHOG:" when DMVPN is deployed.

  Conditions: The symptom is observed when the physical interface (tunnel source) of the router is shut, the routing neighborship flaps, and memory consumption is increased to the point that there is no free memory left. This causes the router to crash.

  Workaround: There is no workaround.

- CSCtc27454

  Symptoms: A Cisco router may crash after displaying the following CPUHOG message for the Crypto ACL process:

  ```
  %%SYS-3-CPUHOG: Task is running for (xxxxx)msecs, more than (xxxx)msecs (xx/x),process
  = Crypto ACL.
  ```

  Conditions: This symptom is observed when the DMVPN tunnel is shut down.

  Workaround: There is no workaround.

- CSCtc33679

  Symptoms: Routes are not being controlled properly when PIRO is used.

  Conditions: If more than one exit per BR is configured and PIRO is used to control the routes, the nexthop is not being calculated correctly. As a result, traffic for these traffic classes is not taking the correct route.

  Workaround: There is no workaround.

- CSCtc54248

  Symptoms: CDP neighbors are not seen on subinterfaces.

  Conditions: This symptom is seen when CDP is enabled on subinterface and disabled on main interface.

  Workaround: There is no workaround.

- CSCtc73759

  Summary: The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml

- CSCtd10712

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd16959

  Symptoms: Traceback is seen on SSO switchover.

  Conditions: This symptom is observed under the following conditions:

  - Configure CBTS master tunnel with 3 member tunnels
  - Delete all 3 member tunnels and then remove master command from master tunnel so it becomes regular TE tunnel
  - Configure auto-tunnel primary and backup setup
  - Make SSO switchover

  Many different tracebacks are seen on newly active RP, which are related to MPLS TE.

  Workaround: Do not delete CBTS Tunnels.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

Conditions: The symptom is observed when crypto is running and configured on the router. There is also a possible connection with EzVPN.

Workaround: There is no workaround.

- CSCtd78587

  Symptoms: A Cisco Catalyst 6000 switch running Cisco IOS Release 12.2SX software might crash under rare conditions when err-disable recovery tries to recover a port. The following messages are seen in the logs before the switch resets itself: %CPU_MONITOR-6-NOT_HEARD

  Conditions: This symptom may be observed after the following sequence of events:

  1. An interface on the switch gets err-disabled as expected due to a certain feature; for example, due to BPDU Guard
  2. Shortly after, before BPDU Guard err-disable recovery kicks in, the same port gets err-disabled for a different reason; for example, because a diagnostic error is detected on the already err-disabled port
  3. Err-disable recovery (BPDU Guard) tries to recover the port and this leads to the crash.

  Workaround: Disable err-disable recovery.

- CSCtd86472

  The Cisco IOS? Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd91542

  Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

  Workaround: Avoid using the **show ip multicast rpf tracked** command.

  Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, removing the PFS eliminates the issue.

- CSCtd95386

  Symptoms: An IPSec tunnel can be torn down if the router receives a replayed QM (Quick Mode) packet.

  Conditions: This is only a problem when a replayed QM packet is received on an IPSec endpoint.

  Workaround: There is no workaround.

- CSCte01606

  Symptoms: When Bidirectional Forward Detection (BFD) is enabled, issuing certain CLI commands that are not premption safe may cause the device to restart. This condition has been seen when issuing commands such as **show mem** or **show mem frag detail**.

  Conditions: The issue may occur if BFD is enabled on a device that utilizes Pseudo Preemption to implement this feature. The device must be running an affected software build.

  Workaround: Disable BFD

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.4/3.8:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C

  CVE ID CVE-2010-3049 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCte15193

  Symptoms: The **no spanning-tree vlan [vlanno]** command is not removed on standby alone.

  Conditions: The symptom is observed under the following conditions:

  - The **no spanning-tree vlan** *vlanno* command is configured first
  - The **default spanning-tree vlan** *vlan- range* command is entered next
  - The vlanno falls within the designated range, but the last vlan number in the range does not have "no spanning-tree vlan <>" configured for that.

  Workaround: Enter the **default spanning-tree vlan** *vlanno* command to remove it.

- CSCte56437

  Symptoms: NAT programming on a Cisco Catalyst 6500 may become corrupted; the source and/or destination IP addresses of traffic passing through the NAT box are changed to the wrong IP addresses.

  Conditions: This symptom is observed when the NAT configuration is changed during a high-volume traffic session.

  Workaround: There is no workaround.

- CSCte61528

  Symptoms: Router crashes when configuring "tftp hostname" with a longer name.

  Conditions: The symptom is observed with a Cisco 7200 series router loaded with the 151-0.25.T image.

  Workaround: There is no workaround.

- CSCte64621

  Symptoms: VSA stops passing traffic after the first IPSec rekey.

Conditions: The symptom is observed VSA specific.

Workaround: There is no workaround.

- CSCte65688

  Symptoms: Easy VPN server prints "Client_type=UNKNOWN" in "%CRYPTO-6-EZVPN_CONNECTION_UP: (Server)" log, when Software VPN Client establishes an IPSec session.

  Conditions: The symptom is observed when:

  - Easy VPN is configured between a Cisco VPN Client and a Cisco IOS router.
  - "crypto logging ezvpn" is configured.

  Workaround: There is no workaround.

  Further Problem Description: This is simply a cosmetic issue. Currently, this message can identify hardware VPN clients (IOS/PIX/VPN3002) only.

- CSCte68288

  Symptoms: Spurious memory access is seen when a set of configurations is placed under "crypto pki trustpoint *name*".

  Conditions: The symptom is observed when the router is loaded with the c7200-adventerprisek9-mz.151-0.25.T image.

  Workaround: There is no workaround.

- CSCte77990

  Symptoms: QoS marking does not work.

  Conditions: The symptom is observed with the c7200-advipservicesk9-mz.122-33.SRE image.

  Workaround 1: Use an adventerprisek9 image instead of advipservicesk9 image.

  Workaround 2: Use policer with both confirm and exceed actions set to "mark" and "transmit".

- CSCte78562

  Symptoms: Trying to run a regexp action on an undefined environment variable generates the following traceback:

  ```
  %SYS-2-FREEBAD: Attempted to free memory at 61, not part of buffer pool
  ```

  Conditions: This symptom is observed if an Embedded Event Manager applet tries to execute a regexp action on an undefined variable.

  Workaround: Trying to perform a regexp search on an undefined variable is not allowed. Make sure all arguments to the regexp action are properly defined.

- CSCte91471

  Symptoms: Clock synchronization with the NTP server could be lost for several hours if router (NTP client) runs NTPv4.

  Conditions: The symptom is observed if the router clock is reset (for example: by using the **clock set** exec command). The router then takes a long time to synchronize again.

  Workaround: There is no workaround. The clock will automatically synchronize after few hours.

- CSCte91782

  Symptoms: Cannot unconfigure "crypto pki server <>" when "crl" is configured.

  Conditions: The symptom is observed on a router loaded with Cisco IOS interim Release 15.1(1.1)T.

  Workaround: There is no workaround.

- CSCtf03436

  Symptoms: A two-level policy attached on a multilink interface is getting detached when the interface undergoes a shut/no shut.

  Conditions: The symptom is observed with a two-level policy configured with shaper/bandwidth percent. It is seen on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCtf23298

  Symptoms: There is high CPU usage when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Conditions: This symptom occurs when a Terminal Access Controller Access- Control System (TACACS) server is configured with a single connection.

  Workaround: Remove single connection option.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no-shut on the tunnel interface of the other hub.

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.
  2. Hub 2 tunnel is shut and unshut.
  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf48179

  Symptoms: When using an authentication header only (no encryption over the tunnel), a percentage of the outgoing traffic is dropped by the receiver due to incorrect IP header checksums. The percentage dropped depends on the traffic that is flowing over the tunnel.

  Conditions: This problem occurs only when the traffic mix over the tunnel includes both packets with the DF bit set and packets with the DF bit clear. When the DF bit setting differs between two subsequent packets, the second packet is sent with an incorrect IP header checksum.

  Workaround: There is no workaround.

- CSCtf50155

  Symptoms: Disable CDP on the L2 interface, which has a subinterface with VLAN encapsulation configured. CDP neighbors are not shown for the subinterface.

  Conditions: This symptom is observed when running Cisco IOS Release 12.2(33) SXI.

  Workaround: There is no workaround.

- CSCtf52106

  Symptoms: There is a failure of EEM TCL scripts when using the “exit_comb” keyword for the Interface Event Detector.

  Conditions: The symptom is observed when using the “exit_comb” keyword in an EEM TCL script.

  Workaround: There is no workaround.

- CSCtf53537

  Symptoms: Serial interfaces are messed up in second redundancy switchover.

  Conditions: This issue is seen upon second switchover in sb_throttles.

  Workaround: Issue, due to change in if_numbers of serial interfaces.

- CSCtf54561

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

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

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

- CSCtf56107

  Symptoms: A router processing a unknown notify message may run into a loop without relinquishing control, kicking off the watch dog timer and resulting in a software-based reload.

  Conditions: The symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCtf57641

  Symptoms: A router crashes after performing a DNS lookup.

  Conditions: The symptom is observed when a command is used which sends out a DNS query such as **ping www.cisco.com** and the DNS server response contains a specially crafted packet.

  Workaround: Configure “no ip domain-lookup”.

- CSCtf65159

  Symptoms: While configuring empty default URL profile, we are seeing inconsistent memory access.

  Conditions: This symptom occurs while configuring empty default URL profile.

  None: There is no workaround.

- CSCtf70959

  Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

  Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

  Workaround: Use a non profile-based dialer interface.

- CSCtf71010

  Symptoms: Traffic does not flow through the hub.

Conditions: The symptom is observed when a Cisco 3900 series router is configured for VRF-aware tunnel protection for IKEv2 sessions.

Workaround: There is no workaround.

- CSCtf71990

  Symptoms: An alert message is not sent if “source-ip-address” is configured in the call-home configuration. The following message is shown:

  ```
  %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP servers (ERR
  7, error in connecting to SMTP server)
  ```

  Conditions: The symptom is observed when “source-ip-address” is configured.

  Workaround: Remove “source-ip-address”.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: The symptom is observed with the following setup and configuration:

  ```
  Router 1:
  interface e0/0
  ip address 192.168.1.1 255.255.255.0
  bfd interval 51 min_rx 51 multiplier 4
  bfd echo
  no shut
  exit

  interface loopback 0
  ip address 10.10.1.1 255.255.0.0
  exit
  ip route static bfd e0/0 192.168.1.2
  ip route  10.20.0.0 255.255.0.0 e0/0 192.168.1.2

  Router 2:
  interface e0/0
  ip address 192.168.1.2 255.255.255.0
  bfd interval 51 min_rx 51 multiplier 4
  bfd echo
  no shut
  exit

  interface loopback 0
  ip address 10.20.1.1 255.255.0.0
  exit

  ip route static bfd e0/0 192.168.1.1
  ip route  10.10.0.0 255.255.0.0 e0/0 192.168.1.1

  interface e0/0
  no ip route static bfd e0/0 192.168.1.1
  ```

  Though the BFD state is DOWN the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

  Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtf79264

  Symptoms: A Cisco route processor (RP) loses part of its odr-route for the spoke network. With a busy network, and with more than 1000 spokes, the second RP can have the same symptom.

  Conditions: This symptom is observed with a default odr timer.

Workaround: Modifying the odr timer can help, but will not solve the problem.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- CSCtf95308

  Symptoms: Router crashes on modifying the radius profile and including unexpected values in it, such as empty strings and strings with special characters.

  Conditions: This symptom is seen during an active ISG with sessions coming up and going down.

  Workaround: Avoid changing the radius profile values with active sessions.

- CSCtg08496

  Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg13269

  Symptoms: On peers of Route Reflectors (RR), the received prefixes counter shows an incorrect number when session flaps occur during a network churn.

  Conditions: The symptom is observed with BGP RRs.

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

- CSCtg18555

  Symptoms: A memory leak is observed with process_online_diag_pak.

  Conditions: This symptom is observed on a card supporting TestNonDisruptiveLoopback and TestFabricChHealth tests.

  Workaround: Disable the HM tests TestNonDisruptiveLoopback and TestFabricChHealth on line cards to stop the leak.

- CSCtg19546

  Symptoms: MPLS forwarding of labeled frames across a tunnel may fail. This symptom arises when an incorrect TAG adjacency is created for the tunnel.

  Conditions: This symptom is observed when adding or removing crypto and a tunnel protection configuration from a tunnel interface also configured with MPLS. When this symptom occurs, an incorrect or missing IPSec post encap feature is observed under the TAG adjacency for the tunnel.

  Workaround: Removing the crypto and/or removing and reconfiguring mpls ip from the tunnel can recover connectivity.

  Alternate Workaround: VTI cannot be combined with MPLS label switching, since IPSec can only encapsulate IP packets, not MPLS packets. This is due to design. In GRE mode, however, this is possible, so use a GRE tunnel with IPSec tunnel protection along with MPLS label switching. Be sure to remove and reapply the “tunnel protection ipsec profile” configuration so that IPSec features will be properly applied to the IP-and MPLS-switching feature paths.

- CSCtg22080

  Symptoms: Memory leak occurs at crypto_ca_cert_hexmode_quit_function.

Conditions: This symptom occurs at crypto_ca_cert_hexmode_quit_function.

Workaround: There is no workaround.

- CSCtg22674

  Symptoms: The router experiences high CPU for several minutes due to “MPLS TE LM” process.

  Conditions: This symptom occurs when a router has many (perhaps as few as 100) MPLS TE tunnels that traverse over a link which experiences repeated flapping in a short duration.

  Workaround: There is no workaround.

  Further Problem Description: Use the command **show process cpu** to determine CPU utilization. If this problem exists, the MPLS TE LM process holds greater than 90% resources for 5 minutes or more.

```
CPU utilization for five seconds: 100%/0%; one minute: 100%; five minutes: 
100%
   PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   216   867694836  18357673      47266 99.67% 99.09% 99.11%   0 MPLS TE LM
```

- CSCtg26538

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

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

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

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

  Workaround: There is no workaround

- CSCtg28806

  Symptoms: Router crashes at PKI manual enroll.

  Conditions: The symptom is observed on a Cisco 2921 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg41606

  Symptoms: With Reverse Route Injection (RRI) configured with the **reverse-route** command, if the crypto map is applied to a multi-access interface (e.g.: ethernet) then egress traffic may fail when the router cannot populate an ARP entry for the crypto peer address.

Conditions: The symptom could occur when the upstream device does not support proxy arping.

Workaround: Use the **reverse-route remote-peer** *next-hop-ip* command instead of just **reverse-route**.

- CSCtg41733

  Symptoms: Certain crafted packets may cause a memory leak in the device in very rare circumstances.

  Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.

  Workaround: Disable SIP if it is not needed. To protect infrastructure devices and minimize the risk, impact, and effectiveness of direct infrastructure attacks, administrators are advised to deploy infrastructure access control lists (iACLs) to perform policy enforcement of traffic sent to infrastructure equipment. Administrators can construct an iACL by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. For the maximum protection of infrastructure devices, deployed iACLs should be applied in the ingress direction on all interfaces to which an IP address has been configured. An iACL workaround cannot provide complete protection against these vulnerabilities when the attack originates from a trusted source address.

  The iACL policy denies unauthorized SIP packets on TCP port 5060 and 5061 and UDP port 5060 that are sent to affected devices. In the following example, 192.168.60.0/24 is the IP address space that is used by the affected devices, and the host at 192.168.100.1 is considered a trusted source that requires access to the affected devices. Care should be taken to allow required traffic for routing and administrative access prior to denying all unauthorized traffic. Whenever possible, infrastructure address space should be distinct from the address space used for user and services segments. Using this addressing methodology will assist with the construction and deployment of iACLs.

  Additional information about iACLs is in Protecting Your Core: Infrastructure Protection Access Control Lists.

```
ip access-list extended Infrastructure-ACL-Policy

     !
      !-- Include explicit permit statements for trusted sources
      !-- that require access on the vulnerable protocols and ports
      !
      permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060
      permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5061
      permit udp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 5060

      !
      !-- The following vulnerability-specific access control entries
      !-- (ACEs) can aid in identification of attacks
      !

      deny tcp any 192.168.60.0 0.0.0.255 eq 1720
      deny tcp any 192.168.60.0 0.0.0.255 eq 5060
      deny tcp any 192.168.60.0 0.0.0.255 eq 5061
      deny udp any 192.168.60.0 0.0.0.255 eq 5060

      !
      !-- Explicit deny ACE for traffic sent to addresses configured within
      !-- the infrastructure address space
      !

      deny ip any 192.168.60.0 0.0.0.255

     !
      !-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
      !-- with existing security policies and configurations
      !
      !-- Apply iACL to interfaces in the ingress direction
      !

    interface GigabitEthernet0/0
     ip access-group Infrastructure-ACL-Policy in
```

Note that filtering with an interface access list will elicit the transmission of ICMP unreachable messages back to the source of the filtered traffic. Generating these messages could have the undesired effect of increasing CPU utilization on the device. In Cisco IOS Software, ICMP unreachable generation is limited to one packet every 500 milliseconds by default. ICMP unreachable message generation can be disabled using the interface configuration command no ip unreachables. ICMP unreachable rate limiting can be changed from the default using the global configuration command ip icmp rate-limit unreachable interval-in-ms.

More information about how to detect and mitigate this type of issues can be found at the Cisco Applied Mitigation Bulletin: "Identifying and Mitigating Exploitation of the Multiple Vulnerabilities in Cisco Voice Products" at the following link:

http://www.cisco.com/warp/public/707/cisco-amb-20100922-voice.shtml

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2010-4683 has been assigned to document this issue.

Additional information on Cisco’s security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtg42904

  Symptoms: Router crashes with the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address after applying the flow monitor to
  virtual-template interface
  ```

  Conditions The symptom is observed on a router configured with EasyVPN.

  Workaround: There is no workaround.

- CSCtg44108

  Symptoms: Bus error crashes occur frequently.

  Conditions: This symptom is observed on a Cisco 3945e Integrated Services Router (ISR) that is running Cisco IOS Release 15.1(1)T. IPSec is configured on a GRE multipoint tunnel interface.

  Workaround: There is no workaround.

- CSCtg49109

  Symptom: After a switchover, some of the modules go to MajFail state.

  Conditions: This issue is observed when high traffic is triggered, a lot of packets are dropped by the platform, and numerous IPC messages time out.

  Workaround: There is no workaround.

  Further Problem Description: Due to some unexpected events, one of the IPCs boolean “IPC message blocked” is failing to get set (that is, failing to get unblocked), which is in turn blocking the ICC process from processing further messages. This results in the failure.

- CSCtg49331

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

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

  Workaround: Use ingress replication mode. If egress replication mode is used and the issue is present, service can be restored by using this command:

  clear ip mroute *A.B.C.D*

  Or perform a shut/no shut on the affected interface.

- CSCtg50024

  Symptoms: A router experiences crashes due to TLB (load or instruction fetch) exception.

  Conditions: This problem is observed on a Cisco 7206VXR router with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg52885

  Symptoms: The HSRP state on dot1q sub-interfaces remain in INIT state.

  Conditions: This symptom is observed after a physical link flap on a trunk port.

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

- CSCtg53953

  Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (neighbor *ip-address* disable-connected-check, neighbor *ip-address* peer-group pgrp, and others).

  Conditions: This symptom applies only to situations where *ip-address* is the IP address of a peer that has a dynamically created session (a neighborship that is the result of the “bgp listen range ...” feature).

  Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg55338

  Symptoms: If a router is reloaded with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source, the crypto socket is not created and IPSec is not triggered.

  Conditions: This symptom is observed on a Cisco router with a GRE tunnel interface configured with tunnel protection and a dialer interface as the tunnel source.

  Workaround: After the reload, remove and reapply the tunnel protection on each tunnel interface.

- CSCtg55447

  Symptoms: GETVPN keyserver TEK sequence number goes out of sync during network split/KS failure. This causes the GM to reject the older key and reregister.

  Conditions: This symptom is seen during primary keyserver failure or network failure between primary keyserver and secondary keyserver.

  Workaround: There is no workaround.

- CSCtg57831

  Symptoms: In the event of a failover, there is a serial number mismatch on the active and standby.

Conditions: The symptom is observed in an High Availability CA servers environment, using Cisco IOS Release 15.0(1)M2.

Workaround: There is no workaround.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

  Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

  Workaround: There is no workaround.

- CSCtg59328

  Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  Conditions: This symptom is observed when the following tasks are completed:

  - Bring up a PPPoE session and ensure that it is synced to standby.
  - From the PPPoE client run the commands **no ip address** followed by **ip address negotiated** under the Virtual- template interface.
  - As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP re-negotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

  Workaround: There is no workaround.

- CSCtg60302

  Symptoms: CPP ucode crashes after shutting down mpls-te tunnel interfaces.

  ixia ------PE1 ------------PE2 --------------ixia

  This is a 6PE topology with an MPLS TE tunnel between PE1 and PE2 and traffic passing through the TE tunnel. When the TE is shut down, the CPP crashes.

  Conditions: This symptom is observed when the traffic rate is about 500 packets per second.

  Workaround: There is no workaround.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link, it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: The symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a **shut** and **no shut** on the local P2P interface.

- CSCtg73798

  Symptoms: After one or more line card resets or online insertion/removals (OIRs), an MPLS xconnect virtual circuit may come up but reports a TX fault to the LDP peer.

  Conditions: The symptom may occur on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE or later, Release 12.2(33)XNC or later, or Release 15.0(1)S or later.

  Workaround: Remove and reapply the relevant xconnect configuration.

- CSCtg75452

  Symptoms: RP crashes in dual RP system after doing a **config replace** on POS-configured SDH link.

  Conditions: The symptom is observed if you configure a POS SDH link on a 1XCHSTMOC12/DS0 SPA port and do a **config replace** to a basic router configuration that includes redundancy mode change. This crashes the RP and produces a core file.

  Workaround: There is no workaround.

- CSCtg79262

  Symptoms: A Cisco IOS Embedded Event Manager (EEM) Tool Command Language (Tcl) policy can get stuck in the EEM active scheduler queue. The policy will consume a scheduler thread and cannot be cleared automatically by the maxrun timer or manually using the EEM exec command **event manager scheduler clear all**.

  Conditions: This symptom occurs in very rare circumstances. For example, if the system has enough memory to schedule and start running the EEM policy, but the policy fails due to a lack of memory.

  Workaround: The only way to recover is to reload.

- CSCtg89960

  Symptoms: “no ipv6 spd queue max-threshold *spd value*” causes standby to reload.

  Conditions: This symptom occurs Cisco IOS c7600 router having dual RP and running c7600s72033-adventerprisek9-mz.150-0.12.S image.

  Workaround: There is no work around.

- CSCtg92587

  Symptoms: High CPU in the SNMP Engine process is observed every five minutes.

  Conditions: This symptom occurs when SNMP queries are performed on TE MIB with hundreds of TE tunnels configured.

  Workaround: There is no workaround.

- CSCtg93243

  Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

  Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used packets get forwarded after decryption as expected.)

  Workaround: There is no workaround.

- CSCtg95940

  Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

  Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

  Workaround: There is no workaround.

  Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCtg98116

  Symptoms: An ES-20 crashes on performing a **config copy** from startup-config to running-config.

  Conditions: The symptom is observed with a 4k EVC and QoS policy attached to the EVC when a **config copy** is performed from startup-config to running-config.

Workaround: There is no workaround.

Further Problem Description: ES-20 recovers and works fine after the crash.

- CSCth00317

  Symptoms: When a large number of service groups are configured with multiple service instances on a port-channel, the following anomaly is observed: on addition of a new member-link, not all the policies applied to the port- channel will be configured in the line card.

  Conditions: The symptom is observed upon adding a new member-link (having large policies) to the EVC port-channel.

  Workaround 1: Do a shut/no-shut of the member link.

  Workaround 2: Reset the line card on configuration of the port-channel.

- CSCth02812

  Symptoms: A prolonged unicast flood can be seen on an ingress path after a TCN event. The flood will last until entries in the arp table are refreshed.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SXH3a (issue has been tracked back to Cisco IOS Release 12.2(18)SXF in an L2 asymmetric environment. The flood is only seen if there is no bi-directional flow on the switch. This issue can be seen in all STP modes.

  Workaround: Clearing ip arp will correct this issue. Lowering the arp timeout will also minimize the impact of the flood.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCth05476

  Symptoms: On router bootup, the SIP200 line card is flooded with "%CWSLC-3- DIAGFAIL: Failed to handle diag" messages.

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

  Workaround: There is no workaround.

- CSCth08962

  Symptoms: A single bit error in the SRAM of the ATM SPA will generate the following error message:

  ```
  EST5EDT,M3.2.0/: spa_atm_v2[241]: SPA ATM4/2 SAR: An error was reported by SAR
  firmware (unsolicited msg): Description: Single-bit SRAM ECC correctable error. [Error
  code 4]
  ```

  It does not cause an operation impact, but the error message will repeat every 6 seconds.

  Single bit correctable errors should be counted but not display an error message since the information is already corrected by parity. Also the rate of these messages may increase during certain conditions, which may choke the queues on the platform.

Conditions: This symptom occurs under normal operating conditions.

Workaround: There is no workaround.

- CSCth09876

  Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto- discovered if IP SLAs are removed from the responder first.

  Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

  Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth13415

  Symptoms: One way audio in call transfer due to 491 response during resume re- INV.

  Conditions: The symptom is observed when you have an UPDATE message passing through the CUBE and then a re-INV crossover happens. The re-INV crossover results in a 491 but the 491 is not correctly forwarded by the IPIP GW. This can result in one way audio issues if the crossed over re-INV was changing the media state from hold to resume.

  Workaround: There is no workaround.

- CSCth14305

  Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

  Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

  Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth15105

  Symptoms: BFD sessions flap after unplanned SSO (test crash).

  Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

  Workaround: There is no workaround.

- CSCth16011

  Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- CSCth16962

  Symptoms: Primary KS KEK timer gets stuck or reset to zero after a GDOI policy change and rekey. Once the KEK timer gets stuck/reset to zero, there are repeated rekeys, which will impact the whole GET VPN domain. The trigger occurs after a failure event in the primary key server and the secondary key server becomes primary followed by a policy change.

  Conditions: This symptom occurs when KEK timer gets stuck at Zero and there are repeated rekeys to GMs resulting a rekey storm.

  Workaround: There is no workaround.

- CSCth19516

  Symptoms: A router crashes if you have PFR and SAF enabled on the same device.

Conditions: The issue is seen when you have SAF enabled and PFR with multiple links. When the network gets congested or delay is seen and if there is a change over from IN-POLICY state to OOP the router crashes.

Workaround: Disable SAF completely and reload the router.

- CSCth23814

  Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

  Conditions: This symptom is observed when a monitor is configured with a flow record that has the “BGP next hop” field configured.

  Workaround: Ensure that the “BGP next hop” field is not configured for a flow.

- CSCth24984

  Symptoms: High CPU usage is seen when the RP is working as a DMVPN hub.

  Conditions: The symptom is observed when there is 1000 static BGP neighbors (spokes) over MVPN.

  Workaround: There is no workaround.

- CSCth25634

  Symptoms: Password is prompted for twice for authentication.

  Conditions: This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example: aaa authentication login default group radius line

  Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example: enable password *keyword* aaa authentication login default group radius enable.

  Further Information: The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the “line’’ authentication method is configured with fallback to the “none’’ authentication method. In other words, if the following is configured:

  ```
  aaa new-model
  aaa authentication login MYMETHOD line none
  line con 0
    login authentication MYMETHOD
    password <some password>
  ```

  then users providing the wrong password at the password prompt will be granted access.

- CSCth33949

  Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

  Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

  Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth35515

  Symptoms: Line card crash could occur on an SSO when a router runs MPLS.

  Conditions: This symptom may occur when multiple back to back switchovers occur.

  Workaround: There is no workaround.

- CSCth36114

  Symptoms: A crash is seen after executing the **write memory** command via SDM.

Conditions: The symptom is observed on a Cisco 1841 platform that is running Cisco IOS Release 15.1(1)T.

Workaround: Use Cisco IOS 12.4 versions.

- CSCth37092

  Symptoms: A crash is observed in the PKI-HA feature when the standby tries to sync up with the active router.

  Conditions: When the PKI server is created on the active router with a "database archive password" configuration, the PKI server is cloned on the standby. Soon after, the active router crashes.

  Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing "bgp dampening".

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4. - eBGP + VPNv4 peer session is established and DUT.
  - Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net's topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth40213

  Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

  Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

  Workaround: There is no workaround.

- CSCth41801

  Symptoms: Flows get stuck in LC, even though the RP flow times out and the HPLA flows are removed. If we have reached the LC flow limit when this happens, new flows may not be learnt even though the number of active flows in the system is less than the LC scale value.

  Conditions: This symptom is observed when the hardware timeout value is greater then the software timeout value. In this case, the code ignores the event from RP and does not delete the count from the LC table. In such a scenario, if the LC flow limit has been reached, new flows would not be learnt even though existing flows get timed out.

  Workaround: The only workaround in such a situation is LC OIR, which may not be acceptable. This issue can be avoided if the HW timeout value is less than the SW timeout value.

- CSCth42798

  Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

  Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

  Workaround: There is no workaround.

- CSCth55579

  Symptoms: Router reloads at clean_out_RA_certs after enrolment with CA server.

  Conditions: The symptom is observed after enrolment with CA server.

Workaround: There is no workaround.

- CSCth60232

  Symptoms: The port-channel interface may flap when adding or removing a VLAN from the trunk on a port-channel interface when one or more interfaces are in a state other than P or D.

  Conditions: This symptom is observed only when the port-channel interface has interfaces in states other than P or D.

  Workaround: Shut down the non-P members and make the vlan changes.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate the video stream.

  Conditions: This symptom is observed in two scenarios:

  Scenario 1: This symptom was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

  ```
  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server
  ```

  1. Call is originated by 7985
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response

     m=video 53722 RTP/AVP 96 97 34 31

     b=AS:1920

     a=rtpmap:96 H264/90000

     a=fmtp:96 profile-level-id=42e016;max-mbps=108000;max-fs=3600

     a=rtpmap:97 H263-1998/90000

     a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1

     a=rtpmap:34 H263/90000

     a=fmtp:34 CIF4=1;CIF=1;CIF=1;QCIF=1

     a=rtpmap:31 H261/90000

     a=fmtp:31 CIF=1;QCIF=1

     a=sendrecv
  3. CUBE sets video m-line to 0 in the SDP of the SIP “ACK” response

     m=video 0 RTP/AVP 96

  Scenario 2: End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

  CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

  Workaround: There is no workaround.

- CSCth64271

  Symptoms: Routers in redundant configuration end up in Manual Swact = disabled.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth64316

  Symptoms: Unable to configure “radius-server” using SNMP set.

  Conditions: The symptom is observed when you configure via SNMP MIB.

Workaround: Radius server can be configured through the CLI.

- CSCth66177

  Symptoms: The standby route processor (RP) triggers an active RP crash.

  Conditions: This problem is observed when the standby RP crashes due to a memory parity error.

  Workaround: There is no workaround.

- CSCth66604

  Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).

  Conditions: The symptom is observed with an ISSU upgrade or downgrade.

  Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.

- CSCth67788

  Symptoms: sVTI stops forwarding traffic when a local policy is configured on a device.

  Conditions: The symptom has been observed on a router that is running Cisco IOS Release 15.0(1)M1.

  Workaround 1: Do not use a local policy.

  Workaround 2: Configure "no ip route-cache cef" on the tunnel interface.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCth70437

  Symptoms: Crypto sessions drop after the following error message:

```
000059: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D91910, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000060: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D91CE4, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000061: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D920B8, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
000062: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=83D82F8C, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
0x8039460Cz 0x80397B40z
```

  Conditions: This symptom is observed on Cisco IOS 8XX series routers and when crypto is applied to dialer interface.

  Workaround: There is no workaround.

- CSCth71349

  Symptoms: Some SSS sessions are staying in "attempting" state for a while when using ISG Static Session Creation.

  Conditions: The symptom is observed when using ISG Static Session Creation.

  Workaround: Stop incoming traffic from subscribers and wait until the sessions recover, then re-apply the traffic.

- CSCth74953

  Symptoms: The SPI value is shown as 0x0, hence the ipsec sa validation is failing.

  Conditions: This symptom is observed when the crypto profiles are being applied. The symptom is not observed with simple crypto maps.

  Workaround: There is no workaround.

- CSCth82164

  Symptoms: A peer's key is cached indefinitely in the key cache.

  The following messages indicate bypassing the revocation check:

  ```
  *Jul 13 18:43:18.095: ISAKMP:(1002): peer's pubkey is cached
  *Jul 13 18:43:18.095: CRYPTO_PKI: Found public key in hash table. Bypassing
  certificate validation
  ```

  Conditions: A method (OCSP, CDP, etc.) to check for certificate revocation is used, then it is changed to "none" ("'revocation check none''), and finally it gets changed to some revocation method again.

  This configuration transition "'revocation check -> no revocation check -> revocation check'' is what causes a problem.

  Workaround: There is no workaround.

  Further Information: The problem is independent of which revocation method is used (OCSP, CDP). The problem will happen when revocation check is disabled with the command "revocation none''. This would cache the peer's key infinitely into the cache. After this, turning on any revocation method will have no effect; validation will always succeed since the keys are cached.

  The problem will only happen if someone turns off revocation and then later realizes that it was a mistake and turns it back on. If remote peer's key is cached within that period then that cache entry will never be deleted. End Result: If the same remote peer tries to establish the tunnel again we would bypass validation and would not check if it is still a valid peer or not.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.0/4.1:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:U/RC:C

  CVE ID CVE-2011-0935 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCth84714

  Symptoms: With scaled number of MLP bundles on Sip200 with DLFI enabled, the sip200 crashes.

  Conditions: This symptom occurs with the following conditions:

  1. Reload the SPA having MLP bundles.
  2. Shut/no shut the controller.
  3. Flap the links by any other means.

  Workaround: The issue is not seen without high traffic and without LFI enabled.

- CSCth84995

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

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

Workaround: There is no workaround.

- CSCth85618

  Symptoms: Extra syslog gets printed but no other functionality is impacted.

  Conditions: This symptom occurs under normal conditions.

  Workaround: There is no workaround.

- CSCth87195

  Symptoms: Flexwan ATM interface goes down.

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

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

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have "neighbor *neighbor address* prefix-list out" configured under "address-family nsap" under "router bgp" when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with "nsap address-family".

- CSCth92171

  Symptoms: The serial interface stays down longer if a switchover is done while flapping the multilink interface from the far end.

  Conditions: This symptom is observed when switching over to the standby while flapping the multilink interface from the far end.

  Workaround: Shut the flapping links, then perform the switchover.

- CSCth93218

  Symptoms: The error message "%OER_BR-4-WARNING: No sequence available" displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCth94814

  Symptoms: Crash is seen in static route component.

  Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

  Workaround: There is no workaround.

- CSCth94827

  Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

  Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

  Workaround: There is no workaround.

- CSCth96398

  Symptoms: Local MPLS labels change after an SSO causing a traffic drop a for short period of time.

  Conditions: The symptom is observed when LDP graceful restart is configured and SSO is supported on the platform. Only the prefixes which have a local label but not a remote label before the SSO are affected. After SSO, these prefixes get assigned a new local label. The traffic should recover once the LDP neighbors learned the new labels.

  Workaround: There is no workaround.

- CSCth99021

  Symptoms: Spurious memory access at hqf_send_blt_msg_to_linecards is seen on performing SSO switchover. Some times the router crashes with the same decode.

  Conditions: The symptom occurs on performing an SSO switchover.

  Workaround: There is no workaround.

- CSCth99104

  Symptoms: Certificate that should not be allowed bypasses validations checks.

  Conditions: This happens when the PKI validation test command is used.

  Workaround: Do not use the PKI validation test command.

  Further Information: The PKI validation test command invokes the pubkey insert api which erroneously adds pubkey entries when at times it should not. this results in all subsequent validations bypassed for the same certificate.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.7/1.4:

  https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:L/AC:L/Au:S/C:P/I:N/A:N/E:F/RL:OF/RC:C/CDP:ND/TD:ND/CR:ND/IR:ND/AR:ND

  No CVE ID has been assigned to this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

  Conditions: The symptom is observed under the following conditions:

  1. If the client starts to send LCP echo requests during the PPP Authentication phase.
  2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

  Workaround: There is no workaround.

- CSCti02076

  Symptoms: On a system running Cisco IOS, after unconfiguring an IPv6 link- local address from an interface, any global ipv6 addresses may disappear.

  Conditions: This issue may occur on systems running Cisco IOS when IPv6 is being configured. This issue occurs if an attempt is made to remove the IPv6 link-local address without use of the **link-local** keyword.

  Workaround: There is no workaround.

- CSCti03199

  Symptoms: During switch-over, standby crashes after every recovery due to config-sync.

  Conditions: The symptom is observed when the standby tries to sync with the active and when "crypto pki trustpoint" is configured with an unavailable port-channel as source-interface.

  Workaround: There is no workaround.

- CSCti04670

  Symptoms: A crash may occur while the system is in flux with iEdge sessions going up and down while at the same time the **show ssm** command is issued on the console.

  Conditions: This symptom is seen when issuing the **show ssm** command.

  Workaround: Issue the **show ssm** command and then show logging to see the results.

- CSCti05663

  Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

  Conditions: The symptom is observed in the case of an numbered relay.

  Workaround: There is no workaround.

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are "IN" policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go "Out" of policy.

  Workaround: There is no workaround.

- CSCti08811

  Symptoms: A router running Cisco IOS may reload unexpectedly when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip
    version 2
    no validate-update-source
    network 10.0.0.0
    no auto-summary
    !
    address-family ipv4 vrf test
  ```

```
   no validate-update-source
   network 172.16.0.0
   no auto-summary
   version 2
  exit-address-family
```

and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

Workaround: There is no workaround.

- CSCti15990

  Symptoms: EzVPN will not come up if the dialer interface flaps.

  Conditions: This symptom is observed when the dialer interface is profile- based.

  Workaround: If deploying with PPPoA is not a constraint, then using non-profile based dialer interface as ezvpn outside interface will solve the issue. Other wise there is no workaround.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP out-of-sync with the active RP. A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, the router is in HA mode SSO, and is reloaded from the RP.

  Workaround: Perform a Shut/no shut of the affected interfaces.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. List > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti22190

  Symptoms: The EIGRP autonomous system command does not NVGEN.

  Conditions:

```
interface Tunnel2
 ip vrf forwarding vpn2
no ip next-hop-self eigrp 10
```

  Now configure the address-family ipv4 command under legacy mode. For example:

```
router eigrp 10
no auto-summary
address-family ipv4 vrf vpn2
 no auto-summary
```

Now show the running configuration; the autonomous system command is not NVGENed.

Workaround: Use the **address-family ipv4 vrf vpn2 autonomous 10** command.

- CSCti22544

  Symptom: IKE fails to come up while using RSA signature. PKI debugs show the following message:

```
PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example, crypto pki trustpoint yni-u10 enrollment.

  Workaround: There is no workaround.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- CSCti25319

  Symptoms: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute Open Shortest Path First (OSPF) is configured.

  Conditions: This symptom occurs only for those configurations in which a network mask covers multiple supernets. For example, for the following network statement,

```
router ospf 1
network 192.168.0.0 0.255.255.255 area 0
the above mentioned symptom occurs if the interfaces are configured with IP
addresses as follows:
    ip address 192.168.0.1 255.255.255.0
    ip address 192.168.1.1 255.255.255.0
    and so on.
```

  Workaround 1: Enable OSPF using interface command “ip ospf *AS* area”

  Workaround 2: Configure multiple network statements with mask/wildcard equal to supernet as shown in the example below:

```
router ospf 1
    network 192.168.0.0 0.0.0.255 area 0
    network 192.168.1.0 0.0.0.255 area 0
    and so on.
```

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2010-3050 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCti25780

  Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

  Conditions: This symptom is observed when some of the files are compiled with optimization.

  Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti26852

  Symptoms: Router crashes at ppp_sip_sw_session_cleanup.

  Conditions: The symptom is observed with multilink PPP scaled configurations and with a Cisco 7600 series platform. The crash may be seen following a SPA OIR. The crash decode is:

```
sw_mgr_sm_valid_seg_class (seg_class=0x30343408)
at ../xconnect/seg_sw_mgr_util.c:443
#1  0x120ab814 in sw_mgr_get_segtype (seg_class=0x30343408)
at ../xconnect/seg_sw_mgr_util.c:478
#2  0x1435cd2c in ssf_dp_drop_remove_L2_context (seg1_class=0x30343408)
at ../machine/../sss/ssf_switching_registry.regh:173
#3  0x1435d48c in ssf_dp_remove_dp_only_L2_features (seg_class=0x30343408)
at ../sss/ssf_switching_util.c:113
#4  0x11c850f8 in ppp_sip_sw_session_cleanup (session=0x3a1c54f0)
at ../VIEW_ROOT/cisco.comp/ppp/core/src/ppp_sip_switching.c:537
```

  Workaround: There is no workaround.

- CSCti28710

  Symptoms: Chunk memory leak is observed on oer_mc_nfc_add_template and oer_mc_nfc_get_source

  Conditions: This symptom occurs on oer_mc_nfc_add_template and oer_mc_nfc_get_source.

  Workaround: Change the border IP address.

- CSCti31984

  Symptoms: Router crashes.

  Conditions: This symptom occurs when "Show stats" is used to show auto Ethernet monitor operation.

  Workaround: There is no workaround.

- CSCti32498

  Symptoms: Ingress HQoS policy queues are removed after LC OIR on subinterface.

  Conditions: This symptom occurs when flat SG having shaper is applied in ingress on subif and HQoS queueing policy is applied on subif.

  Workaround: There is no workaround.

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when "next-hop-unchanged allpaths" is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

  ```
  route-map static-nexthop-rewrite permit 10
  match source-protocol static
   set ip next-hop <router ip address>
  !
  router bgp <asn>
   address-family ipv4 vrf <vrf name>
   redistribute static route-map static-nexthop-rewrite
   exit-address-family
   exit
  exit
  ```

  Workaround 2: Instead of configuring static routes with a next-hop, specify an interface name.

  For example, if you had:

  ip route x.x.x.x 255.255.255.0 y.y.y.y

  And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

  ip route x.x.x.x 255.255.255.0 interface serial2/0

  Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

  When used in conjunction with the newly added configuration:

  ```
  router bgp <asn>
   address-family vpnv4 unicast
    bgp route-map priority
  ```

  The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34462

  Symptoms: After FPD upgrade, a **shut** on the active shows **no shut** on the standby.

  Conditions: The symptom is observed after an FPD upgrade.

  Workaround: Perform a **no shut** then shut the interface on the active to sync it properly.

- CSCti34627

  Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

  Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

  Workaround: Disable GR.

- CSCti34795

  Symptoms: In RA mode, SCEP enrolment requests stay in pending status. They will not time out automatically and cannot be cancelled with the **no crypto pki enroll** *tp*.

  Conditions: The symptom is observed when “enrolment mode ra” is configured under the Trust-Point.

  Workaround: Do not use RA mode, although in certain environments it is not scalable.

- CSCti39902

  Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

  Conditions: Configure RRI on the UUT.

  Workaround: There is no workaround.

- CSCti43395

  Symptoms: Tracebacks are seen during DHCP message exchange. Crash may also be seen with the tracebacks.

  Conditions: This symptom is seen when DHCP relay agent is configured with “ip dhcp relay information option vpn” and clients with duplicate MAC address are coming in at the same time.

  Workaround: Unconfigure “ip dhcp relay information option vpn”. Or, disallow clients with duplicate MAC.

- CSCti45732

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

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

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

- CSCti47550

  Symptoms: With a scaled L3 ACL on EVC on ES+ line cards, some of the ACEs do not work, while others work as normal.

  Conditions: The symptom is observed when the line card or router is reloaded with the ACL configuration present.

  Workaround: Remove and add ACL on the EVC.

- CSCti48014

  Symptoms: A device reloads after executing the “show monitor event *comp*... all detail” command (where *comp* is an option listed under “show monitor event ?”).

  Conditions: This symptom is observed if the configurations are done in the order below:

  ```
  monitor event-trace <comp> stacktrace <depth>
  monitor event-trace <comp> size <size value>
  ```

  and any related event gets recorded in between the above two configurations.

  Workaround: To avoid the crash, change the order of the above configurations; that is, configure the **size** command first and then configure the **stacktrace** command.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- CSCti49472

  Symptoms: System "accounting off" record is seen with suppress-CLI enabled.

  Conditions: With AAA CLI for suppressing system accounting records on switchover enabled, "Accounting OFF" is sent from a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCti49508

  Symptoms: The command **show platform isg session all** displays stale entries on a Cisco 7600 series router for ISG sessions that are not on the router.

  Conditions: This symptom is observed under the following conditions:

  1. A number of port channel subinterfaces are configured with ISG
  2. ISG sessions are active on the subinterfaces
  3. The main port channel is removed without removing the sessions or ISG configuration from the individual port channel subinterfaces, using the **no interface port-channel** <> command

  Workaround: There is no workaround.

  To avoid this symptom:

  1. Delete the session/ISG configuration from the individual port channel subinterface
  2. Then delete the port channel.

- CSCti50419

  Symptoms: For PPPoMPLS/HDLCoMPLS pseudowires, after you perform the switchover, traffic loss is seen and CE interfaces stay down.

  Conditions: The symptom is observed on performing an SSO switchover with PPPoMPLS and HDLCoMPLS pseudowires. The control word gets programmed incorrectly on the line card leading to traffic loss.

  Workarounds:

  1. Unprovision and provision the pseudowire.
  2. Perform a SPA OIR.

- CSCti50607

  Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

  Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

  Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  - The non-reloading device must have a "neighbor x.x.x.x transport connection- mode passive" configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword "established" or "eq bgp".
  - It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
  - When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
  - Both peers must be multisession capable.
  - "transport multi-session" must not be configured on either device, or enabled by default on either device.
  - "graceful restart" must not be configured.

  Workarounds:

  1. Remove the configuration "neighbor x.x.x.x transport connection-mode passive" or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure "neighbor x.x.x.x transport multi-session" on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command.
  4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**.
  5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

  Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where "neighbor x.x.x.x transport single-session" is configured and NSF is not configured.

  The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

  Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the Cisco IOS Release 12.2(33)SB router is the one not reloading.

- CSCti53664

  Symptom: CoPP hardware counters not incrementing when **sh policy-map control-plane** command is run for traffic coming on ES20+ cards.

  Conditions: This symptom is observed when CoPP is configured and traffic is coming in on ES20+, which is destined to switch the ip address.

Workaround: Move the l3 interface from the switch for the traffic coming in on ES20+ line cards.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti56980

  Symptoms: Applying a service-policy under an interface or subinterface on an ES+ card in a Cisco 7600 series router may fail with the following error:

  random-detect aggregate is not supported in output direction for this interface Configuration failed!

  Conditions: The symptom only occurs when a SIP400 is being replaced by an ES+ card on which the QoS configuration will be applied.

  Workaround: Reload the router with the ES+ card installed.

- CSCti58027

  Symptoms: MPLS TE FRR fails on P2MP tunnels.

  Conditions: This symptom occurs on Cisco IOS c7600 series routers that are running Cisco IOS Release 15.0(1)S and when the following conditions are met:

  - Link protection configured for primary tunnel.
  - Incoming, primary output, and secondary output interfaces are all on the same line card.

  Workaround: Move the input interface to another slot.

- CSCti58272

  Symptoms: A PKI server with the **grant auto trustpoint** command will crash on client re-enrolment if PKI-AAA is enabled on the trustpoint associated with the **grant auto** command.

  Conditions: If trustpoint “pki-trustpoint” contains an authorization list PKI- AAA option, and pki-trustpoint is used as the “grant auto trustpoint” option on the PKI server:

```
!
crypto pki server ca-server
  ...
  grant auto trustpoint pki-trustpoint
  ...
crypto pki trustpoint pki-trustpoint
  authorization list aaa
!
```

  The device crashes whenever a re-enrolment attempt is made to the PKI server.

  Workaround: Remove authorization list from the trustpoint (and skip the PKI- AAA process).

- CSCti59562

  Symptoms: DHCP accounting stop does not clear IP initiated sessions and radius-proxy sessions.

  Conditions: This symptom occurs when VRF mapping is being used.

  Workaround: There is no workaround.

- CSCti59656

  Symptoms: When a TP tunnel is configured on a distributed system, the adjacencies are not in sync between the active and standby.

Conditions: Configure TP tunnel in a distributed system.

Workaround: There is no workaround.

- CSCti61949

  Symptoms: Unexpected reload with a "SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header" and "chunk name is BGP (3) update" messages.

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

  Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti62125

  Symptoms: When a 67XX card is inserted in slot 2 of a 7606-S chassis, then other cards (such as ES+, ES, and SIP) in the other slot face fabric CRC errors. The ES+ in the other slot gets hung and leads to a crash.

  Conditions: The symptom is observed when a 67XX card is inserted in slot 2 of a 7606-S chassis.

  Workaround: There is no workaround.

- CSCti62267

  Symptoms: An IPv6 CEF output is not seen in SP.

  Conditions: This symptom is observed when IPv6 is configured on UUT. This symptom is not observed with Ping.

  Workaround: There is no workaround.

- CSCti62913

  Symptoms: IP SLA repeatedly sends traps.

  Conditions: This symptom is observed in Cisco IOS Release 15.1T when IP SLA probes start failing and the router is configured to send traps, as in the following sample configuration:

```
ip sla 1
 icmp-echo 10.22.22.22 source-ip 10.11.11.11
 threshold 2000
 timeout 2000
 frequency 3
ip sla schedule 1 life forever start-time now
ip sla reaction-configuration 1 react timeout threshold-type consecutive 3 action-type
trapOnly
```

  Workaround: There is no workaround.

  Further Problem Description: When reaction condition is reached, a flag should be set and only one probe should be sent. No additional traps should be sent until the flag is set.

- CSCti65716

  Symptoms: The access interface connecting to the client is on global routing domain. If a service logon profile on a VRF is downloaded to the client, the client could potentially stay on a VRF even when a service logoff is performed later. The client traffic has to return to global domain when a service logoff is performed.

  Conditions: This symptom is see when access interface is on global routing domain. Service logon is on a VRF.

  Workaround: There is no workaround.

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used.
  - Use HSRP with sub-interfaces on ES20 module
  - Reload the ES20 module

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. Reconfigure HSRP on all subinterfaces
  2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

  Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67102

  Symptoms: Tunnel disables due to recursive routing loop in RIB.

  Conditions: The symptom is observed when a dynamic tunnel which by default is passive in nature is created. EIGRP will get callback due to address change (dynamic tunnel come-up). EIGRP tries to run on this interface and install EIGRP route in the RIB which will replace tunnel next-hop result in tunnel disable and routing chain loop result in RIB.

  Workaround: There is no workaround.

- CSCti67429

  Symptoms: A REP segment configured on 7600-ES+20G3CXL interfaces on a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S is not recovering as expected upon link failure recovery of the edge port configured on the 7600. A traffic storm triggered by ISIS protocol configured between 7600 and the MWR 2941s in the REP ring is occurring when the failed REP edge port becomes operational again.

  Conditions: The symptom is observed with a REP ring including two Cisco 7600 series routers equipped 7600-ES+20G3CXL and running Cisco IOS Release 15.0(1) S configured with ISIS and MPLS LDP. The problem is also present in Cisco IOS Release 12.2(33)SRE1.

  Workaround: Configure static routes between the 7600 routers and the MWR 2941s instead of ISIS.

- CSCti67447

  Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

  Conditions: The symptom is observed under the following conditions:

  1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2.
  2. Enable MPLS LDP GR.

  Workaround: There is no workaround.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: Dampening configuration changes for VRFs.

  Workaround: There is no workaround.

- CSCti69990

  Symptoms: A router crashes after deconfiguring IPv6 and then reconfiguring.

  Conditions: The symptom is observed only under specific conditions. Router has IPv6 configured on a number of interfaces and also has GLBP configured. IPv6 configuration is removed from all interfaces and then re-applied.

  Workaround: There is no workaround.

- CSCti72498

  Symptom: A crash occurs on a device acting as DHCP Server.

  Conditions: This symptom is observed when a requested IP address option is present in DHCP requests.

  Workaround: Disable the DHCP ping check with the help of CLI “ip dhcp ping packets 0.”

- CSCti74736

  Symptoms: A traffic drop might appear on a GREoMPLS tunnel after an SSO switchover in an egress direction. If an ingress interface is located on a SIP400 series line card, the following error message will be continuously printed:

  ```
  %INTR_MGR-3-BURST: HY_FD_PP_EC_EC_ERR_INT[0x1] bad payload CRC exceeds threshold
  ```

Conditions: The presence of "mls mpls tunnel-recir" is required for the GREoMPLS feature to work. After the second SSO switchover since bootup, the command will be inactive and the feature broken. The issue is applicable to Cisco IOS Release 12.2(33)SRE2, but not to Release 12.2(33)SRE1.

Workaround: Reload the router.

- CSCti74962

  Symptoms: "%PM-SP-4-PORT_BOUNCED: bounced by Consistency Check IDBS UP" message seen on A3-1 new active router after line card OIR followed by an SSO switchover.

  Conditions: This symptom will occur only with a line card OIR followed by an SSO switchover.

  Workaround: There is no workaround.

- CSCti76466

  Symptoms: A static PW over P2MP functionality outage occurs.

  Conditions: This symptom is observed with static PW over P2MP Tunnel configurations.

  Workaround: There is no workaround.

- CSCti77521

  Symptoms: Policy-map is not attached to a DLFIoATM interface after a SPA OIR.

  Conditions: The symptom is observed upon performing a SPA OIR. The issue is seen with ATM SPA on a SIP400.

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

- CSCti80876

  Symptoms: Malloc subroutine fails on a setup with 600 s,gs with a CFC card.

  Conditions: This symptom occurs when churning the l2 Switched Virtual Interface (SVI) OIFs on SP.

  Workaround: There is no workaround.

- CSCti80904

  Symptoms: A router reloads at sec_send_command while booting up.

  Conditions: The symptom is observed on a Cisco 887 and a Cisco 888 router.

  Workaround: There is no workaround.

- CSCti81177

  Symptoms: Features like Videomon do not work on routed port.

  Conditions: This symptom occurs when an interface is configured as a switchport and reconfigured to routed Port.

  Workaround: Reload the line card.

- CSCti81444

  Symptoms: Traffic does not flow in egress direction over VPLS PW on router reload.

  Conditions: The symptom is observed after a router reload. POE bits for the imposition interface are not getting programmed on the egress line card.

  Workaround: There is no workaround.

- CSCti82141

  Symptoms: The following symptoms are observed:

  1. The “none” option will be missing in the **show run** output after “ntp pps-discipline none inverted stratum *#value*” is configured.
  2. “Invalid input detected” error message will be thrown during the bootup and the configured “ntp pps-discipline none inverted stratum *#value*” will vanish after a reload.

  Conditions: The symptom is observed when the “inverted” option is included in the “ntp pps-discipline” CLI.

  Workaround: Configure the CLI without the “inverted” option.

- CSCti82670

  Symptoms: An RSP will crash when the CFM automated test script (consisting of 53 tests) is run twice in succession.

  With SUP720, the crash is seen with a single run.

  Conditions: The automated test script must be run on 3 connected routers.

  Workaround: Adding a **no shut** on UUT interface with UP- MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run.

  Further Problem Description: Other problems observed are:

  - The CFM MIB will return infinite results for getmany.
  - A **show** command will crash the router.

- CSCti83705

  Symptoms: IPv4 unicast traffic not forwarded out of a Cisco 7600 series router’s GREoMPLS in VRF tunnel.

  Conditions: The symptom is observed with an IPv6 Address Family (AF) configured under VRF. If the IPv6 AF is in the startup configuration then the feature is broken straight after boot up. If the IPv6 AF is configured after boot up, then feature gets broken after this configuration.

  Workaround: Remove IPv6 AF from the tunnel’s VRF.

- CSCti83737

  Symptom: A module will crash with a software-forced crash. The following will be seen in the crash logs.

  ```
  Aug 29 06:11:05 UTC: DFC7: sip10g_tefrr_program_vc_list() TMEM_ASSERT failed on line
  5692 %Software-forced reload
  06:11:05 UTC Sun Aug 29 2010: Breakpoint exception, CPU signal 23, PC = 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a SIP-600 and 7600-ES20-10G3C.

  Workaround: There is no workaround.

- CSCti84762

  Symptoms: Update generation is stuck with some peers held in refresh started state (SE).

  Conditions: This is seen with peer flaps or route churn and with an interface flap.

  Workaround: Do a hard reset of the stuck peers.

- CSCti85402

  Symptoms: Cisco 10000 VRF transfer will fail for IP DHCP sessions.

  Conditions: This symptom occurs after RP switchover.

Workaround: There is no workaround.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword.
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface).
  3. Change the configuration in such a way that nexthop is reachable.
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the **no service dhcp** command is configured.

  Workaround: There is no workaround.

- CSCti87912

  Symptoms: While bringing up PPP sessions, server fails to add a route to the client after the IPCP negotiation happens.

  Conditions: This symptom occurs with the following two conditions:

  1. “ip unnumbered...” per user configuration that is received from radius is applied on the virtual-access interface.
  2. Virtual-template that used for Virtual-access creation is configured with “ip unnumbered <>”.

  Workaround: There is no workaround.

- CSCti88062

  Symptoms: Traffic stops flowing through ports configured with REP over EVC BD when an ES20 line card is replaced by an ES+ in the same slot.

  Conditions: The symptom is observed on a router running MST, having an ES20 card configured with EVC BD which is replaced by an ES+ in the same slot with an EVC BD configuration. MST puts the BD VLAN in a disabled state and the traffic on that VLAN stops flowing.

  Workaround: Reload the router.

- CSCti92798

  Symptoms: A Cisco router crashes while configuring http commands with atm.

  Conditions: This symptom is observed on a Cisco7200 router running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti94938

  Symptoms: With more than 1 L2TP sessions on virtual template interface, when applying non-existent route-map and modifying non-existent route map, router crashes.

  Conditions: This symptom occurs with PPPoE sessions with modifying policy configuration with non-existent route-map.

  Workaround: Configure route-map first before applying policy.

- CSCti95511

  Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.

  Conditions:

  1. Issue is seen only when configuring header/fast switching buffers.
  2. Buffers need to be created for this pool.

  Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

  1. Not configuring "buffer header permanent" with a high value when available memory is low.
  2. Not configuring "no buffer header permanent" when the number of buffers in the free list is less than the minimum value.

- CSCti97759

  Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

  Conditions: This is seen when DHCP static entry is configured.

  Workaround: There is no workaround.

- CSCti97810

  Symptoms: A "%SYS-2-FREEBAD" memory traceback is seen on an HA router.

  Conditions: The symptom is observed on an HA router approximately 3-4 minutes after loading the image on an HA router.

  Workaround: There is no workaround.

- CSCti98931

  Symptoms: Some sessions may be lost after Layer 2 Tunneling Protocol (L2TP) switchover.

  Conditions: This symptom occurs after L2TP switchover.

  Workaround: There is no workaround.

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj00728

  Symptoms: A router crashes when enabling a DECnet neighbor.

  Conditions: The symptom is observed with a DECnet neighbor limit on a single node of 32. If one exceeds 32, the crash is seen.

  Workaround: Limit neighbor count to 32.

- CSCtj01623

  Symptoms: REP topology stays incomplete after manual pre-emption. When the issue occurs, REP pre-emption will not take effect.

  Conditions: The symptom can be observed for EVC or switchport.

  Workaround: There is no workaround.

- CSCtj04278

  Symptoms: In a DMVPN setup that is running the code of Cisco IOS Release 15.1TPI15, it is possible that NHRP Registrations are not sent by the box. This is seen if crypto is not configured using tunnel protection.

  Conditions: This symptom occurs when tunnel protection is not configured.

  Workaround: perform a shut/no shut of the tunnel interface.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj05591

  Symptoms: Memory corruption and SP crash seen.

  Conditions: The symptom is observed when creating 600 subinterfaces as OIF for Mroute entries.

  Workaround: There is no workaround.

- CSCtj05903

  Symptoms: Some virtual access interfaces are not created for VT, on reload.

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

  Workaround: There is no workaround.

- CSCtj07904

  Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

  Conditions: The symptom is observed when “no passive interface” is configured.

  Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface *interface*” for the interface to be passive.

- CSCtj08368

  Symptoms: Router software crash at process_run_degraded_or_crash.

  Conditions: The symptom is observed when the allocated memory block is freed.

  Workaround: There is no workaround.

- CSCtj08448

  Symptoms: No Shared Port Adaptors (SPA) come up after switch over.

  Conditions: This symptom occurs with RPR mode, if a switchover with traffic is performed.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

Conditions: The symptom is observed when there are redundant paths to the CPE.

Workaround: Use only one path between PE and CPE.

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory- corruption with block overrun.

  Conditions: This symptom is seen when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCtg85402

  Symptoms: Multicast packet software switching MFIB platform flags "NP RETRY RECOVERY HW_ERR HAL" after SSO/ISSU.

  Conditions: Issue seen only with CFC cards and not with DFC. Specific to mVPN configuration with egress CFC cards. Issue seen under rare condition with SSO/ISSU.

  Workaround: Remove and add Default MDT configuration.

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2010-3050 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj11497

  Symptoms: Shared Port Adaptor (SPA) crashes after receiving "%INTR_MGR-3- INTR: PL3 RX Sequence error".

  Conditions: This symptom occurs under normal working conditions.

  Workaround: The SPA reloads automatically and clears the problem.

- CSCtj13146

  Symptoms: Stand by redundancy mode mismatch occurs.

  Conditions: This symptom occurs when a switch from RPR mode to SSO mode happens.

Workaround: There is no workaround.

- CSCtj13191

  Symptoms: V4 multicast groups do not flow across the first hop router. Debugging shows that mfib is dropping the source traffic due to acceptance check failure.

  Conditions: V4 multicast routing is enabled and pim sparse mode traffic is flowing across the first hop router with a traffic source directly connected to it.

  Mfib debugs show this message "(TS) Acceptance check failed - dropping" on the first hop router:

  sh ip mfib "multicast group" shows no C flag for the *,g entry

  Workaround: Disable/enable multicast routing on the router to get the traffic flow to resume.

- CSCtj15805

  Symptoms: Keepalive functionality not working. An ICMP echo reply coming back from a client is ignored by ISG.

  Conditions: The symptom is observed when a VRF mapping service is used.

  Workaround: There is no workaround.

- CSCtj17316

  Symptoms: EIGRP flaps up and down in a large scale network, when there is a lot of data to be sent.

  Conditions: In an EIGRP network that has a large number of peers on a single interface, EIGRP might stop sending data to peers. This causes a flap due to packets not being acknowledged.

  Workaround 1: Find the instability in the network and fix the interface.

  Workaround 2: Summarize more routes.

  Workaround 3: Change more routers to stub.

  Workaround 4: Upgrade to rel7 of EIGRP.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  template peer-session ce-v4 transport connection-mode passive

- CSCtj17561

  Symptoms: Description for T1 broken in Prowler/Chopper SDH > C-11 mode. This might lead to sync issues while switching over.

  Conditions: The symptom is observed in SDH > C-11 mode.

  Workaround: There is no workaround.

- CSCtj17667

  Symptoms: The **debug radius** debug command may cause memory corruption and crash in rp2 and 1ru images.

  Conditions: This symptom is seen with the **debug radius** command in rp2 and 1ru images.</B>

  Workaround: Do not use the **debug radius** command.

- CSCtj18753

  Symptoms: Memory leak is seen with MLDP scale test.

  Conditions: The issue is seen only when there is a switchover from default- data-default MDT trees.

  Workaround: Avoid default-data-default MDT tree switchovers.

- CSCtj20163

  Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

  Conditions: The symptom is observed with the following conditions:

  1. Execute **show mpls mldp database**.
  2. Reload Encap PE.
  3. Crash is seen on P router when MLDP neighbors go down.

  Workaround: There is no workaround.

- CSCtj20362

  Symptoms: Router does not allow configuring more than one secondary IP address in the same subnet, on an interface in the same VRF.

  Conditions: This symptom occurs when configuring a secondary address on an interface, which has already one secondary IP address in the same subnet. This applies to VNET capable interfaces.

  Workaround: There is no workaround.

- CSCtj20776

  Symptom: Accounting-stop record is sent for radius proxy session when re- authentication happens for that session.

  Accounting-stop record is sent for radius proxy session when re- authentication happens for that session.

  Conditions: This issue is seen in the following scenarios:

  1. Authentication request comes from AP.
  2. Accounting request comes from AZR and session on ISG is associated to AZR.
  3. ISG receives a re-authentication request from AP.

  The Accounting-stop record is sent for Radius-Proxy session and the services under the session, but the radius-proxy session is still active and no stop record is sent for the session on clearing the session. Also acct- terminate- cause in the stop record is set to none.

  Workaround: There is no workaround.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

```
Router1#sho inv
NAME: "chassis", DESCR: "2801 chassis"
PID: CISCO2801 , VID: V04 , SN: FTX1149Y0KF
NAME: "motherboard", DESCR: "C2801 Motherboard with 2 Fast Ethernet"
PID:CISCO2801 , VID: V04 , SN: FOC11456KMY
NAME: "VIC 0", DESCR: "2nd generation two port EM voice interface daughtercard"
PID:VIC2-2E/M= , VID: V , SN: FOC081724XB
NAME: "WIC/VIC/HWIC 1", DESCR: "4 Port FE Switch"
```

```
PID: HWIC-4ESW , VID: V01 , SN: FOC11223LMB
NAME: "WIC/VIC/HWIC 3", DESCR: "WAN Interface Card - DSU 56K 4 wire"
PID:WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
NAME: "PVDM 1", DESCR: "PVDMII DSP SIMM with one DSP with half channel capcity"
PID:PVDM2-8 , VID: NA , SN: FOC09123CTB
```

Workaround: Do a shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= "BGP Scanner", ipl= 0, pid= 549
  with call stack
  0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000
  BGP table version is 1228001, main routing table version 1228001 604000
  network entries using 106304000 bytes of memory
  604000 path entries using 31408000 bytes of memory
  762/382 BGP path/bestpath attribute entries using 94488 bytes of memory
  381 BGP AS-PATH entries using 9144 bytes of memory
  382 BGP community entries using 9168 bytes of memory
  142685 BGP route-map cache entries using 4565920 bytes of memory
  ```

  The **clear ip bgp *** command is not a very common operation in production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj25243

  Symptoms: If non-LLQ or parent (logical) is rate-limited and oversubscribed, this can cause some policer drops in the LLQ queue, if LLQ exceeds the bandwidth allocated to it.

  Conditions: The symptom is observed if non-LLQ or parent (logical) is rate- limited and oversubscribed and if LLQ exceeds the bandwidth allocated to it.

  Workaround: There is no workaround.

  Further Problem Description: This issue is caused by CSCth85449. That caveat was intended to detect congestion on the physical interface and police LLQ traffic if it exceeds the configured bandwidth and the physical link is congested.

- CSCtj28696

  Symptoms: Session QoS will not get applied after an OIR of the line card.

  Conditions: The symptom is observed with sessions (with QoS) on a port- channel subinterface.

  Workaround: Clear session and bring up again.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

Workaround: There is no workaround.

- CSCtj29382

  Symptoms: When cellular interface passes packets and users configure "tx-ring-limit" on cellular interface, system will crash.

  Conditions: This symptom occurs under the following conditions:

  1. Traffic runs through cellular interface.
  2. Change "tx-ring-limit" on cellular interface with traffic running in the background.

  Workaround: Stop the traffic and change "tx-ring-limit".

- CSCtj30155

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtj31743

  Symptoms: Memory leaks are observed at at slaAddSeqNum.

  Conditions: This symptom occurs when "pfs border" is configured.

  Workaround: There is no workaround.

- CSCtj32769

  Symptoms: Data path fails with Layer-2 Virtual Private Network (L2VPN)on ACR interface when asynchronous mode is enabled.

  Conditions: This issue occurs when a VPN is configured on ACR interface in asynchronous mode with cellpacking configurations. This issue does not occur in normal synchronous mode or Layer-2 Virtual Circuits (L2VCs).

  Workaround: Configure the same Maximum Number of Cells Packed (MNCP) value for local and remote provide edge (PE) devices.

- CSCtj35573

  Symptoms: When an interface is configured as an access interface, back-to-back ping will fail.

  Conditions: The ping failure is seen only for access interfaces intermittently. This issue is observed with the SRE2 image with SUP720 and ES+ card, in a situation when the ping packet coming from source has the BPDU bit set.

  Workaround: There is no workaround.

- CSCtj36294

  Symptoms: Traffic fails when PW switchover occurs.

Conditions: This symptom occurs when a primary PW and backup PW are configured. Shut primary PW and allow the traffic to go through backup PW. The traffic is dropped by the router.

Workaround: There is no workaround.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

  Workaround: There is no workaround.

- CSCtj38346

  Symptoms: Router crash is seen when configuring the **default transmit- interface** command.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

  Workaround: There is no workaround.

- CSCtj38519

  Symptoms: EIGRP pacing timer is large when there is a large number of peers on NBMA interfaces.

  Conditions: The symptom is observed when EIGRP is configured with a large number of peers on a single NBMA interface.

  Workaround: Ensure spokes are setup as stub and properly summarized.

- CSCtj38606

  Symptoms: The following error message is seen:

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

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

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

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

  Workaround: There is no workaround.

- CSCtj39558

  Symptoms: Sub-interface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj41215

  Symptoms: On an ES+, a service instance configuration is rejected with following error:

  Service instance configuration Failed. Service-Policy has already been configured on this interface

  Conditions: The symptom is observed when an ES+ is inserted in the same slot where an ES20 was previously present.

  Workaround: Unconfigure service-policy from the interface and then create a service instance.

- CSCtj41867

  Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

  Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured ("qos pre-classify"), and WAAS Express enabled on a several interfaces with MLPPP enabled.

  Workaround 1: Disable QoS classification on VPN tunnel interface.

  Workaround 2: Disable WAAS Express on VPN tunnel interface.

  Workaround 3: Reduce the number of serial interfaces down to one

  Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj42230

  Symptoms: IOSD crashes on unconfiguring the service policy.

  Conditions: The crash is seen when trying to unconfigure service policy without detaching it from the ATM PVP subinterface.

  Workaround: There is no workaround.

- CSCtj43778

  Symptoms: Multiple met cc processes running on DFC.

  Conditions: This symptom occurs when toggling the met cc processes using mentioned commands.

  Workaround: Perform the toggling with sufficient time (1 minute) between the no form of the command and the command itself.

- CSCtj44237

  Symptom: High CPU observed in RP.

  Conditions: The symptom is observed with MVPN configurations.

  Workaround: There is no workaround.

- CSCtj45571

  Symptoms: If OAM VC state reaches to "AIS/RDI" after PVC is flapping, then OAM Loopback status gets stuck in "OAM failed" state. Loopback cell is not generated until shut/no shut is performed on the subinterface.

  Conditions: The symptom is observed when the OAM VC state reaches "AIS/RDI".

  Workaround: Perform a shut/no shut on the subinterface.

- CSCtj46297

  Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

Conditions: The symptom is observed in an FRR setup when performing a shut/no shut on the outgoing interface.

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

- CSCtj47736

  Symptoms: Router crash is seen when doing a **show eigrp service ipv4 neighbor**.

  Conditions: The symptom is observed when the neighbor is learned, then you add a max-service limit on an address family. Then do a shut/no shut on the interface.

  Workaround: There is no workaround.

- CSCtj48220

  Symptoms: A Cisco router may unexpectedly reload due to bus error.

  Conditions: This symptom occurs with AAA.

  Workaround: There is no workaround.

- CSCtj48629

  Symptoms: Though "ppp multilink load-threshold 3 either" is set, the member links are not added by the inbound heavy traffic on the PRI of the HWIC- 1CE1T1-PRI.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtj48913

  Symptoms: Track does not recognize when an HTTP IP SLA probe's status changes to OK.

  Conditions: The symptom is observed with an HTTP IP SLA probe and with a tracker.

  Workaround: There is no workaround.

- CSCtj49133

  Symptoms: After attaching a policy-map to a sub-interface, the policy-map is then renamed and then the sub-interface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.

  Conditions: The symptoms are observed with the following steps:

  1. Attach a policy to a sub-interface.
  2. Rename the policy-map.
  3. Remove the sub-interface.
  4. Removing the definition of policy-map will not succeed.

  Workaround: Remove the service policy from sub-interface before removing the sub-interface.

- CSCtj50072

  Symptoms: High CPU interrupt level caused by IPv4 unicast or multicast traffic received via GREoIP or GREoMPLS tunnel if rate is high. If ingress interface is tunnel and egress is tunnel (MDT included) as well, then outer IP ToS of egress packet will be reset to 0x0.

  Conditions: The symptom is observed after a reload (under 10% probability), GRE tunnel must be in VRF:

```
#show running-config interface tunnel 513
interface Tunnel513
 vrf forwarding REN
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-mode
 tunnel source Loopback513
 tunnel destination 10.0.113.2 (via IP or MPLS interface)
 tunnel vrf REN
end
```

To confirm hit:

```
#show vlan internal usage | include Tunnel513
4074 Tunnel513

#remote command switch show mls vlan-ram 4074 4074
(If there is 256, the defect is present)
```

Workaround: Reload the router.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

  Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

  Workaround: Only reloading the router resolves the issue.

- CSCtj55920

  Symptoms: Flapping BGP session observed. Debug IP TCP transactions found to be advertising incorrect MSS.

  Conditions: This symptom occurs when MP-BGP is running between non-directly connected peers.

  This is a day 1 bug in IOS code since BGP PMTUD feature. The issue happens in a scenario where BGP PMTUD is disabled globally on a fresh config and then peers are configured or upon reload because of the order of parsing (by default PMTUD is enabled and not nvgenn'ed). The impact is a possible session flap if an intermediate link MTU is much smaller than the negotiated PMTU. There is a way to get out of this after the issue happens and if aware an easy enough way to not get into this.

  Workaround 1: Unconfigure the global PMTUD configuration and reconfigure

  Workaround 2: Unconfigure PMTUD on per neighbor using "neighbor x.x.x.x transport path-mtu-discovery disable".

- CSCtj56142

  Symptoms: ISG uses dummy user-name within EAP re-authentication related access-requests as the session identifier.

  Conditions: The symptom is observed during EAP re-authentications and likely after CoA-based service activation on an EAP-authenticated session. This happens only when the EAP access-requests carry a dummy user-name and access- accept does not have the correct username.

  Workaround: There is no workaround.

- CSCtj58405

  Symptoms: Full multicast traffic is not sent from the source PE.

Conditions: The issue is observed only with ECMP links and with a higher scale (above 75 MVRF and 100 mroutes per VRF) for default MDTS. It is seen when one of the ECMP links which was down earlier, comes up. If all the ECMP links are already up, then the issue is not seen.

Workaround: Clear the IP mroute using **clear ip mroute** command.

- CSCtj59254

  Symptoms: Data to default MDT switchover fails in highly scaled scenarios.

  Conditions: The symptom is observed during a default to data MDT switchover.

  Workaround: There is no workaround.

- CSCtj61252

  Symptoms: Router crash when bringing up PPP sessions.

  Conditions: The symptom is observed when adding QoS classes using parametrized QoS attributes where a class name to be added happens to be sub- string of an already existing class.

  Workaround: Do no add or configure class names which are sub-strings of other classes on the router.

- CSCtj61748

  Symptom: Service activation fails occasionally.

  Conditions: This symptom occurs with multiple services in the session authentication or authorization response that are configured in the same service-group.

  Workaround: Remove fields that are related to “service-group” or “service- type” in service definitions.

- CSCtj62999

  Symptoms: PPP sessions do not come up.

  Conditions: This symptom occurs when PBR is configured under Virtual-template interface.

  Workaround: There is no workaround.

- CSCtj64899

  Symptoms: In the Cisco IOS 7600 series router, ISG CoPP does not get installed in SIP-400 LC, when burst is specified.

  Conditions: This symptom occurs for ISG CoPP with burst is configured.

  Workaround: There is no workaround.

- CSCtj65553

  Symptoms: Static route that is installed in default table is missing.

  Conditions: Static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj66392

  Symptoms: Tunnel interface does not go up on standby router and IKE and IPSec SAs are not synchronized to the standby router. Even if tunnel protection is configured, crypto socket is not opened.

  Conditions: This symptom is observed when IPSec stateful failover for tunnel protection is configured.

  Workaround: Use Cisco IOS Release 12.4(11)T4.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj70271

  Symptoms: Non-local replications are programmed as local replications in the MET3 (i.e.: if the replications are on slot 3 DFC module, then the supervisor is programmed with the sublsps of slot 3 as local replications). This causes a waste of TCAM resources and can cause traffic outage.

  Conditions: The symptom is observed with LSM/MLDP configurations.

  Workaround: Use this command: **clear ip mroute** *source group*.

- CSCtj72148

  Symptoms: A Cisco 7600 router might face an SP crash upon first reload after upgrade from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2. After successive reloads, the system functionality is restored.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2.

  Workaround: There is no workaround.

- CSCtj72730

  Symptoms: If an Enhanced Interior Gateway Routing Protocol (EIGRP) **address-family** configuration command is removed, any redistribution commands that refer to that address-family should also be removed. This defect documents a case where the redistribution command is not removed.

  Conditions: This issue occurs when the redistribution command is not removed after removing the corresponding EIGRP address-family configuration command.

  Workaround: Manually remove the redistribution commands that remain after the **address-family** command is removed.

- CSCtj74611

  Symptoms: Active supervisor in the Cisco 7600 series router reloads.

  Conditions: The symptom is observed after a line card is powered off due to keepalive failures. Possible sequence of syslog messages:

```
%OIR-SP-3-PWRCYCLE: Card in module 7, is being power-cycled off (Module not
responding to Keep Alive polling)
<...>
%C7600_PWR-SP-4-DISABLED: power to module in slot 7 set off (Failed to
configure the line card)
<...>
%EM-SP-4-AGED: The specified EM client (EM_TYPE_FABMAN_NORMAL type=29,
id=8887)
 did not close the EM event within the permitted amount of time (900000 msec).
SP: em_fabman_act_event_end_cb: (timer) SWM event 8887  (slot 7 -> HELIOS /
CARD_RUNNING) was not closed properly
```

  Workaround: There is no workaround.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

Workaround: Disable AIM and use onboard CE.

- CSCtj76788

  Symptoms: Standby RP does not come up because of <set ip nexthop recursive vrf <> X.X.X.X> sync failure.

  Conditions: This symptom occurs when the route map has a set clause referring to a VRF and the VRF is deleted without first deleting the route map set clause.

  Workaround: Configure the <set ip nexthop recursive X.X.X.X> and then do <no set ip nexthop recursive X.X.X.X> to effectively removes the set clause.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj77188

  Symptoms: When performing an ISSU downgrade from RLS8 to RLS7 and then aborting it, the backup pseudowires are no longer setup.

  Conditions: This symptom occurs when the ISSU procedure is either cancelled or is left incomplete.

  Workaround: To clear this errored state use the **clear xconnect all** command.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtj79750

  Symptoms: Multicast responses are not obtained.

  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not obtained.

  Workaround: There is no workaround.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: Issue is seen in unconfiguration part.

  Workaround: There is no workaround.

- CSCtj79992

  Symptoms: Receiver end flooded in an MVPN scenario.

  Conditions: The symptom is observed even after stopping traffic.

  Workaround: There is no workaround.

- CSCtj81938

  Symptoms: The L3VPN profile configuration "transport ipv4 source *interface*" is not synced to standby, if the source interface is same as the auto-source that is picked by BGP.

  Conditions: This symptom occurs when the source interface is same as the auto- source that is picked by BGP.

  Workaround: There is no workaround.

- CSCtj82292

  Symptoms: EIGRP summary address with AD 255 should not be sent to the peer.

  Conditions: This issue occurs when summary address is advertised as follows:

  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255

  Workaround: There is no workaround.

- CSCtj85333

  Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS config feature commands **cns config retrieve** exec command, **cns config initial** config command. This symptom may also occur when the config template is downloaded to the router using the device Config-Update operation of Config Engine.

  Conditions: This is normal mode operation, but this symptom will occur when such CNS feature is used.

  Workaround: There is no workaround.

- CSCtj85858

  Symptoms: Coexistance of flat class-default shape policy-map (port level shape) and QOS on sub-targets (sub-interface, service instance, sessions and so on) is not supported on LowQ ES+.

  Conditions: This symptom occurs only on LowQ ES+.

  Workaround: There is no workaround.

- CSCtj86464

  Symptoms: Bundling does not occur with Distributed Link Fragmentation and Interleaving (dLFI) over ATM.

  Conditions: Bundle keeps flapping with dLFI over ATM.

  Workaround: There is no workaround.

- CSCtj86514

  Symptoms: An SNMP walk on Cisco AAL5 MIB may not return information for all PVCs configured on the device.

  Conditions: An SNMP walk query on the Cisco AAL5 MIB may fail to return information of bundled PVCs that are in down state. Information about PVCs in UP state is returned correctly.

  Workaround: To get information of bundled PVCs in down state, you need to poll with more specific OIDs. Instead of doing an snmpwalk on "1.3.6.1.4.1.9.9.66.1.1.1.1.3", do an snmpget on "1.3.6.1.4.1.9.9.66.1.1.1.1.3.<IfIndex>.<VPI>.<VCI>".

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of "SSS Manager Disconnected Session".

Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is back up.

  Workaround: Do Shut/no shut on PfR master or PfR border.

- CSCtj88428

  Symptoms: CPP lock down occurs and fman_fp crashes.

  Conditions: This symptom occurs while performing IOSd SSO switchover with local switching configuration.

  Workaround: Reload the router.

- CSCtj88825

  Symptoms: Fabric utilization goes high and drops are seen.

  Conditions: The symptom is observed when egress replication is configured with multicast. Global ICROIF index (0x02006) is programmed which causes high fabric utilization.

  Workaround: There is no workaround.

- CSCtj91149

  Symptoms: A delay of approximately 30 seconds is observed in dynamic xconnect- based ISG session that comes up on standby, after it is up on active.

  Conditions: This symptom occurs on switchover.

  Workaround: There is no workaround.

- CSCtj91764

  Symptoms: A UC560/UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to CPU.

  Conditions: The crash happens during a complete SNMP MIB walk.

  Workaround: The CISCO-CALL-APPLICATION-MIB can be excluded via configuration.

- CSCtj92092

  Symptoms: VPN-ID is sent as the username AAA authorization fails.

  Conditions: This symptom occurs when a DHCP server is configured to use RADIUS server for providing IP to the client.

  Workaround: There is no workaround.

- CSCtj92341

  Symptoms: PIM packets are bridged causing them to not hit the decap adjacency. Hence, PIM neighborship for a few VRFs is not up.

  Conditions: This symptom is seen when all the VRFs in a scaled setup are removed, and added through a script.

  Workaround: Reload the box or reset the line card.

- CSCtj92837

  Symptoms: Router throws the error messages NoSubTkn> while accessing the filenames with special characters like (' ").

  Conditions: This symptom is observed while accessing the filenames with special characters like (' ").

  Workaround:

  1. Disable IOS.sh feature using "no shell processing".
  2. Escape shell specific characters, so that these characters are not interpreted. For example, flash:START17Mar'10.

- CSCtj94188

  Symptoms: After an LC OIR, the Red AIE peer and AIE peer ID become the same. This causes the PWs to go down.

  Conditions: LC OIR causes the Red AIE peer ID and AIE peer id to become the same.

  Workaround: Use the **clear xconnect all** to reprovision the PWs.

- CSCtj94297

  Symptoms: "F" flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

  Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

  Workaround: Use the **clear ip mroute** in the affected mroute.

- CSCtj94358

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

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

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

- CSCtj94490

  Symptoms: Route Processor (RP) reloads after 30 RP switchovers.

  Conditions: This symptom occurs after 30 RP switchovers during 28000 PPPoEoA sessions while traffic is flowing.

  Workaround: There is no workaround.

- CSCtj94835

  Symptoms: Spurious memory access and tracebacks are seen on router reload.

  Conditions: The symptom is observed when the router is reloaded.

  Workaround: There is no workaround.

- CSCtj95032

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

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

  Workaround: There is no workaround.

- CSCtj95782

  Symptoms: MDT tunnel is assigned to the default VRF instead of the configured VRF.

  Conditions: This symptom is observed when there are multiple VTY sessions into a router and **mdt default** *MDT Group Addr* command is executed in the VRF configuration submode of one VTY session just after the VRF is deleted from another VTY session.

  Workaround: Avoid configuring and unconfiguring a particular VRF from different VTY sessions.

- CSCtj96489

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

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

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

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown. See Further Problem Description below.

  Workaround: There is no workaround. Only power cycle can remove the symptom.

  Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj97360

  Symptoms: Punted datapaths are multicast flows GREoIP->DefaultMDT and GREoMPLS->Default MDT.

  Conditions: This symptom occurs with device bootup with IPv4-only VRF. After bootup IPv6 is enabled for VRF, which triggers the problem.

  Workaround: Do not have IPv6 AF and the mcast configurations in the same VRF.

- CSCtj97823

  Symptoms: The 32-byte topology names are not handled correctly on bootup.

  Conditions: This symptom occurs when 32-byte topology names are not handled correctly on bootup.

  Workaround: Use topology names shorter than 32 characters.

- CSCtj99415

  Symptoms: Traffic is not dropped when the packet size is more than the egress interface MTU.

  Conditions: This symptom occurs when the egress interface is on SIP400. When the outgoing interface is on ES20 the packets are dropped at RP with an error message.

  Workaround: There is no workaround.

- CSCtk00398

  Symptoms: When receiving DHCPv6 SOLICIT from two clients with same DUID, DHCPV6 binds the Delegated-Prefix to incorrect client.

  Conditions: This symptom occurs when two clients are sending SOLICIT with same DUID.

  Workaround: There is no workaround.

- CSCtk00976

  Symptoms: File descriptor reaches the maximum threshold limit. You will be unable to save the configuration or do any file system related operation as file descriptors are exhausted. You will get “File table overflow” error.

  Conditions: The symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

  Workaround: Do not run **dir/recursive <>** command if leaks are detected. Also, if it is running through ANA server polling, disable it.

- CSCtk02155

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

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

  Workaround: Reset the line card.

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

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- CSCtk02661

  Symptoms: Bundles stop forwarding any traffic.

  Conditions: The symptom is observed when you move the SPA to a different bay on a SIP-400 and apply configurations on the new bay.

  Workaround: Reload spa on both ends.

  Alternate workaround: Unconfigure multilink before moving the SPA out.

- CSCtk02666

  Symptoms: During a graceful restart event, the peer undergoes reconfiguration. This may result in stale labels on the RRP.

  Conditions: The symptom is observed with GR + SSO + peer reprovisioning.

  Workaround: Perform a **clear xconnect** or flap the local VC.

- CSCtk05652

  Symptoms: UDLD, that uses end-to-end across an AToM link, causes the CE link on one side to be put in err-disabled state.

  See the following topology:

  SW1 (CE) <-- PE-1 <-> MPLS cloud <-> PE-2 (7600 running 12.2(33)SRE2 --> SW2 (CE)

  UDLD err-disabling the port on SW2 is seen though the link is not unidirectional.

  Conditions: This issue is observed on Cisco IOS Release 12.2(33)SRE2.

  Workaround: Run Cisco IOS Release 12.2(33)SRD5.

- CSCtk06750

  Symptoms: IP-directed broadcast packets do not get forwarded by downstream router.

  Broadcast-source----R1---serial----R2-------rcr

  Conditions: When the serial link encapsulation is set to High-Level Data Link Control (HDLC), which is the default encapsulation, the layer2 HDLC frames are sent out with an incorrect address type in HDLC header. The downstream router does not recognize the payload as a broadcast packet and it does not forward it further as a directed broadcast packet.

  Workaround: Change the encapsulation to Point-to-Point Protocol (PPP) on the affected serial interfaces.

- CSCtk07240

  Symptoms: When a member-link is removed from an L2 port-channel (A port- channel with switchport configured under it), the traffic stops flowing.

  Conditions: A member link of L2 port-channel passing traffic is removed from the port-channel.

  Workaround: Remove and add the port-channel configurations again.

- CSCtk07369

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

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

  Workaround: There is no workaround.

- CSCtk07632

  Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

  Conditions: The symptom is observed when the filter vlan specified is not configured on the box.

  Workaround: Configure the vlan on the box, then configure it as SPAN filter vlan.

- CSCtk10279

  Symptoms: A router configured for LISP may crash if it receives a LISP Map- Reply message with an IPv6 RLOC, when IPv6 routing is not enabled.

  Conditions: This symptom occurs when LISP is configured using the **ip lisp {itr | etr | proxy-itr | proxy-etr}** command, the router does not have IPv6 routing configured using the **ipv6 unicast-routing** command.

  Workaround: Enable the IPv6 routing by entering **ipv6 unicast- routing** command.

- CSCtk12243

  Symptoms: Traffic drop may be seen when you enable or disable IGMP snooping through CLI.

  Conditions: This symptom occurs when you enable or disable IGMP Snooping through CLI on a router operating in ingress replication mode only.

  Workaround: Perform a shut/no shut on interfaces after the CLI change.

- CSCtk12252

  Symptoms: Priority 1, valid SONET controller network clock source does not get picked as an active clock source. Instead, the clock remains as FREERUN.

  Conditions: This issue occurs after reloading the router, when there is a valid but not present, priority 2 network clock source.

  Workaround: Perform a shut/no shut on the near-end Prio1 clock source SONET controller.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, 15.1 (2)T and 15.1(01)S and with the following configurations:

  Router 1:

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.1 255.255.255.0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.0.1 remote-as 200
 neighbor 172.16.0.1 ebgp-multihop 255
 no auto-summary
!

ip route 0.0.0.0 0.0.0.0 10.10.200.1
ip route 172.16.0.1 255.255.255.255 10.0.12.2
ip route 172.16.0.1 255.255.255.255 10.0.120.2
```

  Router 2:

```
interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
 ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.12.2 255.255.255.0
!

interface Ethernet1/0
 ip address 10.0.120.2 255.255.255.0
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.10.200.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk12708

  Symptoms: Router crashes when holdover clock source is deleted.

  Conditions: This symptom occurs when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: The symptom is observed when a subinterface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge domain. The traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, perform a shut/no shut on the interface.

- CSCtk14941

  Symptoms: Memory leak seen at fh_applet_config_entry_proc.

  Conditions: This symptom occurs when the description keyword is used in an EEM applet.

  Workaround: There is no workaround.

- CSCtk15360

  Symptoms: xauth userid mode http-intercept does not prompt for a password and the Ezvpn session does not come up.

  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.

  Workaround: There is no workaround.

- CSCtk15997

  Symptoms: With interworking VLAN configured for a VFI, the VC is up, but packets do not flow.

  Conditions: This symptom occurs when internetworking VLAN is configured for a VFI.

  Work Around: If possible, do not configure interworking VLAN.

- CSCtk16310

  Symptoms: Timeout failure occurs due to”No socket” error.

  Conditions: This symptom occurs with Udp-jitter packet with VRF.

  Workaround: There is no workaround.

- CSCtk18607

  Symptoms: Router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Workaround: There is no workaround.

- CSCtk18774

  Symptoms: Met cc process does not run.

  Conditions: This symptom occurs with SSO.

  Workaround: Reload the router.

- CSCtk19108

  Symptoms: MVPN traffic failing.

  Conditions: The symptom is observed after an SSO switchover.

Workaround: There is no workaround.

- CSCtk30807

  Symptoms: A box that acts as a DHCP relay/server crashes when the DHCP service is toggled (no service dhcp/service dhcp).

  Conditions: This issue occurs when the box is also configured as ISG.

  Workaround: There is no workaround.

- CSCtk31340

  Symptoms: Cisco route processor (RP) crashes when a port-channel is removed and the member link is defaulted.

  Conditions: When a port-channel is removed (no int port-channel 200) and the member link is defaulted, the port-channel does not automatically remove the configurations on the member link. This crashes the route processor.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk31515

  Symptoms: Router or line cards crash upon removing VLAN interfaces that are in the OIF list.

  Conditions: The symptom is observed with a series of VLAN interfaces in the access and with the hosts joining groups. Configured is “ssm-mapping”. Access facing line cards can be DFC or CFC.

  Workaround: There is no workaround.

- CSCtk32104

  Symptoms: PPPoE data traffic gets process switched.

  Conditions: This symptom occurs on PPPoE data traffic.

  Workaround: There is no workaround.

- CSCtk32975

  Symptoms: The system crashes.

  Conditions: This symptom occurs when traffic is flowing through the device and fair-queue is configured on ATM PVC.

  Workaround: There is no workaround.

- CSCtk33682

  Symptoms: Storm control stops working.

  Conditions: The symptom is observed after a shut/no shut of the interface on an ES-20.

  Workaround: Remove/add the storm control command on the interface.

- CSCtk33784

  Symptoms: After ISSU from SRE1 to SRE3 seeing CONST_MFIB_LC-SP-6-MET_MCAST_ALLOC_FAILURE for particular group is continuously observed.

  Conditions: This symptom occurs when 10 groups and 32 OIFs are configured.

  Workaround: There is no workaround.

- CSCtk33821

  Symptoms: When polling VidMon metrics through SNMP during MSE intervals, no metric values are returned.

  Conditions: This symptom is observed when the MSE interval is being polled.

  Workaround: There is no workaround.

  Further Problem Description: When we get a MSE interval, the Cisco 7600 does not export the interval data to SNMP. During the MSE interval MRV will be - 100, CMM uses this value to determine the Media stop event. So it is critical to export the MSE interval to SNMP.

- CSCtk34026

  Symptoms: Adding, deleting and re-adding an access subinterface may sometimes cause loss of data path.

  Conditions: The symptom is observed when the configuration sequence involves an add-delete-add sequence.

  Workaround: Create access subinterfaces from scratch.

- CSCtk35650

  Symptoms: Router hangs while generating IP SLA auto schedule with maximum length.

  Conditions: This symptom occurs while generating IP SLA auto schedule.

  Workaround: There is no workaround.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk36029

  Symptoms: The **match protocol** *icmp* command is not available under class map configuration.

  Conditions: This symptom is seen on the Cisco 7600 with ISG CoPP.

  Workaround: There is no workaround.

- CSCtk36059

  Symptoms: Active SRE does a silent reload while undergoing an ISSU from Cisco IOS Release 12.2(33)SRD to 12.2(33)SRE.

  Conditions: The symptom is observed with scaled configurations.

  Workaround: There is no workaround.

- CSCtk36064

  Symptoms: QoS policy-map with set CoS is applied on switchport interface of ES+ LC in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Conditions: This symptom is seen on a Cisco 7600 router. ES+ LC, QoS policy- map with set CoS is applied on switchport interface in ingress. CoS value is not copied to EXP while adding label in L3VPN/VPLS scenarios.

  Workaround: There is no workaround.

- CSCtk36090

  Symptoms: Router crashes at draco2_inband_dma_pak after a router reload with the following Cisco IOS Release 12.(33)SRE image:

  s72033-adventerprisek9_dbg-mz.nightly_sre_2010-11-20

  Conditions: The symptom is observed following a router reload.

  Workaround: There is no workaround.

- CSCtk36377

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

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

  Workaround: Delete VRF and add it back.

- CSCtk36582

  Symptoms: Accounting on/off messages from AZR clears session from all the sessions in the client pool.

  Conditions: This symptom occurs in the following scenarios:

  1. When there are two AZRs 192.168.100.1 and 192.168.100.2, configure the client in the ISG under radius proxy as “client 192.168.0.0 255.255.0.0”
  2. Account on or off from any of the clients is clearing sessions from both the clients.

  Workaround: Configure clients individually instead of pool configuration.

- CSCtk37068

  Symptoms: Policing is not happening.

  Conditions: This symptom occurs when CoPP is enabled.

  Workaround: There is no workaround.

- CSCtk39301

  Symptoms: Tracebacks such as the following can appear on the RP:

  ```
  %C6K_MPLS_RP-STDBY-3-INFINITE_OCE: In label: 17 Invalid OCE previous oce type: 29 prev
  ptr: 0x5648A2B0, next oce type: 29 next oce ptr: 0x0
  -Traceback= 42319368z 42322E68z 42BA0EF0z 438DCE10z 438D17F0z 405A209Cz 405AC198z
  405A7900z 405EA768z 405EA9E0z 438D06B4z 438D0EE4z 438DAF98z 438FFE40z 422200D0z
  4222123Cz
  ```

  Conditions: The symptom is observed if there are more than eight or 10 ECMP paths for any prefix (i.e.: when there is a loadbalance object in the forwarding OCE chain).

  Workaround: Reduce the number of paths and do a **clear ip route** to re-initiate hardware programming.

- CSCtk47891

  Symptoms: Traffic might be blackholed when LC is reset, if Fast Reroute (FRR) is in use.

  Conditions: This symptom occurs when FRR is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk47960

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

Remote side will generate the following:

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

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

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

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

- CSCtk53130

  Symptoms: You may be unable to configure pseudowire on a virtual PPP interface. The command is rejected with the following error:

  ```
  Incompatible with ipv6 command on Vp1 - command rejected.
  ```

  Conditions: The symptom occurs when an IPv6 address has already been configured on the virtual PPP interface.

  Workaround: There is no workaround.

- CSCtk53463

  Symptoms: For configuring the **shape average** *cir value bc value* command currently across all platforms, *bc value* is limited by 4ms * *cir value*. The 4ms here represents minimum interval time for bursts. ES+ LC however can support interval value that is faster (smaller) than 4ms. This has been expected behavior with exception of ES+ LC.

  Conditions: Currently all platforms restrict interval time for shape from going below 4ms.

  Workaround: There is no workaround.

- CSCtk53657

  Symptoms: WCCP black-holes traffic, if WCCP is disabled on the cache engine.

  Conditions: This symptom occurs when you configure WCCP to use L2 / Mask on the cache engine, leave the router interface up with the cable connected and disable WCCP on the cache engine. When the "SERVICELOST" message appears on the Cisco 7600 and the hardware is still programmed, WCCP blackholes the traffic.

  Workaround: There is no workaround.

- CSCtk53763

  Symptoms: Traffic for some of the SubLSPs is not flowing with P2MP TE or MLDP.

  Conditions: The symptom is observed with LSM and MLDP configurations with multiple SubLSPs.

  Workaround: Use the following command: **clear ip mroute ***.

- CSCtk54318

  Symptoms: VC creation fails on disabling and re-enabling the card for SIP-400 with 4XT3E3 SPA with below messages on console:

  ```
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed - fr_npc_vc_add: vc
  creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 0
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed - fr_npc_vc_add: vc
  creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 1023
  ```

  Condition: This issue is seen when the below commands are executed on a T3 serial interface of the SPA 4XT3E3 configured as DTE with frame relay encapsulation:

  no card type t3 *slot bay*

card type t3 *slot bay*

Then unconfigure and reconfigure frame relay enacapsulation.

Workaround: Reload the SPA.

- CSCtk55382

  Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail boot diagnostic test.

  Conditions: The symptom is observed when Control Plane Policing (CoPP) is configured on the system. The diagnostic test that fails is the "TestACLPermit" test displayed in "show diagnostic result". The output of "show module" will indicate a "Minor error" on the subslot.

  Workaround: Before a system reload or module reset, disable the CoPP feature. After the module is booted, CoPP can be enabled again.

- CSCtk57002

  Symptoms: For some PIM-SM groups, met3 entry becomes zero after SSO, when OIF is a port-channel.

  Conditions: This symptom occurs when the OIF is a port-channel

  Workaround: Perform a shut and no shut on the port-channel.

- CSCtk58732

  Symptoms: The router may crash if the following configuration is applied:

```
ip sla 1
icmp-jitter 192.0.2.1 source-ip 192.0.2.2 num-packets 1 interval 10
threshold 1000
timeout 1000
frequency 10

ip sla schedule 1 start-time now life forever

track 1 ip sla 1 reachability
```

  The following error message is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
0x62DA2E10
```

  Conditions: This symptom occurs in Cisco IOS Release 15.1(3)T release. The router may continually reload following the crash.

  Workaround: Use the ICMP Echo operation instead, as shown below:

```
ip sla 1
icmp-echo 192.0.2.1 source-ip 192.0.2.2
threshold 1000
timeout 1000
frequency 10
```

- CSCtk59347

  Symptoms: CPU is busy and console is locked up for minutes after entering the **clear counter** command.

  Conditions: This symptom occurs with a large scale configuration with hundreds of interfaces and service groups configured on the system.

  Workaround: Instead of clearing all counters of all interfaces, clear the counters of specific interfaces as needed.

- CSCtk59686

  Symptoms: Complete traffic drop occurs.

  Conditions: This symptom occurs when Stateful Switch Over (SSO) occurs and is followed by line card (LC) rest at head-end.

  Workaround: Delete and recreate the tunnel.

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while performing "write memory" or "show running configuration" on the router after configuring "privilege exec level 15 show adjacency".

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62247

  Symptoms: IKEv2 session fails to come up with RSA sign authentication.

  Conditions: The symptom is observed with a hierarchical CA server structure.

  Workaround: Use non-hierarchical CA servers.

- CSCtk62950

  Symptom: SSH over IPv6 may crash the router.

  Conditions: This symptom occurs with SSH over IPv6.

  Workaround: There is no workaround.

- CSCtk64538

  Symptoms: The **ip igmp join-group** and **ipv6 mld join- group** commands will not work as expected on Cisco 7600 platform.

  Conditions: This symptom occurs with basic configurations of join group on Cisco 7600 series routers.

  Workaround: Use the **ip igmp static-group** or **ipv6 mld static-group** commands instead.

  Further Problem Description: The **ip igmp join-group** and **ipv6 mld join-group** commands are not normal configurations on the Cisco 7600 router. They cause traffic to be punted to RP CPU and cause problems.

- CSCtk65429

  Symptoms: In an encrypted CE-PE session, traffic sourced by the VRF (for example, ping) works, but traffic coming from MPLS does not reach the crypto map.

  Conditions: This issue is observed in CEF code images, like Cisco IOS Releases 12.4(22)T2, 12.4(24)T4 and 15.1(3)T. This issue is not observed in 12.4 mainline releases, such as Cisco IOS Release 12.4(25d).

  Workaround: There is no workaround.

- CSCtk66080

  Symptoms: LACP/PAGP BPDUs are not tunneled by EVC Xconnect on ES+ and ES20.

  Conditions: This symptom occurs with EVC Xconnect with encapsulation untagged/deault and LACP/PAGP BPDUs ingressing on it.

  Workaround: There is no workaround.

- CSCtk66678

  Symptoms: T1s are down after ISSU CC/SPA upgrade from Cisco IOS XE31 or Cisco IOS XE32 to Cisco IOS XE33.

  Conditions: This symptom is observed only with images created between 10/10/2010 to 12/16/2010.

  Workaround: There is no workaround.

- CSCtk67073

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipsla.shtml.

- CSCtk67658

  Symptoms: Traceback and infrequent crash of the new active are seen when SSO is performed on a router.

  Conditions: This symptom occurs when SSO is performed on a router.

  Workaround: There is no workaround.

- CSCtk69810

  Symptoms: After performing In Service Software Upgrade (ISSU) from SRE1 CCO image to latest SRE3 on R4, the rwindex is set to invalid in the “catch all” entry. Because of this, the PIM neighbor on MDT is not up and the traffic does flow.

  Conditions: This symptom occurs after performing ISSU from SRE1 CCO image to latest SRE3 on R4.

  Workaround: Delete MDT and add it under VRF.

- CSCtk74970

  Symptoms: TE autoroute announced tunnel is not installed in the routing table.

  Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute announced tunnel is not installed in the routing table.

  Workaround: Configure “no ip routing protocol purge interface”.

- CSCtk76190

  Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than 10 instances.

  Conditions: The symptom is observed when the “TestSPRPInbandPing” fails for more than 10 instances.

  Workaround: There is no workaround.

- CSCtk83760

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

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

  Workaround: There is no workaround.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- CSCtk95742

  Symptoms: Traffic does not flow from EVC-BD.

  Conditions: This symptom occurs with port-channel EVC-BD configuratIon with ES20 memberlinks. This symptom occurs if ES20 LC is replaced with the ES+ LC and added the same port as ES20 to the port-channel.

  Workaround: Remove and add the EVC.

- CSCtk95992

  Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

  Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

  Workaround: Configure the command **dlsw udp-disable**.

  Further Problem Description: This symptom occurs in the following (and later) Cisco IOS Releases:12.4(15)T14, 12.4(24)T4, 15.0(1)M3, 15.1(1)S, 15.1(2)T, 12.2(33)SXI4, and 12.2(33)SXI4a.

- CSCtk98030

  Symptoms: After replacing an ES20 line card with an ES+ line card or vice versa in the same slot, some service groups reject new members to join if the old line card had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old line card. The named EVC cannot be deleted, complaining that it still has service instances.

  Conditions: The symptom is observed if an ES20 line card has been replaced with an ES+ line card or vice versa in the same slot. The old line card had ethernet service instance members in some service groups and/or named EVCs. The old associations between ethernet service instances and service groups or named EVCs are not cleaned up properly, blocking new association to these groups and EVCs.

  Workaround: Configure new service groups and named EVCs with same configuration as the problematic ones. Abandon the use of the old groups and EVCs. Assign ethernet service instances from the new line card to the new groups and EVCs.

- CSCtk98726

  Symptoms: ANCP shaper fails to be applied on ATM VC.

  Conditions: This symptom occurs after clearing and re-establishing the PPPoE session.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: The symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are 12.2(33)SRE, 15.0M, 12.2(33)XNE and later releases.

  Workaround: No workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in "show crypto session summary" output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.

  Workaround: Use save-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl05785

  Symptoms: Connectivity is broken on Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable. Input path is broken (packets are seen in netdr but do not reach the RP).

  Conditions: This symptom is observed on Cisco 7600 routers that are running Cisco IOS Release 12.2(33)SRE2. This issue is seen on Sip-400 subinterfaces.

  Workaround: Reload the router.

- CSCtl05926

  Symptoms: Packets exceeding the MTU size are dropped with the following error messages:

  *Dec 17 08:24:39.795: %CONTROLLER-3-TOOBIG: An attempt made to send giant packet on GigabitEthernet7/3/1 (1491 bytes from 10010046, max allowed 1476

  Conditions: This symptom occurs if the outgoing interface is on SIP400.

  Workaround: There is no Workaround.

- CSCtl05979

  Symptoms: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated to Standby RP, with policy-maps missing on Standby RP. PAC2 service should poison the PPPoE session.

  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with PAC2 ISG service are established.

  Workaround: Use dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl07955

  Symptoms: BFD neighbor goes down and does not come up again when an unrelated LC is powered down by using **no power enable module X** command.

  Conditions: This symptom occurs when an unrelated LC is powered down.

  Workaround: There is no workaround.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl08594

  Symptoms: After upgrading to Cisco IOS Release 15.1(3)T, routers are not able to connect to the EZVPN server anymore. ISAKMP fails to find the key.

  Conditions: This symptom occurs with the following conditions: - DHCP is configured on outside interface - Outside interface is FastEthernet. This symptom does not occur if the outside interface is VLAN. This symptom is not seen in Cisco IOS Release 15.1(2)T1

Workaround: Downgrade to 15.1(2)T1, use VLAN interface or remove "ip route 0.0.0.0 0.0.0.0 fastethernet4 dhcp" statement from the config and reload the router.

- CSCtl10395

  Symptoms: Control Plane Policing (CoPP) stops dropping packets in hardware on a Cisco 7600 series router after double switchover.

  Conditions: This symptom occurs on the Cisco 7600 platform when CoPP is configured on the router and SSO (HA Switchover) is done twice.

  Workaround: Remove and reconfigure the CoPP.

- CSCtl18652

  Symptoms: After replacing an ES20 with an ES+ line card on the same slot, or vice versa, adding ethernet service instance members from the new line card to an existing service group that was associated with the old line card may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

  Conditions: An ES20 line card has been replaced by a different type of line card or vice versa, on the same slot. New members are assigned to a service group that had members from the old line card. There is a standby RP in SSO mode.

  Workaround: Create a new service group with the same configuration as the existing group and assign new members to the new group. Abandon the use of the old group.

- CSCtl19347

  Symptoms: On configuring additional bundles, LC crashes. This occurs with SIP- 400 when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Conditions: This symptom occurs when copying the dLFI configurations from a disk to the running configuration to bundle up.

  Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl21884

  Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent even though the static route goes down.

  Conditions: The symptom is observed under the following conditions:

  - Enable auto-summary under the BGP process. - Static route is brought into the BGP table via the **network** command.

  Workaround: Use **clear ip bgp *** or disable **auto-summary** under the BGP process.

- CSCtl22871

  Symptoms: CoS value (applied from setcos policy) does not get copied to EXP while adding a label to the VPLS case, VPLS cfgd on EVC BD Vlan.

  Conditions: This symptom occurs on ES+ and QoS policy-map when set CoS is applied on EVC BD with VPLS configured on BD Vlan.

  Workaround: There is no workaround.

- CSCtl23348

  Symptoms: IOS crashes on OSPFv3 code.

  Conditions: This symptom occurs when the redistribution statement and the redistributed protocol are deleted simultaneously.

  Following is an example of a CLI that causes the IOS to crash, if it is copied and pasted:

  ```
  ipv6 router ospf 1
  no redistribute bgp 1
  !
  no router bgp 1
  ```

  Workaround: Do not delete the routing process at the same time as redistribution.

- CSCtl41921

  Symptoms: There is a traffic duplication.

  Conditions: This symptom occurs with bootup with scale having 2000 sLSPs.

  Workaround: Do a shut/no shut on the tunnel.

- CSCtl43925

  Symptoms: Including a P2P GRE tunnel in VRF on the access side, causes the multicast traffic for the VRF to be dropped.

  Conditions: After removing a GRE header and encapsulation change from Tunnel VLAN to QoS vlan, the next entry to be hit has incoming vlan as VPN QoS vlan. This symptom occurs only when CR=1. However, when the tunnels are brought up in vrf, CR=0 gets programmed, causing packets to get bridged and dropped.

  Workaround: Reload the LC or router in SM mode. Wait for a little while and start traffic again to trigger a re-install.

- CSCtl46703

  Symptoms: T1/E1 tributary on Prowler SPA stays down occasionally after LC/SPA is reloaded.

  Conditions: This symptom occurs after LC/SPA is reloaded.

  Workaround: Reconfigure clock configuration (e.g. vtg 1 t1 1 clock source line/internal) on the affected T1/E1.

- CSCtl46903

  Symptoms: VLAN mapping or translation feature does not work on ES+, when the port is configured as L2 switchport.

  Conditions: This symptom occurs when the port is configured on L2 switchport.

  Workaround: Configure the feature under EVC framework or L2 switchport on LAN cards.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed under the following conditions:

  - Use ECMP.
  - Use **mode monitor passive**.

Workaround: Remove equal cost routing. For instance, in a situation where you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly as necessary.

Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl50930

  Symptoms: For some SIP messages like OPTION, SBC asserts failure when called through VRF.

  Conditions: This symptom occurs on 1001, 1002, or 1004 non-redundant modes.

  Workaround: Configure the redundant mode SSO.

- CSCtl54033

  Symptoms: Resignaling sub-LSPs for P2MP TE tunnels may take up to 10 seconds, after the sub-LSP has been pruned or torn down.

  Conditions: This symptom occurs when a P2MP TE tunnel is configured to request FRR protection, but for the physical link down the path on the tunnel headend, there is no backup tunnel configured at the failure point (TE tunnel headend) to protect the sub-LSP. The TE tunnel headend will take 10 seconds for sub-LSP resignaling.

  Workaround: Configure FRR backup tunnels at TE tunnel headend to provide link protection for P2MP TE tunnels for the physical link that is connected to the TE tunnel headend in the TE tunnel path.

- CSCtl54415

  Symptoms: A Cisco router or switch may reload.

  Conditions: This symptom is experienced on multiple platforms when single- connection timeout is configured under an aaa group server, and there is no TACACS key configured:

  ```
  aaa group server tacacs+ <NAME>
   server-private x.x.x.x single-connection timeout 2
   server-private x.x.x.x single-connection timeout 2
   ip tacacs source-interface Loopback0
  (no tacacs-server key configured)
  ```

  Workaround: Either configure the correct matching key or do not configure single-connection timeout.

- CSCtl55828

  Symptoms: LDP/OSPF PDUs get dropped when line rate traffic is running on the Interface in case the link is over subscribed.

  Conditions: This symptom occurs with the following Hardware and software:

  Hardware - ES+ LC

  Software - Cisco IOS Releases 15.0(1)S, 15.0(1.1)S, 15.1(1)S Link over subscription, output drops at the MPLS interface.

  Workaround: There is no workaround.

- CSCtl57055

  Symptoms: A router may unexpectedly reload when the rttMonStatsTotalsEntry MIB is polled by SNMP.

  Conditions: The symptom is observed on a router that is running a Cisco IOS 15.1T release, is configured for SNMP polling, and when the rttMonStatsTotalsEntry is polled with an IP SLA probe configured.

  Workaround 1: Configure NMS to stop polling the rttMonStatsTotalsEntry or create a view and block the MIB on the router.

  Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl58005

  Symptoms: Accounting delay start is sent before any NCP has been negotiated, with “aaa accounting delay-start” configured. According to PRD, accounting start should not be sent until first NCP has been negotiated.

  Conditions: This symptom occurs when “aaa accounting delay-start” is configured.

  Workaround: There is no workaround.

- CSCtl67195

  Symptoms: The following three BGP debug commands are not allowed to enable:

  debug ip bgp vpnv4 unicast debug ip bgp vpnv6 unicast debug ip bgp ipv6 unicast

  Conditions: The symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- CSCtl69609

  Symptoms: When bringing down the shortest route, traffic blackholing occurs in MLDP on one of the OIFs.

  Conditions: This condition occurs in MLDP and branch point combination.

  Workaround: There is no workaround.

- CSCtl82922

  Symptoms: Fast memory leak occurs on standby Switch Processor (SP)/SP or DFC in the “mfib-const-lc” process. Once this process depletes memory, the starving system generates “MALLOC” errors for any other processes that request memory at that time. Eventually, standby SP crashes and the system operation recovers.

  “Holding” number in standby SP can grow with the speed of 60kB/s:

  ```
  #remote command standby-sp show proc mem | i mfib-const-lc|Holding

  PID TTY  Allocated     Freed    Holding    Getbufs    Retbufs Process

  281   0  106300144    4061004  103339316          0          0 mfib-const-lc

  Pr
  ```

  Conditions: This symptom is seen with the multicast stream timeout & restart in an MVPN environment. Stream S,G entry might not be installed in HW, and following MFIB Platform flags error might be seen for this stream along with the memory leak:

  ```
  #show ip mfib vrf <vrf_name> verbose | i HW_ERR

  (176.2.76.2,229.2.76.2) Flags: ET K DDE
  ```

Platform Flags: NP RETRY RECOVERY HW_ERR HAL:5

Workaround: There is no workaround.

- CSCtl83736

  Symptoms: Each V4 session set-up leaks approximately 100 bytes. Each V6 session set-up leaks approximately 112 bytes.

  The following command can be used to verify the above symptom:

  show platform software memory messaging ios rp active | inc st_sb_cfg

  Note that the "diff:" number increases continuously.

  Conditions: This symptom occurs in IP sessions.

  Workaround: There is no workaround.

- CSCtl85926

  Symptom: Output drops are observed when traffic is sent beyond 64k rate with single E1 when E1 is configured as unframed. Issue is seen rarely with using time-slots 1-31. After LC OIR, this symptom is not observed. If the channel is removed and attached, this issue reappears.

  Conditions: This symptom occurs on the following hardware and software:

  Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA

  Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later.

  Workaround:

  1. Configure a service policy like the following:

     policy-map test1

     class class-default

     queue-limit 386 ((this number is a interface bandwidth(in kbps)*1000 / (8 * 250 * 2) value for the

     correct behavior.). for T1 (1544, it will be 1544 * 1000 / (8*250*2) = 386). for Full E1, it will be 496.

  2. Reload line card.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: The symptom is observed when BGP is configured and you issue one of the following commands:

  show ip bgp all attr nexthop

  show ip bgp all attr nexthop rib-filter

  Workaround: Do not issue either of these commands with the **all** keyword. Instead, issue the address-family specific version of the command for the address family you are interested in.

  For example, the following are safe:

  show ip bgp ipv4 unicast attr nexthop

  show ip bgp attr nexthop

  show ip bgp vpnv4 vrf *vrfname* **attr nexthop**

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl90890

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtl93514

  Symptoms: QoS configurations do not get applied on the interfaces when the router is upgraded from ES20 to ES+.

  Conditions: This issue happens when the ES20 is replaced with ES+. Remove the ES20 LC and insert the ES+ LC on the same slot.

  Workaround: Remove all QoS policies applied on the ES20 interfaces. Insert ES+ and reapply all QoS policies once the ES+ interfaces are up.

- CSCtl97648

  Symptoms: Tab completion does not work.

  Conditions: This symptom occurs when IOS.sh is not enabled.

  Workaround: Enable Cisco IOS Shell (IOS.sh) using “term shell”.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtl98270

  Symptoms: Changing the VC hold-queue under the PVC on a WIC-1ADSL card is not reflected correctly in the **show hqf interface** output.

  Conditions: The symptom is observed in Cisco IOS 15.1(2)T2 Release and later releases.

  Workaround: Execute a shut/no shut to fix the issue.

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  config check syntax route-map hello match local-preference no match local-preference

  Conditions: The symptom is observed with the commands above.

  Workaround: There is no workaround.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic and in some cases may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn16899

  Symptoms: PIM neighborship is lost between source node and receiver nodes.

  Conditions: This issue is seen when TE FRR is configured for the link between source node and root node and after FRR cutover is done.

  Workaround: Shut and no shut the egress interface of the backup tunnel on the root node.

- CSCtn17267

  Symptoms: Broadband call admission control (CAC) is not working.

  Conditions: This symptom occurs under the following conditions:

  1. DHCP initiated sessions.
  2. PPPoE sessions on an interface where IP session configurations are present.

  Workaround: There is no workaround.

- CSCtn25100

  Symptoms: PPP sessions take longer to come up.

  Conditions: This symptom occurs in all conditions.

  Workaround: There is no workaround.

- CSCtn38711

  Symptoms: A router crashes.

  Conditions: This symptom occurs during SSO on a heavily loaded Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn41245

  Symptoms: Subinterface ingress stats do not work for access subinterfaces.

  Conditions: This symptom is observed only for the access subinterface. Interface stats and regular subinterface stats work as expected.

  Workaround: There is no workaround.

- CSCtn41662

  Symptoms: Standby RP crashes sometimes when policymap configuration is done. This crash happens randomly with the following crash decode:

  ```
  0xA65C01C:qm_make_final_vmr(0xa65bf14)+0x108
  0xA64799C:qm_send_merge_replace_request(0xa647834)+0x168
  0xA6471B0:qm_tm_merge_replace(0xa646ee4)+0x2cc
  0xA63B3FC:qm_tcam_modify_service_policy(0xa63adbc)+0x640
  0xA63A8AC:qm_process_mqc_event_hdlr(0xa63a51c)+0x390
  0xA63BE7C:qm_process_events_q_hdlr(0xa63bad0)+0x3ac
  0xA63CAA0:qm_process(0xa63c9cc)+0xd4
  ```

Conditions: This symptom occurs randomly when policymap, class-map is modified, which is applied on different interfaces. This does not happen consistently.

Workaround: There is no workaround.

- CSCtn60353

  Symptoms: In sub-package ISSU, some OM objects on standby RP may be missing.

  Conditions: This symptom occurs with ISSU between two releases and new release that adds new TDL message type.

  Workaround: Force a reload of the standby RP before a final RP switchover.

- CSCtn83293

  Symptoms: Out-to-in packets may drop because the ARP reply is missing from NAT router.

  Conditions: This symptom may happen under the following conditions:

  1. Inside global address is a subnet of the NAT outside interface.
  2. When the translation is created off of VRF NAT mappings.

  Workaround: Avoid using inside global address in VRF NAT static mapping or in the address pool of a dynamic mapping that belongs to an interface subnet.