Caveats for Cisco IOS Release 12.2(33)SB3 through 12.2(33)SB14

Caveats

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

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

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

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

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

This section consists of the following subsections:

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

Resolved Caveats—Cisco IOS Release 12.2(33)SB15

- CSCua40273

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCud24977

  Symptom: Crashes are observed on Cisco ISG ASR device.

  Conditions: Customer experienced this crash and the same crash was seen in ES special image asr1000rp2-adventerprisek9.V152_1_S1_CSCTY21366_2.bin in Cisco IOS Release 15.2(1)S2.

  Workaround: There is no workaround.

- CSCud31424

  Symptom: Missing forwarding for the VRF traffic after the PXF crash.

  Conditions: This behavior is observed following the PXF crash.

  Workaround: Shut/no shut on all PVC of VRF impacted.

- CSCui22578

  Symptom: ATM VC DOWN during switchover.

  Conditions: This symptom is observed during image upgrade or switchover, few ATM VCs go to DOWN or INAC state.

  Workaround: Remove and reconfigure the affected ATM sub-interfaces.

- CSCug34485

  Symptom: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

Condition: The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

Cisco has released free software updates that address this vulnerability.

Workaround: Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf

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 5.8/5.8:

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

CVE ID CVE-2013-0149 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

Resolved Caveats—Cisco IOS Release 12.2(33)SB14

- CSCty42892

  Symptoms: High CPU is experienced, caused by PPPoE session churn.

  Conditions:

```
router#sh processes cpu sorted
CPU utilization for five seconds: 91%/13%; one minute: 85%; five minutes:
82%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 382       42136      3099      13596 26.71%  9.04%  6.16%   5 Virtual Exec
 181   167143080 185108104        902 12.07% 12.95% 12.98%   0 SSM
connection m
 353    97467076  25441365       3831  8.39%  9.65%  9.81%   0 VTEMPLATE
Backgr
 242   580521844  12914275      44952  5.67%  6.70%  6.58%   0
c10k_periodic_st
 324   162851700   4632273      35156  3.75%  1.39%  1.42%   0 MFI LFD Stats
Pr
 237   127724132  13724836       9306  3.51%  0.85%  1.17%   0 Collection
proce
router#sh pppoe summary
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                                TOTAL     PTA   FWDED   TRANS
TOTAL                           18299   18184       4     111
ATM1/0/0                         1086    1082       0       4
ATM1/0/2                          265     262       0       3
ATM1/0/3                          591     583       0       8
ATM2/0/0                          473     472       0       1
```

```
ATM2/0/1                          1204    1200       0       4
GigabitEthernet3/1/0              3548    3532       0      16
GigabitEthernet3/1/1              3875    3852       2      21
GigabitEthernet5/1/0              3045    3021       0      24
GigabitEthernet5/1/1              3301    3273       0      28
iadsl-mch-uruapan-9#
```

So we can see the process using the most CPU is SSM manager. This looks like a pure QoS/C3PL issue. It is occurring under the SSM process context (as that is the client in this case).

```
Enter hex value: 0x408EF9BC 0x409927CC 0x4095BA60 0x4095B998 0x4047D588 0x40952480
0x40952F00 0x40953090 0x4046E384 0x4046F4D0 0x4046F74C 0x4046FB9C 0x404704B0
0x408EF9BC:process_may_suspend(0x408ef77c)+0x240
0x409927CC:ppcp_process_may_suspend(0x40992600)+0x1cc
0x4095BA60:dup_policymap_runtime_obj(0x4095b884)+0x1dc
0x4095B998:dup_policymap_runtime_obj(0x4095b884)+0x114
0x4047D588:fobjects_create_runtime_policymap(0x4047d404)+0x184
0x40952480:service_policy_install_common_impl(0x40951b08)+0x978
0x40952F00:service_policy_install_common(0x40952d50)+0x1b0
0x40953090:service_policy_install(0x40952f2c)+0x164
0x4046E384:qos_peruser_install_ssf_serv_policy(0x4046e2e0)+0xa4
0x4046F4D0:qos_peruser_dp_sss_update_qos(0x4046f358)+0x178
0x4046F74C:qos_peruser_dp_sss_install_context(0x4046f620)+0x12c
0x4046FB9C:qos_peruser_dp_sss_update_feature(0x4046f974)+0x228
0x404704B0:qos_peruser_dp_sss_update_feature_lock(0x4047046c)+0x44
```

Workaround: Reload.

- CSCtz06767

  Symptoms: SNMP OID ifHCOutOctets shows huge values in ATM interface.

  Conditions: The symptom is observed with ATM interfaces.

  Workaround: There is no workaround.

- CSCua50090

  Symptoms: PXF crashes in ESR PRE3 router.

  Conditions: The symptom is observed with MLPoLNS and normal LNS sessions across the router.

  Workaround: There is no workaround.

- CSCuc00787

  Symptoms: %ALIGN-3-CORRECT: Alignment correction made at 0xXXXXXXX writing 0xB0D0B11.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB10 or later.

  Workaround: There is no workaround.

- CSCuc19506

  Symptoms: 100MB of memory is currently not being properly mapped. This is leading to low memory conditions on some routers and fragmentation.

  Conditions: The issue seems to be introduced between Cisco IOS Release SB8 and SB9.

  Workaround: There is no workaround.

- CSCuc45762

  Symptoms: Router crash.

Conditions: When you issue the command **description xxxx**, it will accept the command and sync the active to standby. Then when you try to apply the default interface command for that interface, one sec reinitialize the fields of description to sync active to standby and there is some mismatch between active and standby, so the standby continuously reloads. The solution is to check the description string length does not maximum limit.

Workaround: Ensure the **description** command does not exceeded max of 200 characters. The limit of the description string is 200.

- CSCud05469

Symptom: A Cisco 10000 series router crashes when there are several PPPoE sessions in TRANS state and the command **show pxf cpu statistics interface** is entered:

```
10k2#show pppoe summ
    PTA  : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)

                      TOTAL     PTA   FWDED   TRANS
TOTAL                  3794    3594       0     200
GigabitEthernet6/0/0   3794    3594       0     200
10k2#show pxf cpu statistics interface g6/0/0

NOTE: Stats with active drops are prefixed by < or > characters:
    < Denotes input drops within the last second, > for output drops

  Interface GigabitEthernet6/0/0 (vcci 2525,  VLAN 1)
                               packets   pkts/sec          bytes    kbits/sec
  DATA RECEIVED                      0          0              0            0
   Total input drops                 0          0              0            0
  DATA TRANSMITTED              281744       1154       16676232          530
   Total output drops                0          0              0            0

...

Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x611EF5A4


-Traceback= 611EF5A4 611F0F34 611F12F0 611F159C 611ECC04 60538294 601C668C
605534B0 6065B670 6065B65C
$0 : 00000000, AT : 62FC0000, v0 : 00000009, v1 : 0B0D0B0D
a0 : 00000001, a1 : FFFFFFFF, a2 : 00000000, a3 : 00000000
t0 : 606A4F98, t1 : 3400FF01, t2 : FFFF00FF, t3 : 606A4F78
t4 : 606A4F78, t5 : 00000000, t6 : 00000020, t7 : 0000FF00
s0 : 67DC81D8, s1 : 62EC3B40, s2 : 71FC5C6C, s3 : 000003E8
s4 : 0000001D, s5 : 24C7BF58, s6 : 00000001, s7 : 000003E8
t8 : 63C7B7E4, t9 : 6069C9C8, k0 : 22D65934, k1 : 606906B0
gp : 62FC5F68, sp : 71F2FBF0, s8 : 24C7BE70, ra : 611EF5A0
EPC  : 611EF5A4, ErrorEPC : BFC00D7C, SREG     : 3400FF03
MDLO : 00000000, MDHI     : 00000002, BadVaddr : 0B0D0B3D
CacheErr : 00000000, DErrAddr0 : 00000000, DErrAddr1 : 00000000
DATA_START : 0x62C89630
Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception

Writing crashinfo to bootflash:crashinfo_20121102-
```

Conditions: The symptom is observed on a Cisco 10000 series router with any IOS version.

Workaround: Do not execute this command when there are several PPPoE sessions in TRANS state.

Resolved Caveats—Cisco IOS Release 12.2(33)SB13

Cisco IOS Release 12.2(33)SB13 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB13 but may be open in previous Cisco IOS releases.

- CSCsr64777

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

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

  Workaround: NetFlow version 9 could be used for exporting.

- CSCta44723

  Symptoms: Router crashes because alignment in aaa_idb_name_cleanup.

  Conditions: This is a memory alignment issue. The pointer pointing to “remote_id” in the “idb_name” structure is not properly aligned.

  Workaround: There is no workaround.

- CSCtb13469

  Symptoms: The Cisco CMTS crashes with error messages after configuring the SPA. The following error message is observed:

  ```
  SLOT 2: Jul 31 19:32:58.651 HKT: %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling
  of the chunk SIP netsync al, Chunk index : 58, Chunk real max : 58 -Process= "SIP
  netclk LC process"
  ```

  Conditions: “Chunk” can be used under interrupt context. Chunk infra protects from race conditions by raising interrupts when accessing critical sections, but currently it only raises interrupts to NETS_DISABLE level. As a result, if chunks are used in interrupts higher than that, it creates an issue.

  Workaround: There is no workaround.

- 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.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

  Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

  Workaround: Clear both sessions sharing the same IP.

- CSCtz00253

  Symptoms: Users will fail authentication when method EAP is used.

Conditions: A router working as a broadband aggregation device receives and processes authentication requests from multiple clients. In a standard deployment, the router will forward client credentials to an external Radius server for authentication. During the processes of packet exchange between the router and Radius server, specification mandates that each packet exchanged be encapsulate or tagged with an ID number. This ID number must increase by one, every time the content of the packet is new (every new access-request sent by the router). The exception to this rule is when the content is not new (i.e. a retransmission). In this case, the ID number must be equal to the previously sent ID. With EAP authentication, this is not happening. The router sends retransmitted content to the Radius server using a new ID value; therefore the Radius rejects the authentication.

Workaround: Configure the client to authenticate using a different authentication protocol (CHAP, PAP, MS-CHAP, MS-CHAP-V2).

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz61815

  Symptoms: After the PRE failover, the interfaces on SONET AUG/TUG controller on ESR-4OC3-CHSTM1 stay UP/DOWN and impact the traffic.

  Conditions: This symptom occurs when users remove the AU-4-TUG-3 controller through **no mode** command and reconfigure the same followed by a PRE failover.

  Workaround: Reconfigure the SONET controller or hw-mod reset the chstm card.

- CSCtz89608

  Symptoms: A router that is operating in an ISG environment experiences a crash due to memory corruption.

  Conditions: This symptom occurs within the SSS context.

  Workaround: There is no workaround.

- CSCub75120

  Symptoms: Traffic is not flowing after PRE switchover.

  Conditions: This symptom is observed on PTA based PPPoE sessions with QinQ encapsulation.

  Workaround: Clear all the sessions and re-establish the sessions.

Resolved Caveats—Cisco IOS Release 12.2(33)SB12

Cisco IOS Release 12.2(33)SB12 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB12 but may be open in previous Cisco IOS releases.

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  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_mar13.html

- CSCtl09030

  Symptoms: The Cisco ASR1k configured to function as ISG and DHCP relay/server crashes in the ARP input process or IP inband session initiator process in dhcpd_find_binding function.

  Conditions: This symptom is observed when the Cisco ASR1k is configured with DHCP relay or server and DHCP initiated IP sessions are configured. This issue is seen when the ISG inband IP session initiator is configured and an ARP request is received from a client whose DHCP IP session has timed out or cleared.

  Workaround: Disable ISG DHCP session initiator.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: The symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Release 12.2(33)SRB or later. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, e.g.: 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). It is seen with the following process:

  1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
  2. The allocated label changes from 16 to 17, e.g.: due to interface flapping or BGP attribute change.
  3. However, before the BGP import happens, a more specific prefix (e.g.: 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, RT policy.

  Workaround: Remove RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCto72927

  Symptoms: Configuring an event manager policy may cause a Cisco router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCtr28857

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

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

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

- CSCtr91106

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

  This advisory is available at the following link:

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

- CSCts04073

  Symptoms: A Cisco 10000 series router crashes when making configuration changes on an ATM module.

  Conditions: The symptom is observed when you remove a subinterface with PPP encapsulation and “create on-demand” and then reconfigure it quickly.

  Workaround: After deleting the subinterface, make sure all the VCs on the subinterface are cleaned up by doing a **show atm pvc**. When it is clean, start reconfiguring the subinterface.

- CSCts15034

  Symptoms: A crash is seen at dhcpd_forward_request.

  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.

  Workaround: If possible, from a functional point of view, remove the **ip dhcp relay information option vpn** command. Otherwise, there is no workaround.

- CSCts63581

  Symptoms: The standby PRE4 resets after write memory command at “Failed to sync private-config to standby RP”.

  Conditions: The symptom is observed with a scaled configuration that is more than NVRAM can store.

  This may occur when the standby NVRAM is locked by some other process and when config sync tries to access the standby NVRAM it fails. It then restarts the standby.

  Workaround: Significantly decrease configuration size, if possible.

- CSCts63737

  Symptoms: LI intercepts traffic from all L3 MPLS VPNs that have the target IP address in RIB.

Conditions: This symptom is observed with L3 MPLS VPNs with a duplicate IP addressing scheme and when LI tap is applied to one of the duplicate addresses. This issue is seen when the target route is flapped.

Workaround: There is no workaround.

- CSCts66808

  Cisco IOS Software contains a queue wedge vulnerability that can be triggered when processing IP tunneled packets. Only Cisco IOS Software running on the Cisco 10000 Series router has been demonstrated to be affected.

  Successful exploitation of this vulnerability may prevent traffic from transiting the affected interfaces.

  Cisco has released free software updates that addresses this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-c10k-tunnels

- CSCts68630

  Symptoms: IPv6 ACL may not match the traffic as per the configuration when there is an ACL configuration change.

  Conditions: This issue is seen when you configure an ACL list with a mix of ACL entries with the source address set to "any" and set with a specific value.

  Workaround: You can enter the ACL list entries in sequence in increasing order, for example:

```
permit icmp any host 2A00:2180:400:212:31:220:174:1 sequence 10
    permit icmp any host 2A00:2180:4400:204:109:193:249:1 sequence 20
    permit icmp any host 2A00:2180:4400:192:199:150:1:1 sequence 30 log-input
    permit tcp any eq bgp host 2A00:2180:4400:204:109:193:249:1 sequence 110
    permit tcp any host 2A00:2180:4400:204:109:193:249:1 eq bgp sequence 115
    permit tcp any eq bgp host 2A00:2180:4400:192:199:150:1:1 sequence 120
    permit tcp any host 2A00:2180:4400:192:199:150:1:1 eq bgp sequence 125
    permit udp any eq 1645 any range 1024 49151 sequence 210
    permit udp any eq 1812 any range 1024 49151 sequence 220
    permit udp any eq bootps any eq bootps sequence 310
    permit udp any host 2A00:2180:4400:204:109:193:249:1 range 3784 3785 sequence 410
    deny ipv6 any 2A00:2180::/37 sequence 510
    deny ipv6 any host 2A00:2180:4400:204:109:193:249:1 sequence 610
    deny ipv6 any host 2A00:2180:4400:192:199:150:1:1 sequence 615 log-input
    permit ipv6 any any sequence 999 log-input
```

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtx32321

  Symptoms: Unable to allocate memory due to memory fragmentation.

  Conditions: The symptom is observed with a Cisco 10000 series platform and when network applications allocate and de-allocate memory. Memory gets fragmented easily and this issue is seen.

  Workaround: There is no workaround.

- CSCty12754

  Symptoms: RFSS traceback seen on standby PRE while booting an image.

  Conditions: The symptom is observed while booting an image on HA setup.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SB11

Cisco IOS Release 12.2(33)SB11 is a rebuild release for Cisco IOS Release 12.2(33)SB. This section describes a severity 2 caveat that is open in Cisco IOS Release 12.2(33)SB11. There are other open caveats in Cisco IOS Release 12.2(33)SB11. However, open caveats are normally listed only for maintenance releases, and the listing of CSCts75470 is an exception.

- CSCts75470

  Symptoms: Packets do not get intercepted at MD due to multiple ACEs.

  Conditions: This symptom is observed after performing “microcode reload pxf” on IAP and CE1.

  Workaround: Delete the Tap and recreate it.

Resolved Caveats—Cisco IOS Release 12.2(33)SB11

Cisco IOS Release 12.2(33)SB11 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB11 but may be open in previous Cisco IOS releases.

- CSCsx64858

  Symptoms: A router may crash after the **show ip cef vrf** *VRF* **platform** command is issued.

  Conditions: This symptom occurs when BGP routes are learned via two equal paths within a VRF. If an update occurs so that only one path remains while the **show ip cef vrf** *VRF* **platform** command is issued, the router may crash.

  Workaround: There is no workaround.

- CSCsz56169

  Symptoms: A software-forced crash occurs after the **show user** command is issued.

  Conditions: This symptom occurs after the user issues the **show user** command and then presses the key for next page. This issue is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(21a).

  Workaround: Do not issue the **show user** command.

- CSCtb72734

  Symptoms: DHCP OFFER is not reaching the client when the unicast flag is set.

  Conditions: This symptom occurs only on Cisco ASR devices where creation or removal of the ARP entry does not maintain sequential ordering. As a result, the packet could arrive at the forwarding plane after the ARP entry has already been removed or before the ARP entry has been created.

  Workaround: There is no workaround.

- CSCtc47677

  Symptoms: The Cisco 7600 high availability router goes to RPR mode from SSO when forced switchover is performed.

Conditions: This symptom occurs when the **ip multicast vrf** *vrf1* **rpf select** *vrf2* command is configured. Later if the *vrf2* is deleted and a forced switchover is done, the router goes to RPR mode.

Workaround: Create the "vrf2" again and remove the **ip multicast vrf** *vrf1* **rpf select** *vrf2* first, followed by save and reboot.

- CSCtc94873

  Symptoms: After few show memory commands the telnet session to a Cisco 7600 series router is suspended and the router crashes. The traceback shows:

  ```
  -Traceback= 406AAEA0 406AB400 418164AC 418050B8 4067460C 406787E4 4067B7D8
  4063076C 423BB0F4 4065D058 417CB1C8 417CB1B4 Decode
  ```

  Conditions: This symptom is observed with a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 and with **show memory** commands.

  Workaround: Do not use **show memory fragment** commands.

  Further Problem Description: When BFD is enabled and when the command **show memory [fast] fragment detail** is invoked, the crash/hang is observed at times. This is partially fixed with this DDTS to overcome the SCHED-SEMNOTLOCKED error. Another part of it is fixed with CSCtd94438.

- CSCth87458

  Symptoms: Memory leak is detected in the SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

  Conditions: This symptom is observed during internal protocol robustness testing.

  Workaround: Allow SSH connections only from trusted hosts.

  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-2011-2568 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

- CSCti61949

  Symptoms: Unexpected reload occurs with a "SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header" and "chunk name is BGP (3) update" messages.

  Conditions: This 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.

- CSCtj48387

  Symptoms: After a few days of operation, a Cisco ASR router running as an LNS box crashes with DHCP-related errors.

  Conditions: This symptom occurs when DHCP is enabled and sessions get DHCP information from a RADIUS server.

  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.

- CSCto84267

  Symptoms: PRE crashes after CPU hogs (due to PPP Event) are observed.

  Conditions: This symptom occurs several seconds before the reload, when the following message is seen in the logs:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (20/17),process = PPP Events.
  ```

  Workaround: There is no workaround.

- CSCto90656

  Symptoms: The 24CT1/E1 card sends a packet with errors. (The inbound interface indicates frame and CRC errors.)

  Conditions: This symptom occurs when connected with a simulator and only occurs on port 0 and 1 on ESR-24CT1/E1. The reported tested release and combination is as follows:

  - PRE4 Cisco IOS Release 12.2(33)SB10 -> NG
  - PRE2 Cisco IOS Release 12.2(33)SB10 -> NG
  - PRE2 Cisco IOS Release 12.2(31)SB5 -> NG
  - PRE1 Cisco IOS Release 12.0(27)S4 -> Good

  Workaround: Reconfigure the **clock source** command in the following order:

  1. Type “clock source line” in controller configuration mode.
  2. Type “clock source internal” in controller configuration mode.
  3. Type “clock source line” in controller configuration mode.

  After this configuration, the symptom is cleared. However, after reloading the chassis, the issue recurs.

- CSCtq20994

  Symptoms: The following error message is displayed:

  ```
  %SYS-6-STACKLOW: Stack for process SSS Feature Manager running low, 0/6000
  and system crashing
  ```

  Conditions: This symptom occurs when there are several activities involved in associating or deallocating sessions.

  Workaround: There is no workaround.

- CSCtq41121

  Symptoms: NAT statements, which use a local interface, once removed, cannot be reconfigured.

  Conditions: This symptom occurs only in the case of dynamic PAT configurations when an interface overload configuration already exists. For example:

  ```
  ip nat inside source list list1 interface Vlan1 overload ip nat inside source
  static tcp 10.0.10.1 8080 interface Vlan1 8080
  ```

  Removal and reconfiguration of the above dynamic PAT configuration is not possible, and the following error message is displayed:

  ```
  %Port 8080 is being used by system
  ```

Workaround: There is no workaround.

- CSCtq49179

  Symptoms: Packets are not matched in the user-defined classes that are classifying traffic based on the DSCP markings on the physical interface.

  Conditions: This symptom is observed only if the call is an MLPPP call over L2tp. The issue is not seen with a non-MLPPP call.

  Workaround: There is no workaround.

- CSCtq61477

  Symptoms: Memory leak is seen with turbo ACL and PPPoE configuration.

  Conditions: This symptom is observed while churning PPPoE sessions.

  Workaround: There is no workaround.

- CSCtr04829

  Symptoms: A device configured with “ip helper-address” drops packets because of a zero hardware address check.

  Conditions: This symptom occurs when the hardware address is zero.

  Workaround: There is no workaround.

- CSCts37435

  Symptoms: MVPN groups are not populated in the VRF.

  Conditions: This symptom is observed in MVPN with an ACL.

  Workaround: There is no workaround.

- CSCts44198

  Symptoms: Duplicate LI ACL entries are created on tapped interface when LI tap is applied on the Cisco 10000 series router.

  Conditions: This symptom occurs when the prefix of the intercepted target IP flaps.

  Workaround: Remove the tap configuration for flapping prefix.

- CSCts48540

  Symptoms: PXF drop occurs on the MPLS-enabled interface due to “acl denied” on the Cisco 10000 Series Router configured with LI targets.

  Conditions: This symptom occurs when all the uplinks are MPLS-enabled and the aggregate or default route for the LI target prefix is advertised via MP-BGP from RR or PE routers.

  Workaround 1: Make sure that LI tap is applied to a non-MPLS interface only.

  Workaround 2: Remove the LI tap configuration.

  Workaround 3: If the LI target prefix flaps, make sure to avoid it, if possible.

- CSCts81327

  Symptoms: On a Cisco 10000 series router that has LI done with a session brought up via radius and that is using SNMP session ID taps, LI is not working.

  Conditions: This symptom is observed only when using session ID taps in SNMP and bringing up sessions via radius.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB10

Cisco IOS Release 12.2(33)SB10 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB10 but may be open in previous Cisco IOS releases.

- CSCsi32894

  Symptoms: When a policy with BRR configuration has a priority class configured as well, the priority class gets a queue update with minCIR set to 0 and the excess ratio set to 1.

  Conditions: This symptom is observed when a policy with BRR configuration has a priority class configured as well, the priority class gets a queue update with mincir set to 0 and the excess ratio set to 1. This should not be the case for two reasons:

  1. Priority should not participate in the BRR calculations (it actually does not, but we end up invoking the queuing API with incorrect parameters).
  2. Though the platforms can determine if a queue update that they get is for a priority queue, and maybe ignore mincir if the excess ratio is set, they do not necessarily have to do that.

  Workaround: There is no workaround.

- CSCso38836

  Symptoms: An alignment error is seen while configuring Virtual-template for PPP over AAL5 encapsulation for PVC in an ATM subinterface. The "% Ambiguous command:" message is displayed and "proto ppp" does not take effect.

  Conditions: This symptom is observed when the following commands are configured:

  ```
  configure terminal
      interface ATM6/0.2 point-to-point
      shutdown
      pvc 4/64
      encapsulation aal5snap
      protocol ppp Virtual-Template1
  ```

  Workaround: There is no workaround.

- CSCso74028

  Symptoms: The local PE is sending graft messages even after receiving data from the remote PE on an MVPN network.

  Conditions: This symptom is observed when the graft-ack messages are lost in transit (could be due to misconfiguration/ACL, etc.).

  Workaround: Fix the misconfiguration so that graft-ack messages are forwarded as expected.

- CSCtb40999

  Symptoms: Autovc behavior is different in standby after SSO.

  Conditions: This symptom occurs when autovc is configured in a range, and a pvc-in-range is configured for no autovc. After doing SSO, the VC is in IN. Autovc should not be displayed in "show atm vc" if it is configured in a range. Please see "steps to reproduce" for more details.

  Workaround: There is no workaround.

- CSCte97113

  Symptoms: The **configure replace** command fails and crashes the standby when you try to replace an existing configuration on the active that has parser views configured with a configuration that does not have any parser views configured.

  Conditions: This symptom is observed when the user is in root view mode while configuring a parser view. During configure replace, the standby is not set into root view mode.

  Workaround: Manually remove/configure the parser view on the active to match with what it is in the saved configuration before opting for configure replace.

- CSCte99373

  Symptoms: The extranet receiver retains RPF pointing to a nonexistent source MVRF, which can lead to a crash.

  Conditions: This symptom is observed when PIM is disabled on the source RPF interface or RPF on the source MVRF mroute changes to NULL (that is, unreachable) under the extranet scenario. If mroute is cleared in the source MVRF, it will lead to a crash.

  Workaround: There is no workaround.

- CSCtf18652

  Symptoms: The router crashes.

  Conditions: This symptom is observed when removing frame-relay inverse ARP and policy-map from the serial interface. It is seen with a Cisco 10000 series router.

  Workaround: When applying **no frame-relay inverse-arp <dlci>**, ensure that the DLCI number is same as the one configured through **frame-relay interface-dlci <dlci>**.

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory-corruption with block overrun.

  Conditions: This symptom is observed when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in the same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCtg72243

  Symptoms: DPM DHCP VRF ID is leaking memory on the standby.

  Conditions: This symptom is observed when you bring up a DHCP session with a VRF configuration. When the session is synced to the standby, memory for the VRF ID is leaked on the standby RP.

  Workaround: There is no workaround.

- CSCth25634

  Symptoms: The password is prompted for twice for authentication.

  Conditions: This symptom occurs when login authentication has the line password as fallback and RADIUS as primary, for example, when you configure the **aaa authentication login** command as follows:

  ```
  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, users providing the wrong password at the password prompt will be granted access if the following is configured:

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

- CSCth46888

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

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

  Workaround: There is no workaround.

- CSCth75053

  Symptoms: The interface does not pass traffic anymore. The **show pxf interface** command shows that the interface is always in XOFF state.

  Conditions: This symptom is observed on the Cisco 7300 with PXF.

  Workaround: Upgrade the FPGA image to the latest version bundled in Cisco IOS Release 12.2(33)SB10.

- CSCth84370

  Symptoms: The Standby Supervisor gets reloaded when **write memory** is run from one VTY, and then later, **show configuration** is run from another VTY. No particular configuration needs to be done prior to **write memory**.

  Conditions: This symptom occurs when the Dual Supervisor is used and the configuration file is quite long.

  Workaround: Do not run the **write memory** and **show configuration** commands simultaneously.

- CSCti25339

  Symptoms: The Cisco IOS device may experience a device reload.

  Conditions: This symptom 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 Denial of Service (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

- CSCti48793

  Symptoms: The Cisco 7300 running Cisco IOS Release 12.2.33SB8 and earlier versions of Cisco IOS Release 12.2.31SB18 experience a header buffer leak due to a htf_output_enqueue data size of >460 and a large rate on the POS interface.

  Conditions: This symptom is observed when the size of IP data packets is greater than 460 on the POS interface.

  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.

- CSCtj01554

  Symptoms: PRE-2 crashes without valid crashinfo.

  Conditions: This symptom is observed when PRE-2 crashes without valid crashinfo.

  Workaround: There is no workaround.

- CSCtj08533

  Symptoms: QoS classification fails on egress PE if the route is learnt via BGP.

  Conditions: This symptom is observed when there are redundant paths to the CPE.

  Workaround: Use only one path between PE and CPE.

- CSCtj28015

  Symptoms: ISG crashes at "no interface a2/0/0.1 multipoint".

  Conditions: This symptom is observed on the Cisco 10000.

  Workaround: There is no workaround.

- CSCtj34568

  Symptoms: A router running Cisco IOS Release 12.2(33)SB6b crashes after unconfiguring a VRF due to a bus error.

  Conditions: This symptom is observed when a router that is running Cisco IOS Release 12.2(33)SB6b crashes after unconfiguring a VRF due to a bus error. This issue is seen on the VRF that does not have any RD and **route-target import export** configured. PRE2 crashes when you delete the VRF as follows:

  no ip vrf PingTestVRF<cr>

  Workaround: Do not delete the VRF.

- CSCtj37698

  Symptoms: Cisco IOS 10000 Series routers that are acting as VPDN multihop, reset the TOS value to 0 when the **ip tos reflect** command is applied to the VPDN tunnel to LAC. This occurs downstream from LNS to the LAC.

  Conditions: This symptom occurs under a normal VPDN configuration.

  Workaround: There is no workaround.

- CSCtj43910

  Symptoms: The box crashes while displaying output of the **show subscriber session detail internal** command.

  Conditions: This symptom is observed if the terminal length is configured with a small value and if sessions are down while displaying output of the show subscriber session detail internal command.

  Workaround: Configure the terminal length with a very high value. Do not remove sessions while using the more option of the **show sss session detail internal** command.

- CSCtj48220

  Symptoms: A Cisco router may unexpectedly reload due to bus error.

  Conditions: This symptom occurs with AAA.

  Workaround: There is no workaround.

- CSCtj61284

  Symptoms: NAT overload does not work for nondirectly connected destinations in MPLS-VPN configurations.

  Conditions: This symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

  Workaround: There is no workaround.

- 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.

- CSCtj64807

  Symptoms: The router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: This symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with the same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash on any subinterface if the outer VLAN has a second dot1q VLAN as only “any”, immediately delete the subinterface and recreate it. Then, add a dummy VLAN/subinterface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than five inner VLANs, add a dummy VLAN/subinterface.

Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with a second dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtj74542

  Symptoms: The router crashes.

  Conditions: This symptom is observed on a Cisco 10000 series router when you configure more than 33 QinQ subinterfaces, all having the same outer VLAN and at least one of them has a second dot1q configured as “any”. Bring up a PPP session through the subinterface that has the second dot1q configured as “any”. Delete all other subinterfaces. Then, try to clear the PPP session or delete the last subinterface.

  Workaround: There is no workaround.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: This symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

  Workaround: There is no workaround.

- CSCtk62453

  The Cisco 10000 Series Router is affected by a denial of service (DoS) vulnerability where an attacker could cause a device reload by sending a series of ICMP packets.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are also available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-c10k.shtml.

- CSCtk69314

  Symptoms: Traceback seen for the following error message after switchover:

  ```
  Jul 31 03:22:48 EDT: %COMMON_FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface
  for
  ATM3/0/0.15203 with illegal if_number: -1
  ```

  Conditions: This symptom is observed when an incomplete **interface** command is give for ATM interfaces:

  ```
  dt210(config)#int ATM2/0/0.200 %
  Incomplete command.
  ```

  Workaround: There is no workaround.

- CSCtl06259

  Symptoms: On a Cisco IOS 10000 series router running Cisco IOS Release 12.2 (33)SB08e, the **show ip cef vrf <vrf> platform** command might show incomplete output, which may include only the following fields:

  ```
  c10k_label_data = 0xCFEE3D80
  tag_elt_addr = 0x0
  ipv6_tag_elt_addr = 0x0
  ```

  Conditions: This symptom occurs on a Cisco IOS 10000 series router running Cisco IOS Release 12.2(33)SB08e.

Workaround: Use the **clear ip route vrf <vrf>** command to display the correct output.

- CSCtl71478

  Symptoms: In an HA system, the following error message is displayed on the standby RP and LC:

  ```
  OCE-DFC4-3-GENERAL: MPLS lookup unexpected
  ```

  Conditions: This symptom is observed on standby/LC modules when you bring up both the RP and standby/LC routers with or without any configuration.

  Workaround: There is no workaround.

- CSCtn27077

  Symptoms: Multicast packets are being dropped during some instances where the rate-limit on the 7300 is being enforced.

  Conditions: This symptom occurs during high periods of multicast flows or even low periods. There is no specific traffic load that triggers this rate-limit.

  Workaround: The workaround is currently unknown. Preliminary suggestions are to increase the heartbeat packets to at or below 30 seconds so that the S,G does not go into Registering state.

- CSCtn42029

  Symptoms: PXF CPU CEF memory leak at HW Mac rewrite component.

  ```
  #show pxf cpu cef memory
  FP CEF/MFIB/TFIB XCM Type usage: Type Name Col Total Alloc Size Start End BitMap Error
  ...
      6 Mac 5 524279 383641 8 30800000 30C00000 CB394174 0 <===
  HW Mac rewrite memory allocation level
  ...
  C10K CEF/MFIB/TFIB PXF allocations:
  Types Alloc Failed
  Leaves 65598 0
  Nodes 21205 0
  Loadinfo 2047 0
  Adjacency 87576 0
  Rewrite 383642 0 <=== HW Mac rewrite allocated memory
  ```

  Conditions: This symptom is observed when lawful intercept taps are configured on the router.

  Workaround: Use the following workarounds:

  1. Switchover
  2. Reload
  3. Remove all LI taps

- CSCtn59698

  Symptoms: When an MLP bundle comes up on LNS with conditional debugging based on user name 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's 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>**.

- CSCtn68296

  Symptoms: The Cisco 10000 PRE3 router shows traceback. %GENERAL-3-EREVENT: HW_MFIB:Extranet does not allow a source (receiver) to be a receiver (source) for the same group.

  Conditions: This symptom is observed with multicast extranet.

  Workaround: There is no workaround.

- CSCtn81945

  Symptoms: Extranet mroute linkage is corrupted.

  Conditions: This symptom occurs when RPF changes in a source mroute that triggers it to becoming a receiver mroute while receiver mroutes are still linked to it, or a receiver mroute transitions to becoming a source mroute while other potential receiver mroutes have already performed the linkage.

  Workaround: Clear ip mroute in all affected VRFs.

- CSCtn98380

  Symptoms: The router crashes shortly after upgrade to Cisco IOS Release 12.2(33)SB9 with corrupted stack trace.

  Conditions: This symptom is observed when the router is unable to create hardware keepalives for a PPP session on a Gigabit or Fast Ethernet interface.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SB9

Cisco IOS Release 12.2(33)SB9 is a rebuild release for Cisco IOS Release 12.2(33)SB. This section describes three caveats that are open in Cisco IOS Release 12.2(33)SB9. There are other open caveats in Cisco IOS Release 12.2(33)SB9. However, open caveats are normally listed only for maintenance releases, and these listings are an exception.

- CSCtk10598

  Symptoms: Ping fails when second link is added in the bundle.

  Conditions: This symptom occurs under the following conditions:

  - Using multiples links in the bundle
  - Using VPDN
  - Using L2tp establishment via MP-BGP
  - Using L2tp establishment via tagged interface

  Workaround: There is no workaround.

- CSCtk62453

  Symptoms: Padded ICMP packets with TTL 1 on IP session cause a PXF crash.

  Conditions: This symptom occurs when ICMP padded packet with TTL 1 or zero is received, the packet is dropped and an ICMP unreachable is sent. This is the ICMP unreachable packet formation that is causing the crash.

Workaround: There is no workaround.

- CSCtl50957

  Symptoms: A PXF crash is experienced on a Cisco 10000 series router PRE3 that is running Cisco IOS Release 12.2(33)SB9.

  Conditions: This symptom occurs under normal working conditions.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB9

Cisco IOS Release 12.2(33)SB9 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB9 but may be open in previous Cisco IOS releases.

- CSCek10384

  Symptoms: A Cisco 7200 router that is performing NAT could drop IPSec packets.

  Conditions: This symptom is observed on a Cisco 7200 router that is performing NAT functionality for IPSec transit packets. The router will NAT and forward the Inside to Outside IPSec (ESP) packets, but might drop the return IPSec packets from Outside to Inside.

  Workaround: Disable NAT for IPSec.

- CSCek39299

  Symptoms: The standby PRE keeps resetting.

  Conditions: This symptom occurs when the configuration has “bgp dampening”.

  Workaround: Remove the “bgp dampening” configuration before:

  1. Cisco IOS upgrading
  2. Standby PRE resetting/replacement
  3. Force switch over

  After both cards come up, the “bgp dampening” can be added back.

- CSCek48205

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

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

  Workaround: There is no workaround.

- CSCsb37698

  Symptoms: When you configure NAT, an IPv6 configuration is evoked unintentionally in addition to the NAT configuration.

  Conditions: This symptom is observed when you enter the **ip nat pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command. When you do so, the output of the **show running-config** command shows the above-mentioned command and, in addition and unexpectedly, also the **ipv6 nat v6v4 pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command.

  Workaround: There is no workaround.

- CSCsc13670

  Symptoms: The backup configurations that are generated by the Archive feature may be truncated.

  Conditions: This symptom is observed when you reload the router with the Archive feature enabled.

  Workaround: Enter the privileged mode.

  Another workaround is using Kron,

  Since archiving works fine if we use the archive config command we can schedule the command,

  For example,

  kron policy-list CONFIG-ARCHIVE

  cli archive config

  kron occurrence CONFIG-ARCHIVE in 1:0 recurring

  policy-list CONFIG-ARCHIV

- CSCsh96558

  Symptoms: A traceback may be generated during the “ipmcast_ipv6_rpf_lookup” function.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when you configure IPv6 multicast routing on both the PE router and a connected CE router, add an IPv6 address to the connected interfaces, and configure PIM sparse or PIM sparse-dense mode on both routers. The traceback is generated when the neighborship comes up after you have configured one of the interfaces as a PIM-RP.

  Workaround: There is no workaround.

- CSCsi97428

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

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

  Workaround: There is no workaround.

- CSCsk35688

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

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

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

  Further Problem Description: The periodic function is by default called at 60 second intervals. The aggregate processing is normally done based on the CPU load. If there is no CPU load, then the aggregate processing function would be triggered within one second. As the CPU load increases, this function call will be triggered at higher intervals and if the CPU load is very high it could go as high as the maximum aggregate timer value configured via command. By default this maximum

value is 30 seconds and is configurable with a range of 6-60 seconds and in some trains 0. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- CSCso18626

  Symptoms: Destinations via MLPPP sessions may become unreachable following a switchover.

  Conditions: The symptom is observed when MLPPP sessions are active and BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

  Workaround 1: The affected multilink interfaces can be shut/no shut:

  shut/no shut interface multilink <>

  Workaround 2: Repopulating the routes in the affected VRF(s) will also restore reachability:

  clear ip route vrf FOO

- CSCso30942

  Symptoms: A Cisco 10000 router may see PXF-crashes with “PXF DMA TBB Not enough Data”, “PXF DMA TBB Giant”, or “PXF DMA Toaster Stall Error”.

  Conditions: This symptom is seen when a tapped session is sending traffic to an overloaded egress port.

  Workaround: There is no workaround.

  Further Problem Description: The software in use is a customer-specific special based on Cisco IOS Release 12.2(31)SB13 and also impacts Cisco IOS Release 12.2(34)SB.

- CSCso52837

  Symptoms: The following error is received:

  %Error parsing filename (No such device)

  Conditions: This symptom is observed when the **copy run disk0:test** command is executed.

  Workaround: Use a “/” as in **copy run disk0:/test**.

- CSCso70645

  Symptoms: DHCPv6 relay does not add the VSIO option to the forwarded packet.

  Conditions: This symptom is seen while checking for the configuration of VSIO option in the packet.

  Workaround: There is no workaround.

- CSCsq11897

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

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

  Workaround: There is no workaround.

- CSCsq47593

  Symptoms: Network start record accounting has wrong value for Acct-Tunnel- Connecti[68].

  Conditions: When “aaa accounting network default start-stop” is configured, network start/stop accounting will be sent for each VPDN session. One of the attributes of this start record is Acct-Tunnel-Connecti[68] which contains value of call serial number. On Cisco IOS Release 12.4T and Release 12.2SR, this attribute has truncated value. MSB 2 bytes are lost.

  Workaround: There is no workaround.

- CSCsq86500

  Symptoms: The following error message is displayed when the standby is reloaded:

  ```
  "REDUNDANCY-3-IPC: cannot open standby port no such port"
  ```

  Conditions: No specific condition.

  Workaround: There is no workaround. The error message is harmless and does not affect the functionality of the router in any way.

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This issue is observed when sending request to particular server on a server-group.

  Workaround: There is no workaround.

- CSCsr55922

  Symptoms: The EIGRP IPv6 process may incorrectly select a router-ID from the 127.0.0.0 address range.

  Symptoms: The same router-ID may be selected on two separate Cisco routers configured for EIGRP IPv6. External prefixes advertised by one of the EIGRPv6 routers will be ignored by the receiving EIGRPv6 router due to the fact the routerID contained in the external data portion of the prefix matches the receiving routerID; a loop prevention method.

  Workaround: Manually configure a router-ID under the EIGRP IPv6 process with **router-id** *address* command.

- CSCsr88705

  Symptoms: Redistributed routes are not being advertised after a neighbor flap.

  Conditions: This symptom is observed if BGP is redistributing local routes and if there are multiple neighbors in the same update-group and then a neighbor flaps. For the flapped neighbor, some redistributed routes are not being advertised.

  Workaround: Undo and redo the redistribution.

- CSCsr90248

  Symptoms: Changing any of the parameters of a route-map does not take effect.

  Conditions: Occurs when using a BGP aggregate-address with an advertise map.

  Workaround: Delete the aggregate-address statement and then put it back for the change to take effect.

- CSCsr93602

  Symptoms: A PRE crash may occur when the ATM idle timer times out.

  Conditions: This symptom occurs during the provisioning of a new ATM virtual circuit. An idle timeout may result in a PRE crash.

  Workaround: There is no workaround.

- CSCsu09999

  Symptoms: Turning PFC on PQ traffic results in protocol field from being removed from the packet.

  Conditions: This symptom occurs with loss of ping packets when generated by RP with ToS byte set.

  Workaround: There is no workaround.

- CSCsu49189

  Symptoms: Frame-Relay fragment output not seen when modifying the attached map-class.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: Detach and attach Frame-Relay fragment.

- CSCsu76993

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

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

  Workaround: There is no workaround.

- CSCsu88107

  Symptoms: A Cisco 7206VXR/NPE-G2 crashes with the error “Unexpected exception to CPU :vector 400”.

  Conditions: Not specifically known. The issue is seen, however, when the router upgrades from Cisco IOS Release 12.2(31)SB11 to Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu96698

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

  Conditions: This occurs only with very large configurations.

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

- CSCsv29659

  Symptoms: RP configured inside a NAT not shown on test device outside the NAT.

  Conditions: Entering the **show ip pim rp mapping** command fails to display the RP.

  Workaround: There is no workaround.

- CSCsv38225

  Symptoms: Router may reload when you unconfigure and then configure the **ipv multicast-routing** commands in quick succession.

  Conditions: Occurs when these commands are entered in quick succession, such as with copy and paste.

  Workaround: Allow for a delay when entering the commands **ipv multicast-routing** and **no ipv multicast-routing**.

- CSCsv66694

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

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

  Workaround: There is no workaround.

- CSCsv84557

  Symptoms: Acct-Session-Id is not being created when unique-ident is configured.

  Conditions: This symptom is seen when Acct-Session-Id is not being created when radius-server unique-ident is configured in NAS.

  Workaround: There is no workaround.

- CSCsw21000

  Symptoms: Active-RP crash always occurs with core/crashinfo by an abnormal DHCPv4 sequence. This problem is seen soon after the abnormal sequence starts.

  Conditions:

  – ASR is set as a dhcp relay agent.
  – 8k vlan configuration.
  – 8 port-channel configuration.
  – Not any other traffic and stress.

  Workaround: There is no workaround.

  Further Problem Description:

  – Problem may be memory corruption issue.
  – DHCP request packet is abnormal in this case.

- CSCsw41706

  Symptoms: A Cisco router may unexpectedly reload or produce an error similar to the following:

  ```
  Embedded Event Manager configuration: failed to stage user library directory
  <device>:<directory>: error creating file
  ```

  Conditions: This occurs when trying to configure the **event manager directory user library** *device:directory* command.

  Workaround: There is no workaround.

- CSCsw43499

  Symptoms: Accounting start sent on DHCP OFFER rather than ACK.

  Conditions: This issue can cause accounting irregularities if the DHCP process does not complete. For example, with active-active Cisco Intelligent Services Gateway (ISG) redundancy, two DHCP OFFERs will be sent, but only one will be accepted. Since accounting records are generated for both OFFERs, they will be duplicates of each other.

  Workaround: There is no workaround.

- CSCsw92379

  Symptoms: Many “IP ARP: Sticky ARP entry invalidated” syslog messages appear, and the RP reloads unexpectedly.

  Conditions: This symptom is observed when a line card is swapped while thousands of DHCP snooping bindings are present, and the **ip sticky-arp** command is configured.

  Workaround: Configure the **no ip sticky-arp** command.

- CSCsx02019

  Symptoms: Continuous IPC hog and high CPU utilization is seen.

  Conditions: The symptom is seen on a Cisco 7600 series router. It can be re-created by doing the following commands when the router is running 12k DHCP sessions:

```
1.rst7609-6(config)#redu
 rst7609-6(config)#redundancy
 rst7609-6(config-red)#mode
 rst7609-6(config-red)#mode rpr

 2.rst7609-6(config)#redu
 rst7609-6(config)#redundancy
 rst7609-6(config-red)#mode
 rst7609-6(config-red)#mode sso
```

Upon toggling the redundancy states from SSO to RPR and back we can see consistent IPC hogs on the router.

Workaround: There is no workaround.

- CSCsx08861

  Symptoms: ATOM VC status is seen as down in standby RP and traffic loss is seen after switchover for 44 seconds.

  Conditions:

  1. Bring 6RU up (SSO) with 1 AToM VC, 1 AToM VP (Initial VC state: active:UP; standby:HOTSTANDBY)
  2. Delete the AToM VC sub-int (“no int a2/2/0.122”) and delete the AToM VP sub-int (“no int a2/2/0.1001”)
  3. Re-configure back the same AToM VC and VP configuration (VC state: Active:UP; Standby:DOWN for AToM VC)
  4. If I do a force switchover (’redundancy force-switchover’). It will experience ~44 seconds of traffic lost for this VC.

  Workaround: There are two work around for this issue:

  1. Do not reconfigure the ATOM VC immediately after deleting a subinterface.
  2. Do not copy and paste the ATOM VC configuration. Either do it manually step by step or copy the configuration from a file.

- CSCsx09343

  Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

  Conditions: The symptom is observed when using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). It is only applicable if **ip domain-lookup** command is enabled within the configurartion.

  Workaround: There is no workaround.

- CSCsx20177

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

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

  Workaround:

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

    Or with “"advertise passive-only”:

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

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

- CSCsx27496

  Symptoms: Router may crash with an address error in the BGP function.

  Conditions: The symptom is observed when the router is configured for BGP and traffic is passing.

  Workaround: There is no workaround.

- CSCsx46854

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

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

  Workaround: There is no workaround.

- CSCsx64122

  Symptoms: Service policy disappears from Multilink Frame Relay (MFR) interface.

  Conditions: This is observed after MFR interface flaps.

  Workaround: There is no workaround.

- CSCsx87562

  Symptoms:

  The following error is seen following interface range configuration change:

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

  Conditions: This symptom is seen with dual supervisors installed and affects these Cisco Catalyst 4000 releases: 12.2(52)SG/XO, 12.2(50)SG4/5/6/7, 12.2(53)SG/SG1/SG2. This bug applies to all hardware, not specific to Cisco Catalyst 4500 switches.

  Workaround:

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

  Resolution: Fix is available in Cisco IOS Release 12.2(54)SG which is available to download on cisco.com. Fix will also be in Cisco IOS Release 12.2(53)SG3 and Release 12.2(50)SG8.

- CSCsy19751

  Symptoms: Several chunk element leakages are seen when the **show memory debug leaks chunk** command is entered.

  Conditions: Occurs after a reboot.

  Workaround: There is no workaround. Please ignore the leaks as they are false alarms.

- CSCsy24878

  Symptoms: Bulk sync fails.

  Conditions: Occurs when the **relay destination** command is configured on the device.

  Workaround: There is no workaround.

- CSCsy29534

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

Conditions: It was observed in the following context:

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

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

- CSCsy39667

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ Address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The symptom is observed on a Cisco 7200 (NPE-400) and 7200 (NPE-G2) that is running Cisco IOS Release 12.4 T, or 12.2 SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server. If a lease is found to only exist on the PPP aggregator, use **clear interface virtual-access** to recover.
  2. Manual: use the command **clear interface virtual-access**.

  Further Problem Description: This issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire.

- CSCsy47987

  Symptoms: After an RP switchover occurs, some PPP interfaces remain up/down until the router is reloaded or the encapsulation is changed to HDLC.

  Conditions: The symptom is observed on a Cisco 10000 series router with dual PREs when some PPP interfaces are up and some are down after a PRE switchover. In addition, the “interface resets” counter on the problematic interface will increment.

  Workaround: Change the encapsulation to HDLC or try issuing the command **clear ppp interface**.

- CSCsy61006

  Symptoms: Lawful intercept users are appearing in output from **show run**.

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

  Workaround: There is no workaround.

- CSCsy61321

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

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

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

- CSCsy78382

  Symptoms: Sending non-IOS traffic could cause a IOSD crash.

Conditions: The symptom is observed if traffic is non-IOS control packets.

Workaround: There is no workaround.

- CSCsy83266

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

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

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

- CSCsy96407

  Symptoms: Downstream traffic stopped after delete/recover of sub-interface configuration while sessions are up.

  Conditions: Occurred with the following configuration:

  - L2access IP aggregation session
  - ISG as DHCP relay
  - No VPN routing/forwarding (VRF)
  - TAL authentication

  Workaround: There is no workaround.

- CSCsz11384

  Symptoms: The following error is logged:

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

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

  Workaround: There is no workaround.

- CSCsz16580

  Symptoms: Active RPs CPU% spikes by MLD process after reload and longevity tests with 8K VLANs.

  Conditions: This MLD CPU spike is seen right after the bootup when active RP is synching with standby RP and also observed during long duration test with SNMP MIB polling, SBC dynamic calls, and show command load.

  Workaround: During the bootup case, delay the standby RP bringup using EEM or other methods until all the DHCP users addresses are assigned, and SBC signaling pinholes are established.

- CSCsz27104

  Symptoms: Acct-Session-Id attribute received in CoA message is decoded incorrectly.

  Conditions: When session ID is less than 8 hex characters, the decoded value is incorrect.

  Workaround: There is no workaround.

- CSCsz29991

  Symptoms: The following error message is displayed:

  ```
  %OSPF-4-NULL_PREV_LINKAGE with a traceback upon executing "clear ip ospf process"
  ```

  The error will spike the CPU to 100% forever ultimately leading to a Sup/RSP crash. The crash could happen immediately or even after several hours.

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

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

Reloading is the only way to recover if the system has run into the issue already in a non-HA environment, however a switchover may work.

- CSCsz42529

  Symptoms: After reloading the box, active comes up fine, but the standby keeps reloading because of RF client AAA timeout.

  Conditions: This symptom is observed on a Cisco ASR1000 router.

  Workaround: There is no workaround.

- CSCsz43096

  Symptoms: When ACL is enabled with NetFlow, such that packets are sent to the denied IP address then the dropped flow does not have the correct destination key fields.

  Conditions: This symptom is seen when ACL is enabled with NetFlow. This does not affect Cisco IOS Release 12.4T images.

  Workaround: There is no workaround.

- CSCsz61184

  Symptoms: Including a new class that does packet marking on an output service-policy (which also does policing in class-default class) drops packets on the policer in class-default class.

  Conditions: The symptom is observed on a Cisco 10008 router (PRE4-RP) that is running Cisco IOS Release 12.2(33)SB3.

  Workaround: Remove and add again the policer in the class-default.

- CSCsz82587

  Symptoms: MPLS-TE configuration leads to router crash due to online insertion and removal (OIR).

  Conditions: MPLS-TE sessions coming up/down during OIR may lead to router crash.

  Workaround: There is no workaround.

- CSCta08194

  Symptoms: A router may crash.

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

  Workaround: There is no workaround.

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

- CSCta08632

  Symptoms: After supervisor forces switchover several times, a router two hops away has wrong ISIS topology and ISIS routing table.

Conditions:

1. Incremental shortest path first (ISPF) enabled in ISIS.
2. **set-overload-bit** on-startup in ISIS.
3. Supervisor force switchover several times

Workaround: Disable ISPF in ISIS.

- CSCta08772

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

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

  Workaround: There is no workaround.

- CSCta17849

  Symptoms: PXF taps LI datagram, and it taps recursively.

  Conditions: This symptom is observed when DST IP is the same as MD IP and SRCMASK is 0.

  Workaround: Do not use DST IP as same as MD IP.

- CSCta18596

  Symptoms: The following tracebacks and messages appear on the console logs:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61AB0C78 reading 0x22
%ALIGN-3-TRACE: -Traceback= 61AB0C78 623849E8 62384A58 607CCD8C 61372428 613769FC
61376E68 613773C4
```

  In addition, you may see instability of the serial interfaces (i.e.: when an interface is configured, it stays up for a while and then goes down).

  Conditions: The symptoms are observed when upgrading to Cisco IOS Release 12.2(31)SB14 on a Cisco 7200 series router only on the interfaces configured with frame-relay fragmentation configured on the main interface.

  Workaround 1: Use fragmentation in the map-class with FRTS (i.e.: configure “frame-relay traffic-shaping” under the main interface and configure fragmentation under the map-class and apply the map-class to PVC). For example:

```
interface Serial1/0.1/1/4/2:0
  no ip address
  encapsulation frame-relay IETF
          ...
  frame-relay traffic-shaping
  frame-relay lmi-type ansi
  frame-relay intf-type dce
  no clns route-cache
  max-reserved-bandwidth 100
 !
 interface Serial1/0.1/1/4/2:0.101 point-to-point
          ...
  frame-relay interface-dlci 101
   class BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725

 map-class frame-relay BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725
  frame-relay cir 768000
  frame-relay mincir 768000
  no frame-relay adaptive-shaping
  service-policy input BANKOFIRE-IN-S1/0.1/1/4/2:0
  service-policy output BANKOFIRE-OUT-S1/0.1/1/4/2:0
```

```
 frame-relay fragment 600
!
```

Workaround 2: Make sure that the fragmentation size is different in different interfaces (with interface fragmentation).

- CSCta32501

  Symptoms: Device crashes.

  Conditions: This symptom is seen when device is receiving a specially-crafted RADIUS VSA response from the server.

  RADIUS secret is required, and this is a crafted response to a RADIUS request.

  Workaround: There is no workaround.

- CSCta33011

  Symptoms: You may not be able to terminate PPPoE sessions on a Cisco ASR P2. The issue starts after days of normal working operation.

  Conditions: The symptom is observed on a Cisco ASR RP2 configured as an LNS.

  Workaround: There is no workaround.

  Further Problem Description: Except PPP sessions, other functionality works fine. Only PPP is in a stuck state and reload is the only option to recover from this state.

- CSCta34884

  Symptoms: Router crashes due to fluctuating PPP sessions.

  Conditions: This symptom is observed when changing the encapsulation on range PVC from “aal5mux ppp” to “protocol ppp” and removing and reconfiguring the range.

  Workaround: There is no workaround.

- CSCta35152

  Symptoms: With multiple DHCP bindings present in the relay and downstream traffic flowing (100000 pac/sec), if the ARP table is cleared, packets are punted to the RP causing a memory leak.

  Conditions: This issue is seen only with a single PRE setup where the Cisco 10000 router is acting as a DHCP relay.

  Workaround: There is no workaround.

- CSCta46650

  Symptoms: The console gets stuck when the **show arp** command is executed and “esc” is pressed to stop viewing the whole output.

  Conditions: The symptom is observed with 512 ARP sessions on the system and set term len equal to 20.

  Workaround: There is no workaround.

- CSCta59045

  Symptoms: If 32k dual-stack sessions are configured on a PTA device such as a Cisco ASR 1000, the router may crash when the sessions are brought down.

  Conditions: This symptom is observed when both the PPPoE client and the PTA are Cisco ASR 1000 routers. The client crashes when the **test pppoe** command is entered while trying to bring up 16K dual-stack sessions on the PTA device. This symptom is more likely to be observed when the preferred lifetime and valid lifetime of the assigned prefix are configured to be equal. The crash may occur even if the lifetimes are not equal, but it is less likely.

Workaround: Do not configure the valid and preferred lifetimes of the prefix equally. This will decrease the probability of this crash, but does not ensure against it.

- CSCta75687

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

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

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

- CSCta85026

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

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

  % Invalid input detected at '^' marker.

  Router(dhcp-config)#
```

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

  Workaround: There is no workaround.

- CSCta91556

  Symptoms: Packets are getting SSS switched on the LAC towards LNS.

  Conditions: The symptom is observed when bringing up any PPPoE or PPPoA session.

  Workaround: There is no workaround.

- CSCta99162

  Symptoms: When the command **passive-interface default** is entered under router ISIS, the router reloads.

  Conditions: Enter router ISIS configuration mode and enter the **passive-interface default** command. Router reloads.

  Workaround: Configure a passive interface under router ISIS.

- CSCtb15699

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

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

  Workaround: There is no workaround.

- CSCtb38411

  Symptoms: Service policy gets removed in L2TP sessions on LNS.

  Conditions: The symptom is observed when you delete and recreate the policy-map on virtual-template on LNS in a fast configuring fashion (i.e.: copy/paste or via script).

  Workaround: Configure the same commands line by line on console, or delay a bit after removing the policy-map before attaching again.

- CSCtb38975

  Symptoms: Updating the DHCP lease time with a new value has no effect.

  Conditions: This symptom occurs when the renewal process is forced.

  Workaround: There is no workaround.

- CSCtb43293

  Symptoms: ACL functionality may break on a Cisco 10000 series router after redundancy switchover.

  Conditions: This symptom is observed after a redundancy switchover on a PPPoX session with ACL applied.

  Workaround: There is no workaround.

- CSCtb46622

  Symptoms: Memory leaks are seen in a Cisco 10000 series router.

  Conditions: This symptom is observed in a Cisco 10000 router with PPPoX sessions in a scaling environment.

  Workaround: There is no workaround.

- CSCtb55851

  Symptoms: The router crashes pointing to RF code.

  Conditions: The symptom is observed upon issuing the **show redun history** command from the active RP console and at the same time executing **clear redu history** from the VTTY terminal.

  Workaround: These two commands are not supposed to work in parallel. Block the “clear” command if “show” is in progress.

- CSCtb57460

  Symptoms: BGP scanner process is taking a lot of CPU.

  Conditions: The symptom is observed with a five second BGP scanner timer and with a large number of routes. It is seen on a PRE2.

  Workaround: Change to a pre-BGP LMM supported image.

- CSCtb59288

  Symptoms: A router crashes on ATM hw-module reset.

  Conditions: The crash happens when the ATM interface is OIRed.

  Workaround: There is no workaround.

- CSCtb73450

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

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

  Workaround: There is no workaround.

- CSCtb78266

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

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

  Workaround: There is no workaround.

- CSCtc01196

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

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

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

- CSCtc05167

  Symptoms: The mcp_eagle_int image is not booting in Cisco 7200 routers with NPE-G1. The router is hung in the middle of the boot operation.

  Conditions: This issue is observed only with NPE-G1 and I/O card where the I/O card console will be used instead of NPE-G1 console.

  Workaround: There is no workaround. Without I/O card, this issue will not be seen.

- CSCtc20254

  Symptoms: show tb.

  Conditions: This symptom is seen in prepaid scaling scenario.

  Workaround: There is no workaround.

- CSCtc37147

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

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

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

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

- CSCtc40677

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

```
router eigrp 1
  redistribute static metric 10000 100 255 1 1500
  network 10.0.0.0
  no auto-summary
  distribute-list prefix TEST out Virtual-Template1 !
ip route 0.0.0.0 0.0.0.0 Null0
!
ip prefix-list TEST seq 10 permit 0.0.0.0/0 ip prefix-list TEST seq 20 permit
10.0.0.0/8
```

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

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

      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06, Dialer1
```

```
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

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

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

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

- CSCtc51539

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

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

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

  Workaround: Disable BFD.

- CSCtc56918

  Symptoms: Router may crash while unconfiguring QoS 2 level service policy from “frame relay” interface.

  Conditions: Cisco 7200 Series Router Cisco IOS Release 12.2(33)SRE may crash while unconfiguring QoS 2 level service policy from Frame-relay interface and configuring **frame-relay fragment end-to-end** and pinging with large size packet.

  Workaround: There is no workaround.

- CSCtc65224

  Symptoms: A Cisco 10000 series router reloads due to a bus error.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB7.

  Workaround: There is no workaround.

- CSCtc69991

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

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

  Workaround: Use EIGRP as the overlay routing protocol.

- CSCtc78966

  Symptoms: IOSD crash is seen while sending traffic through user-defined IP sessions.

  Conditions: This issue is seen on a Cisco ASR 1000 router with RP2 processor.

  Workaround: There is no workaround.

- CSCtc91553

  Symptoms: High CPU utilization occurs.

  Conditions: Session churn.

  Workaround: The following global configuration has helped in reducing CPU usage:

  no parser command serializer

ip routing protocol purge interface

Further Problem Description: CPU usage will remain high under normal conditions given a constant churn rate of approximately 24 CPS coming up and down.

- CSCtc91560

  Symptoms: High CPU utilization occurs.

  Conditions: The symptom is observed with session churn.

  Workaround: There is no workaround.

  Further Problem Description: CPU usage will remain high under normal conditions given a constant churn rate of approximately 24 CPS, coming up and down.

- CSCtc91594

  Symptoms: High CPU utilization occurs.

  Conditions: The symptom is observed with session churn.

  Workaround: The following global configuration has helped in reducing the CPU:

  no parser command serializer ip routing protocol purge interface

  Further Problem Description: CPU will remain high under normal conditions given a constant churn rate of approximately 24 CPS, coming up and down.

- CSCtd06275

  Symptoms: When issuing the **show policy-map interface brief** command, the system might crash with a bus-error.

  Conditions: The symptom is observed when the system is configured for ISG-services in a scaled ATM-environment.

  Workaround: There is no workaround.

- CSCtd07834

  Symptoms: The mVPN traffic is not forwarded after RPR+ switchover. Router stops sending its loopback prefix as MDT SAFI after RPR+ switchover.

```
WORKING STATE::
UUT#sh bgp ipv4 mdt all
BGP table version is 4, local router ID is 192.168.242.150
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 666:666 (default for vrf mvpn1)
*>i192.168.242.148/32
                    192.168.242.148          0    100      0 ?
*> 192.168.242.150/32
                    0.0.0.0                               0 ?

BROKEN STATE (after RPR+)::
UUT#sh bgp ipv4 mdt all
BGP table version is 12, local router ID is 192.168.242.150
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 666:666 (default for vrf mvpn1)
*>i192.168.242.148/32
                    192.168.242.148          0    100      0 ?
```

  Note that UUT's peering loopback (192.168.242.150) is not imported as local prefix into BGP as MDT SAFI. Because of this we do not advertise it and UUT cannot act as receiver in mVPN.

  Conditions: This symptom is seen in BGP session with MDT address family.

  Workaround: Unconfigure and configure back default MDT of VRF or clear bgp process.

- CSCtd21590

  Symptoms: RP crashes after executing the **no import ipv4 unicast map filter** command.

  Conditions: This symptom occurs when GP import events debugging is on with the **debug ip bgp import updates** command or the **debug ip bgp import event** command

  Workaround: Do not enable the **debug ip bgp import event** command or the **debug ip bgp import update** command.

- CSCtd28348

  Symptoms: On an ESR PRE3 throughput may be reduced down to 80% of expected throughput for high speed VBR-NRT VCs.

  Conditions: The symptom is seen under the following conditions:

  - Seen on VCs with speed more than 240MB.
  - The higher the rate of the PVC the higher the impact (the lower the percentage throughput/expected througput).
  - The lower the MBS the higher the impact (the lower the percentage throughput/ expected throughput).
  - Default MBS seems fine for 300 MB PVCs but may not be for faster VCs.
  - MBS=1 hits the issue for PVCs with speed of 240MB.

  Workaround: Do not set the MBS explicitly.

- CSCtd30544

  Symptoms: Netflow is showing Null in the destination interface even though packets are not getting dropped or blocked.

  Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss** *value* configuration that is applied on the destination interface.

  Workaround: Remove **ip tcp adjust-mss** *value* from the destination interface.

- CSCtd42810

  Symptoms: PPPoEoA sessions are not coming up because some VCs are in inactive state.

  Conditions: This symptom is observed when around 400 PVCs are configured with PPPoEoA sessions.

  Workaround: Save the configuration on the LAC, then reload the LAC.

- CSCtd49742

  Symptoms: Router crashes with SIP-400 non LAG cases.

  Conditions: This symptom is seen when IEDGE is configured.

  Workaround: There is no workaround.

- CSCtd67076

  Symptoms: Standby PRE resets due to parser sync error.

  Conditions: The symptom is seen when a non-existing GigE interface is deleted.

  Workaround: Configure the following:

```
(config-red)# no policy config-sync lbl prc reload
(config-red)# no policy config-sync bulk prc reload
```

- CSCtd74135

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

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

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

- CSCtd75033

  Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

Note The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section "Further Description" of this release note enclosure.

Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372.

Cisco has released a public facing vulnerability alert at the following link:

http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp
      ntp peer 192.168.0.12
```

The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp
      router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE
(fc2)
 Technical Support: http://www.cisco.com/techsupport
 Copyright ) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih

 <output truncated>
```

The following example shows a product that is running Cisco IOS Software Release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
  12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS and NX-OS Software Reference Guide" at the following link:

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note NTP peer authentication is not a workaround and is still a vulnerable configuration.

* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration

ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the multicast group must
```

```
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, while the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic

that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
 match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
 class drop-udp-class
  drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
 service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

- Rate Limiting the traffic to the device.

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded, valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
 match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
 class rate-udp-class
  police 10000 1500 1500 conform-action transmit
         exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
 service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S—Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

- CSCtd97054

  Symptoms: Router will crash with signal 23:

  ```
  %Software-forced reload
  Breakpoint exception, CPU signal 23, PC = 0x40946BA8
  ```

  Conditions: This symptom is seen when device is configured with Multilink PPP (MLPPP).

Workaround: There is no workaround.

Further Problem Description: This bug is related to CSCso78639. Both are required for a full fix.

- CSCtd99802

  Symptoms: There is packet loss due to the BGP session reopening from the peer that has been rejected.

  Conditions: The symptom is observed when a Cisco peer has a BGP session and a non-Cisco peer does not (because of reloading the non-Cisco peer line card or a similar reason). The non-Cisco peer does not send TCP RST properly to close the BGP session on the Cisco peer.

  Workaround: There is no workaround.

- CSCte04701

  Symptoms: PRE2 crashes.

  Conditions: The symptom is observed on a PRE2 with Netflow configured.

  Workaround: There is no workaround.

- CSCte07401

  Symptoms: Normal mode GD fails with tracebacks when you execute the **show memory debug leak chunks** command.

  Conditions: This symptom is seen when you check for memory leaks after clearing an L2TP session.

  Workaround: Wait for all sessions to tear down and then check for leaks.

- CSCte10706

  Symptoms: When you configure FRF.12 “frame-relay fragment 512 end-to-end” on the serial interface, the router crashes.

  Conditions: The symptom is observed when you configure FRF.12 “frame-relay fragment 512 end-to-end” on a CJ-PA.

  Workaround: There is no workaround.

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS? Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

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

- CSCte38945

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

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

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

- CSCte42714

  Symptoms: A Cisco 7304 router crashes continuously after a reload.

  Conditions: The symptom is observed when the router is configured with an mGRE tunnel. Once the tunnel is configured, if the router is reloaded it starts crashing continuously.

  Workaround: Use point-to-point GRE tunnels.

- CSCte47406

  Symptoms: Cisco 10000 PXF crashes with PXF DMA Error - Small Packet Handle Creating a Large Descriptor.

  Conditions: This symptom occurs when a padded tunneled (unicast tunnel) packet is received. The PXF crashes. This symptom is observed on a Cisco 10000 router that is running Cisco IOS Release 12.2(31)SB17.

  Workaround: There is no workaround.

- CSCte48656

  Symptoms: The router crashes at “Illegal access to a low address”.

  Conditions: The symptom is observed while stopping the SSS handling timer. This condition is triggered by an ISG PBHK configuration and when existing translations are inactive.

  Workaround: There is no workaround.

- CSCte49283

  Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

  Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- CSCte52369

  Symptoms: On a Cisco ASR1000 router, the RADIUS will send a NACK for the First COA request message, and Radius Authentication will fail.

  Conditions: This symptom is observed when the RADIUS receives “ACCESS-ACCEPT” with “Unsupported Vendor” attribute.

  Workaround: Send the COA request message again.

- CSCte54129

  Symptoms: Backing out partial fix of CSCte54129 on Cisco IOS Release 12.2(33) SB.

  Conditions: This symptom is seen on Cisco IOS Release 12.2(33)SB8.

  Workaround: There is no workaround.

- CSCte57149

  Symptoms: Router may crash with an address error in the BGP function on a dual RP system that is running Cisco IOS Release 12.2(33)SB8.

Conditions: The symptom is observed when the router is configured for BGP, dual RP system, BGP Multipath inside an “imported” IPv4 VRF and experiences link or route flaps.

Workaround: There is no workaround.

- CSCte57737

  Symptoms: A Cisco 10000 router might crash when provisioning ATM PVCs.

  Conditions: This symptom is observed when the device is running Cisco IOS Release 12.2(33)SB8. Range PVC and DBS are configured.

  Workaround: There is no workaround.

- CSCte58686

  Symptoms: Link flaps after an upgrade to Cisco IOS Release 12.2(33)SRD3.

  Conditions: The symptom is observed following an upgrade from Cisco IOS Release 12.2(33)SRB5 to SRD3.

  Workaround: There is no workaround.

- CSCte58749

  Symptoms: Some interfaces start flapping upon upgrading to Cisco IOS Release 12.2(33)SRD3.

  Conditions: This is a corner case condition. The interface flaps occur under following conditions:

  1. The peer connected on the other side of the interface sends a CODEREJ for a valid ECHOREP sent by a Cisco router.
  2. On receiving CODEREJ for ECHOREP, the router terminates the PPP session. The PPP sessions restart, and the interface flaps.

  Workaround: Disable keep-alive on the misbehaving peer router.

- CSCte63156

  Symptoms: Router hangs and crashes when a DHCP pool configured with “origin aaa subnet” is removed.

  Conditions: The symptom is observed when pool is configured with “origin aaa subnet ...” and without unconfiguring this command, the pool is deleted with the **no ip dhcp pool** command. Also missing is “aaa accounting” with “default method-list” from global configuration.

  Workaround: Globally configure “aaa accounting” with “default method-list” (“aaa accounting network default”).

- CSCte66219

  Symptoms: The following symptoms are observed:

  1. When copying files from the active to standby (or vice versa), you may see an error:

     ```
     %Error writing stby-disk0: (TF I/O failed in data-in phase)
     ```

  2. A failed MD5 checksum when reading a file off the disk. This may or may not indicate a previous failure that went unnoticed. (Note: not all disk errors and not all MD5 checksum errors are due to this problem.)
  3. The disappearance of Smart Modular 128MB PCMCIA cards, typically on the standby PRE.

  Conditions: The issue may be seen with Cisco IOS Release 12.2(33)SB. In particular, this card is susceptible: STI 7.4.0 Compact Flash and PCMCIA Flash cards. Other cards may or may not have the same issue, but empirical data indicates that other cards are at least somewhat less susceptible.

Workaround 1: Once a file is successfully copied to the disk and the MD5 checksum matches the file, that file is fine and not subject to corruption. Cards that are not being written do not spontaneously become damaged. That is, once the file is on the flash disk, it will not become defective. Only cards with actual errors should be RMAed. There is no need to preemptively or proactively replace flash cards.

Workaround 2: The disappearance of the Smart Modular 128MB PCMCIA cards can be resolved by the physical removal and re-insertion of the card or by reloading the PRE.

Further Problem Description: There was a recent change in the Cisco IOS DOS compatible file system. That change resulted in a higher performance file system. But there is a condition which has been seen on at least one variant of flash card that can lead to disk errors and file system damage. This condition arises from a gray area of the ATA specification and can be fixed in software.

- CSCte68994

  Symptoms: After switchover, new active takes a long time to become active.

  Conditions: This symptom is seen when there is a session and a service profile corresponding to it. The profile has been changed on radius and again downloaded for the session.

  Workaround: Avoid changing the service profile before switchover.

- CSCte74444

  Symptoms: Packets that are switched using PBR on the Cisco 10000 platform are dropped unexpectedly.

  Conditions: This symptom is observed when PBR configuration is modified.

  Workaround: There is no workaround.

  Further problem description: The **show pxf cpu pbr action** command shows NULL_ROUTE instead of SET_ROUTE.

- CSCte75548

  Symptoms: ATM bandwidth is lost when configuring the atm pvp.

  Conditions: ATM bandwidth is lost when configuring the atm pvp with out-of- range peak rate value. The loss of bandwidth is cumulative. For example, the same steps are performed twice. The bandwidth lost is double.

  Workaround: There is no workaround.

- CSCte75725

  Symptoms: The following messages will be blasted on the console:

  Possibly multiple users are trying to access the pvc simultaneously.

  Conditions: There are no specific conditions.

  Workaround: There is no workaround.

- CSCte77398

  Symptoms: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCte78165

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

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

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

- CSCte82549

  Symptoms: Router crashes while doing an OIR.

  Conditions: The symptom is observed while doing a OIR with 4096 bundles (single member link).

  Workaround: There is no workaround.

- CSCte85961

  Symptoms: The router crashes while doing a **shut** command followed by the **no shut** command to the main interface.

  Conditions: The issue is seen with scale configuration and giving the **shut** command followed by the **no shut** command in the main ATM interface.

  Workaround: There is no workaround.

- CSCte92581

  Symptoms: A VRF becomes stuck during deletion in a rear condition (not something that is seen every time).

  Conditions: This symptom is observed when the **no ip vrf** command is entered.

  Workaround: There is no workaround.

  Further Problem Description: The stuck VRF cannot be reused.

- CSCte92623

  Symptoms: The service-policy is not parsed and inserted in the multilink interface configurations on the primary and secondary device.

  Conditions: This symptom is observed after doing a hw-module subslot x/x reset on the primary console. The service-policy policy_1_out will not be parsed and inserted in the multilink interface 1 configurations on the primary and secondary.

  Workaround: There is no workaround.

- CSCte92659

  Symptoms: The router loses some memory due to flow id.

  Conditions: The symptom is observed with a 32k session scaling scenario and with the PPP session flapping when accounting associated with flow id is configured.

  Workaround: There is no workaround.

- CSCte95107

  Symptoms: The **sh ip subscriber** command is interpreted as ambiguous command. Also, some subcommands are displayed twice.

  Conditions: This symptom is reproducible on HA platforms and works on non-HA platforms.

  Workaround: There is no workaround.

- CSCte95396

  Symptoms: A subscriber cannot enable the SSS session due to DPM not finding the binding in the DPM table although the DHCP binding exists as shown by performing the **show ip dhcp server binding** command.

  Debug sss policy event/err would show “SG-DPM: DHCP Binding does not exist to query session”.

  Conditions:

  - Subscriber has dhcp binding when doing “show ip binding ...” note: also check the vrf (if any).
  - Subscriber has no entry in the dpm policy.
  - Session trigger needs to be l2-connect dhcp.

  Workarounds:

  - If this is a “low lease time and relay dhcp case”, make sure subscriber does not send a DHCP packet: waiting for the DHCP binding to disappear (i.e., expire), re-enable the user’s dhcp forwarding path.
  - If this is a “dhcp server” case, clear dhcp binding on the ISG.
  - Reload the router

- CSCte97947

  Symptoms: If a service policy is applied under the virtual circuit of the ATM interface, and if a **shut** followed by a **no shut** is issued, a Cisco 10000 series router may reload generating RP and PXF crashinfo.

  Conditions: The symptom is observed because of partial configuration. When moving ATM PVC out of multilink, if “ppp multilink group” is removed only from PVC and not from virtual-template then you hit this issue. This issue is specific to PRE2 and is not applicable to PRE3 and PRE4.

  Workaround: Remove multilink-related configurations from both PVC and virtual-template.

- CSCte98052

  Symptoms: Shaping values may result in stuck MQC queues during times of heavy traffic. The fail signature will present as a unidirectional transmit problem and the command **show policy-map interface** may report:

  ```
  Router#sh policy-map int a4/0.16 | i no-buffer drops
   (queue depth/total drops/no-buffer drops) 195/44432/0
   (queue depth/total drops/no-buffer drops) 0/15036/0
   (queue depth/total drops/no-buffer drops) 64/14962/0
   (queue depth/total drops/no-buffer drops) 64/29470/0 (shows all packets
   dropped)
  ```

  Conditions: The symptom is observed on a Cisco 7304/NPE-G100/PA-CC/PA-A3-T3 that is running Cisco IOS Release 12.2(33)SB7 and deploying a scaled PVC configuration (600+) with relatively low ATM traffic.

  Workaround 1: Remove “service-policy output” from PVC.

  This is a preventative workaround but results in loss of functionality.

  Workaround 2: Perform a **shut** followed by a **no shut** on the affected subinterface.

  This is a recovery workaround which requires manual intervention.

- CSCtf00132

  Symptoms: A Cisco 7200 series router crashes when there are unauthenticated sessions in a multichassis SGBP environment.

Conditions: The symptom is observed when multiple unauthenticated sessions in a multichassis multilink PPP SGBP environment are dialed from the same client on multiple home gateways as part of the same session.

Workaround: There is no workaround.

- CSCtf00234

  Symptoms: With Cisco IOS Release 12.2(33)SB8, PPPoE users are rejected, with the following error message:

  ```
  PPPOE: Max Inner Vlan session count(1) exceeded on TenGigabitEthernet5/0/0.xxx
  ```

  Conditions: The symptom is likely to be seen when you encounter an error during PADR processing which can be triggered due to low memory on the router or a wrong PADR from peer. In this case, some sessions are not freed properly leading to ghost sessions, so the new session are rejected if BBA group is configured with some sort of session limit (for example "sessions per-vlan limit 65530 inner 1").

  Workaround: There is no workaround.

- CSCtf05827

  Symptoms: A Cisco 10000 router crashes with chunk error.

  Conditions: This symptom occurs due to memory corruption longevity and stress test.

  Workaround: There is no workaround.

- CSCtf06143

  Symptoms: A Cisco 10000 series router crashes with memory corruption.

  Conditions: This symptom occurs on WAVL tree corruption when the box is scaled and stressed with ISG.

  Workaround: There is no workaround.

- CSCtf06716

  Symptoms: A Cisco 10000 series router may crash when the sessions are cleared using the **clear subscriber session all** command.

  Conditions: The symptom is observed when the timed policy expire and sessions get disconnected and L4R is applied.

  Workaround: There is no workaround.

- CSCtf07513

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

  Conditions:

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

  Workaround: Do not remove loopback interface before stopping traffic.

- CSCtf12072

  Symptoms: The expected behavior after a failed authorization action does not get applied onto the session when authorization is based on option 82 information. The FSOL does not contain option 82 information.

Conditions: The symptom is observed when the ISG policy is to provide authorization based on the subscriber's option 82 information, such as remote-id and/or circuit-id. However, the option 82 is missing in the DHCPDISCOVER packet. The subscriber session comes up in unauthenticate as expected, but the expected actions (i.e.: applying L4R service) do not get applied onto the session.

Workaround: There is no workaround.

- CSCtf15982

  Symptoms: A router crashes.

  Conditions: This symptom is seen when clearing dangling session in data plane, which corrupts memory and leads to router crash.

  Workaround: Do not try to clear dangling session from CLI and disable auto clearing the dangling session by issuing the **ip subscriber timer clear-dangling 0** command.

- CSCtf19459

  Symptoms: Downstream traffic (to the subscriber) is not forwarded. Only the upstream counters are increasing.

  Conditions: This symptom is seen with the following conditions:

  -In the **show sss sesssion detail** command -In PXF output

  Workaround: Clear the SSS session affected.

- CSCtf19902

  Symptoms: For some clients, relaying of DHCP Discover packets is not triggered following session authentication. For a single ISG, this results in the client never receiving an address. For redundant ISGs, where one is affected by this issue and one is not, this results in the affected ISG never clearing the session, even though it sees the request from the client accepting the other ISG's offer.

  Conditions: This symptom is seen when service-start event under control- policy is configured to unapply all possible services (including the desired service), then apply the new service.

  Workaround: Change the service-start event configuration to only unapply other services, then apply the new service. However, this will require a separate event configuration for each service type.

- CSCtf26061

  Symptoms: Packets sent through PXF are not matching the prepaid service but the default service.

  Conditions: The symptom is observed with packets sent through PXF.

  Workaround: Reload the router.

- CSCtf27303

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

  Conditions: The symptom is observed under the following conditions:

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

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

  Workaround: There is no workaround.

- CSCtf27324

  Symptoms: A ping from a CPE (which is doing PPP to the IP address of the LNS router that terminates that PPP call) fails. PPP has been opened and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

  Conditions: The symptom is observed only when there is a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition, the physical connectivity between the LAC and the LNS is PPP multilink.

  Workaround: Disable CEF on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink, the ping works fine.

  Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.

- CSCtf29908

  Symptoms: A Cisco 10000 series router crashes due to memory corruption. The good blocks before the corrupted ones show allocating process as “C10k ISG keepalives”.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running with ISG sessions and ARP/ICMP keepalives turned on.

  Workaround: There is no workaround.

- CSCtf32348

  Symptoms: Router crashes.

  Conditions: The symptom is observed when you apply “ip security dedicated topsecret sci nsa” on any of the interfaces.

  Workaround: Remove “ip security dedicated topsecret sci nsa” configuration.

- CSCtf38953

  Symptoms: CPU hog is seen at decode_add_uiddb while decoding Access-Challenge packet received.

  Conditions: This symptom is seen when access-request is sent for proxied session and state/class attribute is received in Access-Challenge.

  Workaround: There is no workaround.

- CSCtf44529

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

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

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

- CSCtf46619

  Symptoms: You will not be able to switch through LNS when using L2TP MP-BGP. The ping to the local address fails.

  Conditions: The symptom is observed when using:

  - L2TP MP-BGP.
  - A Cisco 10000 series router.
  - PPP multilink.

Workaround: Use the **compress stac** command (with performance impact on the Cisco 10000 processor).

- CSCtf52083

  Symptoms: When an ISG system with DHCP subscribers get reloaded, some sessions may not restart when DHCP renew messages are received by the ISG router.

  Conditions: The symptom is observed on a system reload/restart.

  Workaround: There is no workaround.

- CSCtf53537

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

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

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

- CSCtf54547

  Symptoms: After resetting the Standby ESR-PRE2, the card continuously stays in a boot cycle.

  Conditions: The symptom is observed when there is “loopback remote” configured under a serial interface. It is seen only with an 8E3DS3 card.

  Workaround: Remove the “loopback remote” configuration.

- CSCtf64224

  Symptoms: While doing SOFTOIR, router crashes in 4xOC3 POS SPA and 1xOC12 POS SPA.

  Conditions: This symptom occurs while doing SOFTOIR. The router crashes with APS enabled in 4xOC3 POS SPA and 1xOC12 POS SPA.

  Workaround: There is no workaround.

- CSCtf64375

  Symptoms: Memory corruption and router crash are seen with overlapping mac- addresses.

  Conditions: This symptom is seen when bringing up Cisco 10000 router sessions with overlapping mac-addresses at 40CPS each set of 10 sessions having the same mac-address.

  Workaround: There is no workaround.

- CSCtf71636

  Symptoms: The router crashes while configuring/unconfiguring random detect.

  Conditions: The symptom is observed with Cisco IOS interim Release 12.2 (31.17.01)SB. The policy given below has to be applied on FR DLCI interface for this issue to occur:

```
Policy Map output-policy
     Class prec2
       bandwidth 460 (kbps)
     Class prec4
       bandwidth 460 (kbps)
```

  Next, the following command sequence causes the router to crash:

```
config terminal
     policy-map output-policy
     class class-default
     fair-queue
     random-detect
     no fair-queue
     random-detect
     no random-detect
```

random-detect

Workaround: There is no workaround.

- CSCtf75053

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

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

  Workaround: There is no workaround.

- CSCtf76623

  Symptoms: A few memory leaks are seen.

  Conditions: The symptom is observed when configuring commands such as:

  policy-map type service class-map type traffic match-any

  Workaround: There is no workaround.

- CSCtf82883

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

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

  Workaround: There is no workaround.

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

- CSCtf84237

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

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

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

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

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

- CSCtf93947

  Symptoms: A Cisco 10000 ESR with PRE3 may experience CPU hog errors and crashes.

  Conditions: The symptom is observed when Netflow is configured and with Cisco IOS Release 12.2(33)SB7.

  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.

- CSCtf98704

  Symptoms: Multiple PXF crashes after a microcode crash emulation.

  Conditions: This symptom is seen with scaled MLP sessions with an MPLS core between LAC and LNS.

  Workaround: There is no workaround.

- CSCtg07149

  Symptoms: OC3POS line card may reset during ISSU upgrade even when there is no change in the major number.

  Conditions: This symptom may occur during ISSU upgrade even though there is no change with the major number of line card images.

  Workaround: There is no workaround. However, the line card comes up fine after the reset.

- CSCtg07201

  Symptoms: DHCP sessions with FSOL that do not contain option 82 information may get stuck in "Attempting" state during authorization.

  Conditions: The symptom is observed when the keepalive feature is applied prior to the authorization action, i.e:

```
policy-map type control DHCP-KA
  class type control always event session-start
   5 service-policy type service name KA-SERVICE
   10 authorize aaa list QOS_AUTHEN_LST password <password> identifier circuit-id
```

  Workaround: While removing the action "5 service-policy type service name KA-SERVICE" in the above example would avoid this problem, keepalive feature is highly recommended when provisioning IP sessions with ISG, or else there is no way for the ISG router to detect and clean-up inactive subscriber sessions.

- CSCtg18746

  Symptoms: Some image builds are broken.

  Conditions: This symptom is seen in images that do not include SSS policy subsystem.

  Workaround: There is no workaround.

- CSCtg21716

  Symptoms: PXF crash is seen when DHCP sessions with unclassified IP come up at the same time.

  Conditions: This symptom is seen when DHCP sessions with unclassified IP come up at the same time.

  Workaround: Do not bring up l2-connected static and DHCP sessions at the same time with the same mac-address on the same interface.

- CSCtg25327

  Symptoms: CPU utilization goes high when a particular client tries to pump broadcast traffic.

  Conditions: The issue is seen in Cisco 10000 router when configured for PPPoE DSL aggregator.

  Workaround: There is no workaround.

- CSCtg26324

  Symptoms: Router acting as a DHCP relay crashes with a CPUHOG.

  Conditions: The symptom is observed when there are several thousand DHCP bindings at the time of issuing the **no service dhcp** command.

Workaround: Remove the DHCP bindings on the router before issuing **no service dhcp**.

- CSCtg38104

  Symptoms: Router crashes at c10k_iedge_print_vcci_policy_detail().

  Conditions: The symptom is observed when the **show pxf cpu isg vcci detail** *vcci num* is given and from the other VTY the session is cleared. The crash happens when the automore is disabled to print the command details.

  Workaround: Do not clear the session while printing the **show** command.

- CSCtg60088

  Symptoms: Withdrawals are not generated on deletion or addition of a VRF.

  Conditions: This symptom is due to incorrect update group being assigned to the newly configured CE.

  Workaround: There is no workaround

- CSCtg62555

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

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

 %Software-forced reload
```

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

  Workaround: There is no workaround.

- CSCtg62787

  Symptoms: Packets with non-default MTU are not forwarded by port-channel with GEC.

  Conditions: The symptom is observed when port-channel has non-default MTU.

  Workaround: Use the default MTU of 1500 bytes.

- CSCtg71660

  Symptoms: Router crashes at saaPathHourlyStatsStart.

  Conditions: The symptom is observed while enabling **default paths-of-statistics-kept**.

  Workaround: There is no workaround.

- CSCtg79881

  Symptoms: Subscriber cannot enable the SSS session due to DPM not finding the binding in the table although the binding exist when performing the **show ip dhcp server binding...** command. If you use **debug sss policy event/err** the following message shows:

```
SG-DPM: DHCP Binding does not exist to query session
```

Conditions: The symptom is observed under the following conditions:

- Subscriber has DHCP binding when doing **show ip dhcp server binding...** (note: also check the VRF, if any).
- Subscriber has no entry in the DPM policy.
- Session trigger needs to be L2-connect DHCP.

Workaround 1: If “low lease time and relay dhcp case”:

- Make sure subscriber does not send a DHCP packet.
- Wait for the binding to disappear.
- Re-enable the user DHCP forwarding.

Workaround 2: If “dhcp server case”, then clear DHCP binding.

Workaround 3: Reload the router.

- CSCtg89472

  Symptoms: High CPU usage (99-100%) is observed on the standby.

  Conditions: The symptom is observed on a Cisco 10000 series router loaded with scaled L2VPN configurations of all circuit types.

  Workaround: There is no workaround.

- CSCtg91201

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

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

  Workaround: There is no workaround.

- CSCtg94250

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

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

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

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

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

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

- CSCtg96357

  Symptoms: Align tracebacks seen on an LNS.

  Conditions: The symptom is observed on an LNS while bringing up one MLP bundle.

  Workaround: There is no workaround.

- CSCth05778

  Symptoms: Router is showing memory leaks.

  Conditions: The symptom is observed when the remote end is sending LCP conf_req messages to a Cisco 10000 series router a lot frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

  Workaround: Shut down the PPP link that is flapping.

- CSCth08505

  Symptoms: PPPoE sessions may not sync to the standby-RP.

  Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

  Workaround: Reloading the standby-RP may resolve this issue.

- CSCth11029

  Symptoms: After switchover, AAA server load balancing is not happening as expected.

  Conditions: This symptom is seen when the **load-balance method least- outstanding** command is configured under a server group. Load balancing for that server group is impacted after switchover.

  Workaround: There is no workaround.

- CSCth13105

  Symptoms: Traceback is seen at policymgr_handle_get_context.

  Conditions: The symptom is observed while creating a session with many policies attached.

  Workaround: There is no workaround.

- CSCth13689

  Symptoms: Spurious memory access is made.

  Conditions: The symptom is observed when using the **show access list compiled** command, when the router is configured with **access-list compiled.**

  Workaround: There is no workaround.

- CSCth18432

  Symptoms: Cannot configure more than eight source in port bundle.

  Conditions: The symptom is observed when configuring port bundles with a higher length value in scale condition.

  Workaround: Appropriately lower the port bundle length in order to scale a greater number of sessions.

- CSCth18982

  Symptoms: BGP sessions flap continuously in a multi-session configuration.

  Conditions: This symptom is observed when the same peer under the same address family is configured under different topologies (MTR with GR-enabled setup) with multiple topoid.

  Workaround: The sessions do not flap if topologies use the same topo-id (tid) for the peers active under different topologies or when GR is not enabled.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

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

  Workaround: There is no workaround.

- CSCth40241

  Symptoms: A Cisco 10000 active standby crashes.

  Conditions: The symptom is observed when bringing up IP subnet subscribers.

  Workaround: There is no workaround.

- CSCth42594

  Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

  Conditions: The symptom is observed with the following conditions:

  1. When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
  2. Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499”).

  Workaround: There is no workaround.

- CSCth45731

  Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby#show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- ------------------
--
0xB400008A   LCP+ CHAP+ IPV6CP+    Undefine 0.0.0.0
```

  Peer address is 0 and interface will show the PPP handle instead of the virtual interface of PPP.

  Conditions: This symptom is seen when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

  Workaround: There is no workaround.

- CSCth58910

  Symptoms: In the scenario that the AToM dataplane takes on a different path from that of the control plane, the pseudowire does not recover when the dataplane recovers from its failure.

  Conditions: This symptom occurs in the following sequence of events:

  - control plane path goes down
  - dataplane path goes down
  - control plane path comes back up
  - dataplane path comes back up.

  Workaround: Perform the **shut** command followed by the **no shut** command on the AC interface.

- CSCth59593

  Symptoms: Spurious memory access is seen.

  Conditions: The symptom is observed when issuing the command **show pxf cpu isg ip-session mtrie** *no*.

  Workaround: There is no workaround.

- CSCth64721

  Symptoms: PXF crash seen on Cisco 10000 series router.

Conditions: The symptom is observed on a Cisco 10000 series router with MLP over LNS bundle upon sending bi-directional ping traffic.

Workaround: There is no workaround.

- CSCth66385

  Symptoms: L4R will not work.

  Conditions: This symptom occurs when bringing up sessions.

  Workaround: There is no workaround.

- CSCth69525

  Symptoms: Multicast traffic is not forwarded towards the CE router on the ATM interfaces.

  Conditions: The symptom is observed with AAL5MUX which shows that there is an active stream towards the CE, but the CE is not receiving this stream. With AAL5SNAP encapsulation, we cannot see any active stream.

  Workaround: There is no workaround.

- CSCth71095

  Symptoms: DHCP binding table is not completely synced to standby RP.

  Conditions: This symptom occurs when box is acting as DHCP Relay and ISG is configured.

  Workaround: Use unnumbered multiservice interface instead of numbered one.

- CSCth74869

  Symptoms: A Cisco 10000 router configured with Parallel Express Forwarding (PXF) fails when one of the redundant link flaps. This symptom is related to the outgoing interface selected by CEF.

  Conditions: This symptom is observed on the Cisco 10K with PXF and CEF.

  Workaround: Clear the vrf routing table for the particular VRF that is affected so that the router selects another interface to use for traffic.

- CSCth87357

  Symptoms: A Cisco 10000 router fails to forward priority queueing traffic (dscp = ef) when interleaving is enabled on the CE connected to the router.

  Conditions: This symptom is observed only when “ppp multilink interleave” is enabled on the CE connected to the router.

  Workaround: There is no workaround, other than removing the command on the CE.

  Further Problem Description: No PQ traffic passes from the local CE to the remote CE, but the same PQ traffic between the local PE and the local CE is forwarded. This symptom applies only to PQ traffic and does not affect normal pings.

- CSCth90547

  Symptoms: The critical chunk allocator is”IM Event small”, which is holding up 4 times the amount held by other major components.

  Conditions: This symptom occurs when remote end is sending LCP conf_req messages at Cisco 10000 lot frequently (1 per 4 msec) than normal scenario (1 per 2 seconds).

  Workaround: Shut down the ppp link that is flapping.

- CSCth92820

  Symptoms: Some serial interfaces are not coming up after performing shut/no shut in fr_scaling.

  Conditions: This symptom is observed with frame relay scaling in a channelized card.

Workaround: Performing a shut/no shut on the hardware module will bring up the interfaces.

- CSCth97341

  Symptoms: L4R is not working properly.

  Conditions: This symptom is observed after a microcode reload.

  Workaround: There is no workaround.

- CSCth99786

  Symptoms: A Cisco ASR1000 acting as an ISG crashes.

  Conditions: This symptom is observed when subscriber policy debugging is enabled; for example:

  ```
  ASR1006-2#debug subscriber policy all SSS policy all debugs debugging is on
  ASR1006-2#show debug SSS: SSS policy all debugs debugging is on
  ```

  Workaround: Disable subscriber policy debugging.

- 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.

- CSCti04678

  Symptoms: A Cisco router crashes with redzone corruption.

  Conditions: This symptom is observed when a router is configured for any subscribers and someone tries to execute some of the show CLI while clearing the sessions.

  Workaround: There is no workaround.

- CSCti04754

  Symptoms: PPPoE sessions are stuck at attemping state forever.

  Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attemping state.

  Workaround: Clear attemping state sessions by the **clear** command from box.

- CSCti18397

  Symptoms: Active PRE is crashed by the standby PRE after it did not receive the keepalives.

  Conditions: The issue can be caused by the **sh mem free** command with bfd configured on the box. BFD has revealed the loop-holes in the **sh mem free** command where under certain stress conditions the **sh mem free** command would end up racing for a block with other processes in the system and would eventually trigger this crash.

  Workaround: Do not execute the **sh mem free** command.

- CSCti25117

  Symptoms: With NAT and PXF enabled, packets that are sent with a valid checksum of 0x0000 have an invalid checksum after NAT translation has taken place.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SB7 and later releases.

  Workaround: Disable PXF or downgrade to prior releases of Cisco IOS 12.2(33) SB7.

- CSCti26540

  Symptoms: A memory leak in both SSS Manager and AAA Attribute list can be created when multiple services are downloaded and one of the services fails.

  Conditions: This symptom is observed when a failure in the finishing application of all services leads to a memory leak in the cleanup code.

  Workaround: Proper service profiles should avoid the memory leak.

- CSCti32940

  Symptoms: When fragmented packets of two fragments are received, and if the packet is destined to the router, it will be dropped if it comes on a port- channel interface.

  Conditions: This symptom is seen with port-channel configurations.

  Workaround: Use standalone interfaces instead of port-channel or change the path MTU such that the packets are coming in three fragments instead of two.

- 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.

- 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.

- CSCti81137

  Symptoms: Port-channel interfaces are flapping.

  Conditions: This symptom is observed with a single member link.

  Workaround: There is no workaround.

- CSCti85402

  Symptoms: Cisco 10000 VRF transfer will fail for IP DHCP sessions.

  Conditions: This symptom occurs after RP switchover.

  Workaround: There is no workaround.

- CSCtj47255

  Symptoms: Log messages from ACL for ICMP packets incorrectly show type/code as (0/0):

  ```
  %SEC-6-IPACCESSLOGDP: list test denied icmp 10.1.1.1 -> 10.2.2.2 (0/0), 1 packet
  ```

  Conditions: This symptom is observed on a Cisco 7300 router that has interface ACL configured to match ICMP packets with log option.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB8a

Cisco IOS Release 12.2(33)SB8a is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB8a but may be open in previous Cisco IOS releases.

- CSCsz17080

  Symptoms: There are several symptoms:

  1. Copying files from the active to standby or vice versa. The error could be:

     ```
     "%Error writing stby-disk0: (TF I/O failed in data-in phase)".
     ```

  2. A failed MD5 checksum when reading a file off the disk. This may or may not indicate a previous failure that went unnoticed.

     Not all disk errors and not all MD5 checksum errors are due to this problem!

  3. The disappearance of Smart Modular 128MB PCMCIA cards, typically on the standby PRE.

  Conditions: There was a recent change in the Cisco IOS DOS compatible file system. That change resulted in a higher performance file system. But, there is a condition which has been seen on at least one variant of flash card that can lead to disk errors and file system damage. This condition arises from a gray area of the ATA specification and can be fixed in software.

  The issue is possible with Cisco IOS Release 12.2(33)SB.

  This issue is not present in Cisco IOS Release 12.2(31)SB.

  In particular, this card is susceptible: STI 7.4.0 Compact Flash and PCMCIA Flash cards.

  Other cards may or may not have the same issue, but empirical data indicates that other cards are at least somewhat less susceptible.

  Workaround: Once a file is successfully copied to the disk and the MD5 checksum matches the file, that file is fine and not subject to corruption.

  Cards that are not being written do not spontaneously become damaged. That is, once the file is on the flash disk, it will not all of a sudden become defective.

  There will be a software fix to this issue.

  Only cards with actual errors should be RMAed. There is no need to preemptively or proactively replace flash cards.

  The disappearance of the Smart Modular 128MB PCMCIA cards can be resolved by physical removal and re-insertion of the card or by reloading the PRE. The same software fix also resolves this issue (i.e. the cards will no longer disappear).

- CSCtd81849

  Symptoms: The following system error message is displayed:

  ```
  %ATA-6-ATA_STATUS_TIMEOUT: Timeout occurred while querying the status of ATA device.
  ```

  Note This error message could also be indicative of other failure conditions present in the operation of the flash card. Therefore, it should not be assumed that the presence of these symptoms is explicitly due to this caveat.

  Conditions: This symptom is observed on any file system operation on a flash card.

Workaround: When the error message is generated, the system resets the flash card and retries the ATA protocol command. If the second attempt succeeds, then the file system operation in progress will continue. If the second attempt fails, then the operation will be halted and the user will be informed of the failure.

In most cases, the file system operation will succeed and work around the issue without requiring any operator intervention.

If the file system operation fails, there may be other issues present and it should not be assumed that this caveat is the root cause.

Further Problem Description: The logic missing in the ATA Protocol implementation may cause ATA Protocol failures while accessing PCMCIA or Compact Flash cards.

Resolved Caveats—Cisco IOS Release 12.2(33)SB8

Cisco IOS Release 12.2(33)SB8 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB8 but may be open in previous Cisco IOS releases.

- CSCsc91697

  Symptoms: DBS-applied values do not get dynamically synchronized to the Standby.

  Conditions: The symptom is observed with DBS-applied values (such as PCR, SCR, and MBS).

  Workaround: There is no workaround.

- CSCse66643

  Symptoms: The following error may be seen on a router:

  ```
  %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "IP Input"
  ```

  Conditions: The symptom occurs when using the add-route option on NAT translations and then redistributing these routes into a dynamic routing protocol, such as EIGRP.

  Workaround: There is no workaround.

  Further Problem Description: These errors do not have any observable impact on the router.

- CSCsl33908

  Symptoms: The image name displayed in **show version** will be truncated to 64 characters if the image name is more than that.

  Conditions: It occurs in High Availability (HA) setup.

  Workaround: There is no workaround.

- CSCsl66427

  Symptoms: Shortly after replacing FlexWAN, SNMP queue starts to fill and SNMP queue full error message is printed:

  ```
  %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
  ```

  Conditions: Occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRD1.

  Workaround: Apply following view:

  ```
  Snmp-server view Flash iso included
  snmp-server view Flash ciscoFlashMIB exclude
  snmp-server view Flash ciscoFlashDevice exclude
  snmp-server view Flash ciscoFlashPartitions exclude
  ```

```
snmp-server view Flash ciscoFlashPartitionTable exclude
snmp-server view Flash ciscoFlashPartitionEntry exclude
snmp-server community name view Flash RW
```

If this is not enough to get rid of SNMP queue full, reload the router so that the view applies at the router bootup.

- CSCsm45254

  Symptoms: One or more OBFL processes can result in an SPA card becoming non-responsive. CPU utilization shows as being high (greater than 90%).

  Conditions: The card experiencing the problem must support OBFL and the issue can happen only on a device supporting OBFL. The problem can be triggered if a card reset happens while data is being written onto the OBFL storage device. It happens in a very rare condition where a partial write results in a sector loop in the filesystem layout of the device.

  Workaround: Try disabling OBFL using the **no hw-module module logging onboard** command and reloading the card experiencing high CPU.

  Further Problem Description: A bug in the wear-leveling code of OBFL NOR flash filesystem causes this corner case. When a card gets reset while the last data sector of any file stored in the flash is being replaced with a new one, it could result in a loop in the chain of data sectors related to that particular file. On the next bootup, OBFL filesystem code fails to identify this loop in the data sector chain resulting in this infinite loop.

- CSCso07419

  Symptoms: Chunk memory gets leaked.

  Conditions: The symptom is observed with quickly churning PPPoEoQinQ sessions and with QoS applied.

  Workaround: There is no workaround.

- CSCso63459

  Symptoms: A system configured for lawful intercept might send SSG-data instead of a generic success message.

  Conditions: This symptom is seen when sending a CoA for enabling/disabling LI.

  Workaround: There is no workaround.

  Further Problem Description: The CoA Ack response shows info about Virtual Access interface and VPI/VCI. The software used is a customer-specific special based on Cisco IOS Release 12.2(31)SB10. A similar special based on Cisco IOS Release 12.2(31)SB3 shows the expected behavior.

- CSCsr01674

  Symptoms: CPU utilization becomes high after the IP SLA Responder is disabled.

  Conditions: The symptom is observed after disabling the IP SLA Responder when both “ip sla responder” and “ip sla responder udp/tcp ...” are configured, and when the IP SLA udp-jitter probe sends packets to this device.

  Workaround: Restoring the IP SLA Responder will bring down the CPU utilization.

- CSCsu62605

  Symptoms: Throughput issue is observed with port-channel interfaces (1+N mode) with only one active member link under a port-channel interface.

  Conditions: The symptom is observed with the following conditions:

  - Port-channel interface with 1001 subinterfaces defined.
  - Hierarchical two-level policy with parent policy shaped to 1MB is attached to each port-channel subinterface.
  - Child policy has 2 PQ + 12 class-based bandwidth queues.

  Workaround: There is no workaround.

  Further Problem Description: The issue is not observed with single GigabitEthernet SPA port and legacy GigabitEthernet cards without port-channel. The issue is seen only with port-channel interfaces using SPA cards. It is not observed with port-channel using legacy GigabitEthernet cards.

- CSCsu92300

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

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

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

- CSCsv91597

  Symptoms: All VCs under a 4OC3ATM port go down.

  Conditions: The symptom is observed when APS is configured with 4OC3ATM cards and when you try to do a manual switchover from working to protect.

  Workaround: An HW-module reset of the card.

- CSCsw82507

  Symptoms: DPM on secondary Cisco Intelligent Services Gateway (ISG) does not clear its session despite the fact that a DHCP termination message is sent. Even though the binding is cleared, the session persists until the idle timeout expires or the session is manually cleared.

  Conditions: Occurs when multiple DHCP relay agents are present between clients and DHCP server.

  Workaround: The session may expire due to idle timeout or be manually cleared.

- CSCsx10028

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

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

  Workaround: There is no workaround.

- CSCsx11266

  Symptoms: Standby crashes after an SSO.

  Conditions: The symptom is observed with the following conditions:

  1. PVCs are discovered in 7600-1.
  2. Policy-map is attached to the PVCs (where ATM map is created).
  3. Traffic is sent from IXIA.
  4. After an SSO, the new active crashes.

  Workaround: There is no workaround.

- CSCsx20258

  Symptoms: Packet counters are not being updated on ISG with a l2 connected subscriber session.

  Conditions: The symptom is observed with a l2 connected subscriber session on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCsx20927

  Symptoms: Files on the standby PRE disk are not displayed/accessible.

  Conditions: The symptom is observed when using simultaneous access to the ATA flash disk.

  Workaround: There is no workaround.

  Further Problem Description: The following error message can be found in logs:

  ```
  %ATA-6-ATA_STATUS_TIMEOUT: Timeout occurred while querying the status of ATA device.
  ```

- CSCsx31996

  Symptoms: When an RP switchover is performed, the booting standby RP is reset. The error message “AAA HA failure” is seen along with some tracebacks.

  Conditions: The symptom is observed when an RP switchover is performed.

  Workaround: There is no workaround.

- CSCsx58268

  Symptoms: The route-map functionality is broken with respect to BGP.

  Conditions: Configure route-map and apply to BGP neighbor as an inbound/outbound policy and then reload the router. The route-map functionality will not work.

  Workaround: There is no workaround.

- CSCsx54861

  Symptoms: Gigaword Accounting attributes are not set in the accounting record.

  Conditions: The symptom is observed when the session’s input or output traffic goes beyond 2^32 bytes.

  Workaround: There is no workaround.

- CSCsx57711

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

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

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

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

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

- CSCsy09743

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

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

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

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

  service-policy XXXXXXXXX

  no service policy XXXXXXXX

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

  ppp multilink ppp multilink group YYY etc

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

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

- CSCsy43147

  Symptoms: A router crashes when the TACACS+ server is configured/unconfigured when the telnet session is up.

  Conditions: The symptom is observed when the single-connection option is used.

  Workaround: Avoid using the single-connection option.

- CSCsy77298

  Symptoms: Option 82 is not appended in DHCP NAK packet by DHCP server.

  Conditions: Not any specific condition.

  Workaround: There is no workaround.

- CSCsy84862

  Symptoms: In a rare event, router may crash in EIGRP code after a peer bounce and route removal.

  Conditions: Crash seen during EIGRP route updates.

  Workaround: There is no workaround.

- CSCsy88764

  SymptomS: ISG PPPoE sessions may lose their authenticated state if they receive Change of Authorization (CoA) for service swapping.

  Conditions: After sending CoA pushes to deactivate an existing service and active new one to ISG PPPOE sessions, the sessions may change state from authenticated to connect. It means the sessions are already in logoff state. As a result, all Subscriber Service Switch (SSS) showings are empty.

  Workaround: There is no workaround.

- CSCsz18711

  Symptoms: NAS-port-ID format reported by AAA accounting VS reply to a CoA account-query are different. Affects back-end server for billing functions.

  Format send by AAA accounting records:

  RADIUS: NAS-Port-Id [87] 25 "GigabitEthernet0/1.118:"

  Format sent in reply to CoA Query:

  RADIUS: NAS-Port-Id [87] 33 "nas-port:10.10.10.101:4/0/0/118"

  Conditions: This behavior was observed in Cisco IOS Release 12.2(33)SB3.

  Workaround: There is no workaround.

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

- CSCsz52815

  Symptoms: If number of hours for statistics is increased to 10 or more after the probe is initially run and then restarted, system crashes with memory corruption

  Conditions: Occurs when the probe is started with the hours of statistics less than 10 and then re-started with the hours of statistics greater than 9.

  Workaround: There is no workaround.

- CSCsz62974

  Symptoms: Router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: Occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- CSCsz71782

  Symptoms: ASR crashes and reboots when RSIM sends VSA 1 command with wrong format.

  Conditions: VSA 1 format string has a colon which should not be there.

  ```
  vsa cisco generic 1 string "qos-policy-out:=remove-class(sub, (class-default, voip))"
  ```

  Workaround: There is no workaround.

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** *IP- address* command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

dlsw remote-peer 0 fst *ip-address*

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

dlsw remote-peer 0 fst *ip-address*

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command.
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
    !--- configured on all interfaces of the affected device so that
    !--- it will be allowed by the CoPP feature.

    access-list 111 deny udp host 192.168.100.1 any eq 2067
    access-list 111 deny 91 host 192.168.100.1 any
```

```
!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.

access-list 111 permit udp any any eq 2067
access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.

class-map match-all drop-DLSw-class
 match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-DLSw-traffic
 class drop-DLSw-class
  drop

!--- Apply the Policy-Map to the Control-Plane of the
!--- device.

control-plane
 service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic
     class drop-DLSw-class
      police 32000 1500 1500 conform-action drop exceed-action drop
```

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

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
    !--- from trusted hosts destined to infrastructure addresses.

    access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK eq 2067
    access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK

    !--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
    !--- all other sources destined to infrastructure addresses.

    access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
    access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK

    !--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
    !--- with existing security policies and configurations.
    !--- Permit all other traffic to transit the device.

    access-list 150 permit ip any any

    interface serial 2/0
     ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in customers environment.

- CSCsz72591

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

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

  Workaround: There is no workaround.

- CSCsz89319

  Symptoms: Free memory is going down because SSS Manager is growing.

  Conditions: This symptom is observed on a Cisco 7600 that is used for ISG and that is running Cisco IOS Release 12.2(33)SRC3 under high network activity.

Workaround: There is no workaround. Reload the router to free memory.

Further Problem Description: The speed of the memory leak depends on the network activity. The more stress on the router, the faster the leak.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCta07104

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

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

  Workaround: The issue will not be seen:

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

- CSCta08000

  Symptoms: Router crashes upon policy-map modification.

  Conditions: The symptom is observed with a flat policy-map when two classes (which match the VLANs) are attached to the port-channel main interface. One class is configured for shaping and the other for policing. The router (PRE3) crashes when removing the policing configuration from the class. The PRE4 shows an “Unable to attach service-policy to the interface” message.

  Workaround: There is no workaround.

- CSCta16724

  Symptoms: Users with level 15 privilege and a “view” cannot do a Secure Copy (SCP).

  Conditions: The symptom is observed when a user with a “view” attempts to do an SCP.

  Workaround: Remove view.

- CSCta30292

  Symptoms: High CPU is seen after MR APS switchover resulting in OSPF link flaps.

  Conditions: This symptom is seen in Cisco routers with Cisco IOS Release 12.2 (34)SB after APS switchover.

  Workaround: There is no workaround.

- CSCta36860

  Symptoms: The ISG will have dangling sessions if multiple CoA messages come in while the ISG is making a CoA request.

  Conditions: The symptom occurs when the ISG makes a CoA request but does not receive a response. During that time, another CoA message comes in to disconnect the session, however, the session will never be disconnected.

  Workaround: Clear the sessions manually.

- CSCta37724

  Symptoms: Modified QoS parameters are not reflected to the ATM VC.

Conditions: The symptom is observed when the interface is shut and any VC QoS parameter is modified, which then triggers VC modification.

Workaround: Do not modify VC parameters in interface shut mode.

- CSCta46107

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

  Conditions: The symptom is observed with the following conditions:

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

  Workaround: There is no workaround.

  Further Problem Description: Using TFTP or SCP works fine.

- CSCta49840

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

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

  Workaround: There is no workaround.

- CSCta72272

  Symptoms: A router may crash while doing an OIR of a PA-MC-E3.

  Conditions: The symptom is observed with a Cisco 7200 series router that is running the 122-31.4.57.SB16 image, with frame-relay configurations and with the controller shut.

  Workaround: There is no workaround.

- CSCta72608

  Symptoms: A Cisco 7304 router crashes.

  Conditions: The symptom is observed when any PA (except PA-MC-8TE1+) is inserted in the slot and then “card type t1 4 0” is configured. The PA-MC-8TE1+ must be inserted in the slot at least once, prior to this.

  Workaround: There is no workaround.

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

  Workaround: Clear VPDN again or reload the router.

- CSCta99225

  Symptoms: Memory leak seen in SSS Feature Manager process.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB. Other platforms/releases may be affected as well.

  Workaround: There is no workaround. A reload will temporarily free the leaked memory.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (a.k.a. tunnel switching). The router may infrequently crash due to a bus error.

This crash is limited to cases where at least one of the following VPDN group commands are configured:

ip pmtu ip tos reflect

Workaround: Disable the above mentioned commands. However the consequences of this on user traffic must be evaluated first.

- CSCtb21155

  Symptoms: There is too much traffic in net-control queue. If output interface is an ATM VBR VC, all VCs on the interface may become blocked.

  Conditions: This symptom is observed on Cisco 10000 series routers that are running Cisco IOS Release 12.2SB and acting as MPLS VPN PE routers.

  Workaround: There is no workaround.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

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

  Workaround: There is no workaround.

- CSCtb36849

  Symptoms: BGP neighbor flaps when many withdraws are sent out to the neighbor.

  Conditions: The symptom is observed when:

  1. RP is redundant and “ha-mode sso” is configured.
  2. There are many withdraws that cannot be sent out in one update packet.

  Workaround: Remove “ha-mode sso” for the neighbor.

  Alternate workaround: Set the MTU size to be the same on both sides of the PE and CE.

- CSCtb44299

  Symptoms: In certain situations, the standby reloads.

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

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

- CSCtb46484

  Symptoms: Router crashes with following error:

  TLB (load or instruction fetch) exception, CPU si Cause 80000008 (Code 0x2): TLB (load or instruction fetch) exception

  Conditions: The symptom is observed when you initiate the sessions from clients (20k with 30 cps). As soon as 200 sessions are in transition state, set the maximum number of sessions.

  Workaround: There is no workaround.

- CSCtb51223

  Symptoms: After RP switchover in SSO mode, some BGP neighbors go into idle state.

  Conditions: The symptom is observed when deleting “ha-mode sso” option before doing a switchover.

  Workaround: Before doing switchover, reload standby RP after deleting “ha-mode sso”.

  Alternate Workaround: Execute the command **clear ip bgp vrf** for the failed peers.

- CSCtb52131

  Symptoms: After a core MPLS enabled interface flaps, hardware MAC rewrite resources may leak. If this condition is repeated many times, the MAC resources may become exhausted, and the following log message will be seen:

  ```
  %GENERAL-3-EREVENT: HWCEF: Failed to allocate HW mac rewrite
  ```

  When the resources become exhausted, packet forwarding may be affected. To see if the problem is happening, monitor the following command output:

  ```
  show pxf cpu cef memory
  FP CEF/MFIB/TFIB XCM Type usage:
   Type Name Col Total   Alloc   Size   Start    End      BitMap  Error


    6  Mac  5   524279  77      8      50800000 50C00000 21236D6C 0
  ```

  While the number of routes remains consistent, the Alloc column will increase until it reaches 524279.

  Conditions: After a core MPLS enabled interface flaps, hardware MAC rewrite resources may leak.

  Workaround: The problem can be cleared by performing a router reload, or PRE failover. This will restore all of the MAC rewrites.

- CSCtb52194

  Symptoms: All access-list configurations are unexpectedly displayed at the top of the configuration.

  Conditions: The symptom is observed following an upgrade to Cisco IOS Release 12.2(33)XND.

  Workaround: There is no workaround.

  Further Problem Description: There is no operational impact as a result of this issue.

- CSCtb81432

  Symptoms: In certain cases, the **show ip aliases** command will not display the VRF routes and the PE will be unable to VRF ping the CE.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)SB7.

  Workaround: Perform a shut/no shut on the CE-facing interface.

  Further Problem Description: A prefix configured on a remotely-connected peer is also configured locally. The local prefix is redistributed into BGP. The remote prefix is also redistributed and advertised by the remote peer. In a rare timing situation, the remote route will be learned before the local route, causing the issue.

- CSCtb83353

  Symptoms: After an RP switchover, the new active RP log shows many tracebacks and all sessions/tunnels are torn down.

  Conditions: The symptom is observed when LNS is configured with 16000 sessions/8000 tunnels (two sessions per tunnel); all sessions with Model D2 QoS. It is seen after an RP switchover.

Workaround: There is no workaround.

- CSCtb83807

  Symptoms: The fix for CSCsz89319 causes the following issues:

  1. Some memory corruption.
  2. An IP session is left dangling if the user profile is misconfigured.

  However, if the fix for CSCsz89319 is not applied, a serious memory leak will occur.

  Conditions: The symptom is observed with the fix for CSCsz89319.

  Workaround: For the IP session issue, check that the user profile is correct.

- CSCtb86439

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

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

  Workaround: There is no workaround.

- CSCtb89424

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

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

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- CSCtb94151

  Symptoms: Attribute Acct-Output-Giga-Word [53] is not provided in an accounting request.

  Conditions: The symptom is observed with PPP sessions on LNS in an L2TP scenario. It is specific to a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCtb95275

  Symptoms: Autocommands configured on VTY line or user-profile are not executing while logging through VTY.

  Conditions: The symptom is observed if the privilege level is not configured in the user profile.

  Workaround: Explicitly configure user privilege in the user profile.

- CSCtb98202

  Symptoms: BGPv6 non-best route is not locally imported.

  Conditions: The non-best v6 route does not get locally imported to the BGP table after the BGP neighbor connection is bounced.

  Workaround: There is no workaround.

- CSCtc00593

  Symptoms: A router experiences nested crashes due to a corrupted program counter.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB7.

Workaround: There is no workaround.

- CSCtc05649

  Symptoms: No SNMP trap is raised and there are missing paths in the output of the **show ip sla mpls-lsp-monitor lpd operational-state** command.

  Conditions: The symptom is observed in an ECMP scenario, when “mpls ip” is removed from one interface out of all the interfaces supporting available paths between A and B. No LPD-group trap is raised when the path is discovered as broken.

  Workaround: There is no workaround.

- CSCtc37839

  Symptoms: A ping to the CPE, which is in a VRF, does not go through.

  Conditions: The symptom is observed with a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB7. It is seen with an LFIoATM bundle with an ATM adapter (ESR-4OC3ATM-SM) being installed in the router. After a quick shut/no shut on the ATM port of the ESR-4OC3ATM-SM card, the problem is observed.

  Workaround: Clear the multilink interface with the command **clear interface multilink x**.

  Further Problem Description: In the Cisco 10000 series router we have a LFIoATM bundle and we can see that the packets are sent out on the multilink and ATM interface. In the incoming direction we do not see the counter increasing on the virtual access interface of the bundle because the PXF drops the received packet.

- CSCtc46174

  Symptoms: A Cisco 10000 series router that is configured for ISG has no limit for number of redirected sessions, which could result in high CPU. The solution is to implement layer 4 redirect session limits in ISG.

  Workaround: There is no workaround.

- CSCtc46512

  Symptoms: There is a crash in SSR regression.

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

  Workaround: There is no workaround.

- CSCtc48125

  Symptoms: Duplicated ARP entry when enabling ISG. When you enable ISG for the existing DHCP users, you may see the following:

```
GPKC10ki01#sh arp | i aaaa.bbbb.cccc
Internet  x.x.x.x          -   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
Internet  y.y.y.y         16   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
GPKC10ki01#
```

  (The one without the age is the ISG user and the one with an age is the DHCP learned address.)

  Conditions: The symptom is observed on a Cisco 10000 series router when enabling ISG on existing DHCP users.

  Workaround: Disable multiple DHCP servers. Use one DHCP server.

- CSCtc49129

  Symptoms: NAT entries are not timed out after the TCP connection closure. It exceeds the PXF NAT TABLE LIMIT.

  Conditions: This symptom occurs with one NAT entry with one TCP session.

  Workaround: There is no workaround.

- CSCtc50985

  Symptoms: Output of the **show ip subscriber dangling** *500* at a steady state shows lots of sessions of the form:

  ```
  dhcp        0000.6401.2a64          [37649]        control   waiting
  ```

  Conditions: The symptom is observed in large scale scenarios or when CPS is much higher than recommended.

  Workaround: Clear the session on the router and reboot, if required.

  Further Problem Description: In scale scenarios, the DHCP handshakes between the client, so the DHCP relay and server might take a long time. Also, the wire or DHCP server is loaded so that it drops some offers or ACKs. In this case, some sessions might be seen dangling without corresponding binding and there is no connectivity to the user.

- CSCtc51554

  Symptoms: Router crashes when CEF is enabled on an LC interface.

  Conditions:

  - Packet should come from Line Card (SPA, GM, LC).
  - Interface should be Ethernet (FE/GigE).
  - Packet should be TCP/IP with any encapsulation like Dot1Q, MPLS.
  - NAT translation should happen.
  - Packet is processed in PXF.

  Workaround: Disable CEF on the affected interface or use native interface.

  Further Problem Description: To provide some additional information, this issue was observed following a code upgrade, and the router was in a continuous crash and reload loop due to CEF being enabled globally on the router. With CEF disabled on the affected interface this issue stopped. Once CEF was re-enabled for that interface, the router crashed.

  If an adjacent HSRP neighbor is running the affected Cisco IOS and has CEF enabled, this router will also likely crash once it becomes the active router for the group.

- CSCtc51952

  Symptoms: An aggressive memory leak in the SSS Manager and/or SSM Connection Manager processes may be seen.

  Conditions: The symptom is observed on a Cisco 10000 series router with a PRE-3, running ISG. It is seen with Cisco IOS Release 12.2(33)SB7.

  Workaround: Reload the router.

- CSCtc65910

  Symptoms: A Cisco 10000 series router may leak buffers from the header buffer pool.

  Conditions: The symptom is observed when lots of traffic is CEF-switched on the PRE. It is not specific to any particular type of interface or PRE, but is specific to the Cisco 10000 series router.

  Workaround: A reload or forced switchover is the only way to clear the buffer leak.

Further Problem Description: When a packet is CEF-switched from an RP and there are already packets present in output hold queue, this packet is also enqueued to the hold queue. Further, if the packet is in particle format then the packet header memory is not freed. So it depends on the type of traffic flow from the router whether this issue will be seen or not and, if seen, how fast it would be.

- CSCtc74804

  Symptoms: Two ARP entries for the same MAC are seen on the intelligent service gateway (ISG) acting as a relay.

  Conditions: This symptom occurs when there are multiple DHCP servers there in the deployment, and a delayed offer comes from one of the DHCP servers to DHCP relay (ISG).

  Workaround: Use only a single DHCP server.

- CSCtc77028

  Symptoms: A Cisco 10000 series router with a mix of passthrough, TAL, prepaid and postpaid sessions may experience a memory leak at sss_pm_post_authorization_cleanup.

  Conditions: The symptom is observed on a Cisco 10000 series router running a PRE-3 and Cisco IOS Release 12.2(33)SB7.

  Workaround: Reload the router.

- CSCtc77088

  Symptoms: On a Cisco 10000 series router, removing an ACL from an ISG-facing interface with the command **no ip access-group** *list* **in** may result in a forwarding failure for all ISG subscriber sessions permitted in ACL.

  Conditions: The symptom is observed on a Cisco 10000 series router running a PRE-3 and Cisco IOS Release 12.2(33)SB7 where **no ip access-group** *list* **in** and ISG exist on same interface.

  Workaround: Use the command **clear sss session all**.

- CSCtc84758

  Symptoms: On a router configured for ISG that is running postpaid Web-Logon users with SESM as the external portal, a memory leak may occur in RADIUS LOCAL SERVER.

  Conditions: The symptom is observed on a Cisco 10000 series router with a PRE-3 and running Cisco IOS Release 12.2(33)SB7 using SESM as a captive portal. The issue can be triggered with this sequence of events:

  1. Postpaid user is redirected to SESM.
  2. SESM sends Access-Request to router after captivating user/pass from postpaid user.
  3. RADIUS LOCAL SERVER creates AAA request and sends it to ISG.
  4. ISG creates another AAA request to send an Access-Request to authenticate the postpaid user.
  5. AAA receives a response from external AAA.
  6. AAA passes the response to RADIUS LOCAL SERVER which transmits an Access-Accept or Access-Reject to SESM.

  If the processing delay of sum (C,D,E,F) is greater than the SESM timeout, SESM will send another Access-Request with the same credentials for the Account logon postpaid user in B.

  If this occurs, policy/AAA will now use this second Account-Logon request from SESM for this user's Account Login and the policy will not free the AAA request from the former Account Logon request, hence the memory leak will present as RADIUS LOCAL SERVER.

  Workaround:

  1. Make sure SESM Account Logon Timeout > RADIUS timeout.

2. Decrease load on external AAA (RADIUS) machines.

- CSCtc86075

  Symptoms: A router crashes when the command **show aaa user all** is issued.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(34)SB.

  Workaround: There is no workaround.

- CSCtc87569

  Symptoms: If "ip subscriber routed" is removed from an ISG-facing interface while subscriber sessions exist, a memory leak in the PXF iEdge IP process may be observed with the **show memory debug leaks chunks** command.

  Conditions: The symptom is observed on a Cisco 10000 series router running PRE-3 and Cisco IOS Release 12.2(33)SB7. The router is running ISG with "ip subscriber routed" configured.

  Workaround: Using the **reload** command will recover memory.

- CSCtc87822

  Symptoms: On a PE router, eBGP-learned VRF routes might not be advertised to eBGP neighbors in the same VRF.

  Conditions: The symptom is observed if DUT first learns the route from IBGP-VPNv4 (same RD) and then learns the route from the CE.

  Workaround: Soft clear towards the CEs missing the routes.

- CSCtc90779

  Symptoms: A router may crash after displaying align fatal errors pointing to PPPoE functions.

  Conditions: The symptom is observed on a Cisco 7206VXR router (NPE-G1) that is running Cisco IOS Release 12.2(31)SB15.

  Workaround: There is no workaround.

- CSCtc98374

  Symptoms: ISG service policies may not get applied to a session.

  Conditions: The symptom is observed with a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB7.

  Workaround: Use auto service or transparent service logon.

- CSCtd03664

  Symptoms: LNS sessions input gigawords are not getting set properly.

  Conditions: The symptom is observed when AAA accounting is configured for sessions.

  Workaround: There is no workaround.

- CSCtd03798

  Symptoms: In an MPLS VPN, when a Cisco 7300 series router is being used as a PE, some prefixes lose reachability. The packet capture between PE and CE shows that the header checksum is incorrect:

  Protocol: ICMP (0x01) Header checksum: 0x93a8 (should be 0x9308)

  Conditions: The symptom is observed under the following conditions:

  – An MPLS VPN where a Cisco 7300 series router is being used as PE with NSE-100.

- Both ingress and egress interfaces must be link ethernet interface (SPA/PA GigE or FE).
- Egress interface towards CE must contain QoS marking and it should be a dot1q interface.

Workaround: Remove QoS marking.

Alternate workaround: Use Native GigE.

- CSCtd15853

Symptoms: When removing VRF configuration on remote PE, local PE receives withdraw message from remote PE to purge its MDT entry. However, local PE does not delete the MDT entry.

```
/// Topology ///

                iBGP
         <-------------------->
   12.2(33)SB7             12.0(27)S4a
   1.1.1.1/32              2.2.2.2/32
   PE1(UUT)   ------------ PE2
```

PE1 receives MDT entry from PE1 and PE2.

Please focus a entry of "2.2.2.2/32" from PE2.

```
PE-1
---
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*> 1.1.1.1/32       0.0.0.0                                0 ?
*>i2.2.2.2/32       2.2.2.2                  0    100      0 ? <<<---- HERE
*>i3.3.3.3/32       3.3.3.3                  0    100      0 ?
---
```

To trigger the issue, vrf configuration is remove on PE2.

You can see that PE2 sends withdraw message to PE1(1.1.1.1).

```
PE-2
---
PE2-PRE1#
PE2-PRE1#
PE2-PRE1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
PE2-PRE1(config)#
PE2-PRE1(config)#no ip vrf V1
Tunnel interface was deleted. Partial configuration may reappear on reuse.
% IP addresses from all interfaces in VRF V1 have been removed
```

```
PE2-PRE1(config)#
PE2-PRE1(config)#
*Nov  9 12:29:35.447: %LINK-5-CHANGED: Interface Tunnel3, changed state to
administratively down
*Nov  9 12:29:36.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel3,
changed state to down
PE2-PRE1(config)#
PE2-PRE1(config)#end
PE2-PRE1#
PE2-PRE1#
*Nov  9 12:30:05.435: BGP(2): nettable_walker 2:1:1:2.2.2.2/32 no best path
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send unreachable 2:1:1:2.2.2.2/32
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send UPDATE 2:1:1:2.2.2.2/32 --
unreachable <<--- HERE
*Nov  9 12:30:05.435: BGP(2): updgrp 1 - 1.1.1.1 enqueued 1 updates,
average/maximum size (bytes) 45/45
PE2-PRE1#
PE2-PRE1#
PE2-PRE1#sh ip vrf

PE2-PRE1#


---
```

The MDT entry(2.2.2.2/32) is not deleted even if PE1 indeed receives withdraw message from PE2. “clear ip bgp *” would be needed to purge the MDT entry.

```
PE-1
---
PE1-PRE2#
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:3.3.3.3/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:1.1.1.1/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP(4): 2.2.2.2 send UPDATE (format) 2:1:1:1.1.1.1/32,
next 1.1.1.1, label 0, metric 0, path Local
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:2.2.2.2/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP(4): updgrp 1 - 2.2.2.2 updates replicated for neighbors:
*Nov  9 12:30:05.799: BGP(4): 2.2.2.2 rcv UPDATE about 1:1:2.2.2.2/64 --
withdrawn, label 3 <<--- HERE
*Nov  9 12:30:05.799: BGP: 2.2.2.2 Modifying prefix 1:1:2.2.2.2/64 from 4 -> 3
address
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*> 1.1.1.1/32       0.0.0.0                                0 ?
*>i2.2.2.2/32       2.2.2.2                  0    100      0 ? <<---- HERE
*>i3.3.3.3/32       3.3.3.3                  0    100      0 ?
PE1-PRE2#

PE1-PRE2#
PE1-PRE2#clear ip bgp *
PE1-PRE2#
*Nov  9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Down User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 VPNv4 Unicast
topology base removed from session  User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 IPv4 MDT
topology base removed from session  User reset
*Nov  9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Down User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 VPNv4 Unicast
topology base removed from session  User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 IPv4 MDT
topology base removed from session  User reset
*Nov  9 12:31:22.555: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Up
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 3.3.3.3,
origin ?, localpref 100, metric 0
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd 1:1:3.3.3.3/32
PE1-PRE2#
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
* i3.3.3.3/32       3.3.3.3                  0    100      0 ?
---
```

Conditions:

- mVPN is configured on PE router.
- Both Pre-MDT SAFI and MDT-SAFI IOS are running in a Multicast Domain.

CCO : MDT SAFI

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCtd24065

  Symptoms: The output of the command **show subscriber statistics** shows that number of "SHDBs in use" is greater than the total number of unique subscribers for the deployment. This might contribute to issues such as an "out of IDs" message or sessions not coming up.

  Conditions: The symptom occurs for DHCP-initiated sessions either when:

  1. Session idle times out followed by a lease expiry or you release the lease.
  2. Session is cleared using the **clear subscriber session** command and there is a lease expiry or you release the lease.

  Workaround: There is no workaround.

  Further Problem Description: This can also contribute to a small amount of observed memory leak.

  This problem occurs in code branches where IP session HA is not supported. In these branches, the above steps cause a SHDB handle to not be cleared properly when other data structures are cleared.

- CSCtd30478

  Symptoms: When ISG is enabled on a Cisco 10000 series router, an SNMP MIB query for interface(s) statistics shows that the packets and byte (octet) counts for the sub-interface(s) are twice as much as the actual input packets on the main interface.

  Conditions: The symptom is observed when the interface(s) statistics are queried via SNMP. It is seen only when ISG is configured/enabled on the interface/sub-interface.

  Workaround: There is no workaround.

- CSCtd32975

  Symptoms: On a Cisco 10000 series router with PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and ISG, the memory on the standby RP may become severely fragmented.

  After an SSO switchover, the new-active RP initially takes over with fragmented memory causing frequent malloc errors and eventually requiring a reload to recover.

  Conditions: The symptom is observed on a Cisco 10000 series router with PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and with 10K ISG sessions in a mix of web-login, TAL, prepaid, and passthrough.

  Workaround: Reload will recover memory.

- CSCtd33145

  Symptoms: On a Cisco 10000 series router/PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and ISG, the memory on the standby RP may become severely fragmented due to some SSS functions.

  After an SSO switchover, the new-active RP initially takes over with fragmented memory causing frequent malloc errors and eventually requiring a reload to recover.

  Conditions: The symptom is observed on a Cisco 10000 series router/PRE-3 that is running Cisco IOS Release 12.2(33)SB7 with 10K ISG sessions in a mix of web-login, TAL, prepaid, and passthrough.

  Workaround: A reload will recover memory.

- CSCtd35091

  Symptoms: The input queue on ISG access interface gets filled up causing the interface to wedge.

Conditions: The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

Workaround: There is no workaround other than a router reload.

- CSCtd38225

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

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

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

- CSCtd38351

  Symptoms: SNMP monitoring of sub-interfaces may report spikes in outbound traffic.

  Conditions: The symptom is observed when ISG is enabled on a Cisco 10000 series router.

  Workaround: Use and compare against main interface counters.

- CSCtd42928

  Symptoms: An IP DHCP ISG subscriber session is not being created for a particular subscriber. Other subscribers are not affected.

  Conditions: The symptom is observed under the following conditions:

  1. Scale scenario (greater than 20k sessions).
  2. Using debugs and show commands it is determined that no session or binding exists for the subscriber, but a DPM context exists.

  Workaround: There is no workaround.

  Further Problem Description: In such conditions the only way to start the session for the subscriber is a reload or switchover.

- CSCtd56237

  Symptoms: A router may crash at c10k_get_ips_segment_from_vcci during high call ISG call volume and appreciable punted (non PXF) interrupt traffic.

  Conditions: The symptom is observed with a Cisco 10000 series router/PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and ISG with 15000 postpaid and prepaid Web Logon and TAL sessions.

  Workaround: There is no workaround.

- CSCtd57146

  Symptoms: Router crash while configuring “ip vrf forwarding blue” on loopback interface in MVPN setup.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS 12.2(33)SB8.

  Workaround: There is no workaround.

- CSCtd71372

  Symptoms: DHCP-initiated IP sessions sometimes get into a dangling state, either in data plane or control plane. This leads to lost connectivity for the end users who have the sessions dangling.

  Conditions: The symptoms are due to some not yet identified race conditions in DPM/DHCP.

  Workaround: There is no workaround.

- CSCtd87264

  Symptoms: DHCP unicast BootP offers can not be propagated back in the incoming interface as the ARP entry is missing. This happens only when the relay function is combined in a VRF and the incoming interface is unnumbered.

  Conditions: The symptom is observed when SRD/SRE Cisco 7600 series router is a DHCP relay/snooping agent. The request must come in a VRF.

  Workaround: Move the relay agent function to the global routing table.

- CSCte15138

  Symptoms: A router intermittently shows the following message:

  ```
  %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: Class All classes: - remove
  feature
  ```

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

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB7

Cisco IOS Release 12.2(33)SB7 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB7 but may be open in previous Cisco IOS releases.

- CSCdy26008

  Symptoms: The negotiated IP address is not cleared from an asynchronous interface when a call ends, even though the IP address is returned properly to the IP peer pool.

  Conditions: This symptom is observed when the peer is configured to dial in to the network access server (NAS) and to obtain an IP address through IP Control Protocol (IPCP) negotiations with the NAS. The NAS is configured with pools of IP addresses to be allocated to the peer when the peers generate a PPP call to the NAS. The NAS is also configured to authenticate the peer through RADIUS.

  Workaround: There is no workaround.

- CSCec72958

  Symptoms: A Cisco router that is configured for Network Address Translation (NAT) may reload unexpectedly because of a software condition.

  Conditions: This symptom can occur when the router translates a Lightweight Directory Access Protocol (LDAP) packet. NAT translates the embedded address inside the LDAP packet. This problem is strictly tied to NAT and LDAP only.

  Workaround: There is no workaround.

- CSCee19691

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

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

Workaround: There is no workaround.

- CSCee30355

  Symptom: A Cisco router may experience a memory leak. The "Holding" column in the output of the show process memory command shows that the "VTEMPLATE Backgr" process allocates memory without freeing it. This column will continue to grow until all the memory is consumed.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP version 2. In addition configuration with 800+ virtual-access interfaces using VPDN reported a memory leak for the RIP multicast group.

  Workaround: Schedule the router for a periodic reload before it completely exhausts all available memory.

- CSCeg80842

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

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

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

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

- CSCeh06778

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

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

  Workaround: There is no workaround.

- CSCek75694

  Symptoms: A router running Cisco IOS 12.4T may reload unexpectedly

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCek78031

  Symptoms: Some BGP routes are missing from RIB so packets cannot reach the destination.

  Conditions: A connected route covers the BGP route in question, but the connected route is less specific than some other route that is also in the RIB. It leads to BGP to have some prefixes' nexthops inaccessible, and those prefixes are not installed in to RIB, therefore traffic is stopped.

  Workaround: There is no workaround.

- CSCin01217

  Symptoms: A router may not allow the peak cell rate value on an interface that is bundled with more than one ATM T1 interface or more than one ATM E1 interface to be set to a value that is more than the bandwidth of one T1 ATM interface or one E1 ATM interface.

Conditions: Occurs on Cisco 3600 routers Cisco IOS Release 12.2(6.8)T2

Workaround: There is no workaround.

- CSCin91677

  Symptoms: The Unavailable Seconds (UAS) that are displayed in the output of the **show controllers serial** *slot/port* command are incorrect. The display of the UAS starts only after 20 contiguous severely errored seconds (SES) instead of after 10 contiguous SES.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

  Workaround: There is no workaround.

- CSCsb61514

  Symptoms: Packets larger than 1526 bytes get dropped between supervisor and Cisco Multi-Processor WAN Application Module (MWAM) on a Cisco 7600.

  Conditions: Drops were seen even after increasing MTU size.

  Workaround: Reduce MTU on tunnel end systems, which increases fragmentation.

  Further Problem Description: The problem is reproducible with extended pings of size 1527 bytes, which get dropped in direction SUP->MWAM as diagnosed with **deb ip icmp**.

- CSCsb98906

  Symptoms: A memory leak may occur in the “BGP Router” process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCsc78999

  Symptoms: An Address Error exception occurs after Uninitialized timer in TPLUS process.

  Conditions: This is a platform independent (AAA) issue. It may be seen with a large number of sessions while accounting is configured with a T+ server.

  Workaround: Disable accounting, or use RADIUS accounting instead of a T+ server.

- CSCsd99763

  Symptoms: A Cisco 7200 series router reloads unexpectedly while configuring BGP access list.

  Conditions: This symptom is observed on a Cisco 7206VXR (NPE-G1) processor (revision A). The following commands serve as an example that causes router to reload unexpectedly:

```
config t
   router bgp 100
   neighbor EXTERNAL route-map MAP3 out
   address-family ipv4 multicast
   neighbor EXTERNAL route-map MAP3 out
   !
   ip as-path access-list 1 deny ^$
   ip as-path access-list 2 permit ^(700)+(_1123)|_2374$|^(_700)+(_2374)+(_1123)+$
   ip as-path access-list 3 permit _3400_
   ip as-path access-list 4 permit ^(700)+(_3400)|_1123$|^700$|_23\[0-9\]$
   !
   route-map MAP3 permit 10
```

```
match as-path 1
!
route-map MAP3 deny 20
match as-path 2
!
route-map MAP3 permit 30
match as-path 3
!
route-map MAP3 permit 40
match as-path 4
set metric 300
end
```

Workaround: There is no workaround.

- CSCse26506

  Symptoms: When you perform an OIR of an ATM line card, a CPUHOG condition may occur in the "BGP Event" process.

  Conditions: This symptom is observed when the ATM line card is configured with about 15,000 /32 routes.

  Workaround: There is no workaround.

  Further Problem Description: The ATM line card connects to about 15,000 different gateways, each of which is covered by its own /32 route. In addition, there is a less specific route that covers everything. The symptom occurs when BGP attempts to remove a large number of these tracked entries without suspending any.

- CSCse29570

  Symptoms: Router might unexpectedly reload during CNS configuration download.

  Conditions: The downloaded configuration must disable the CNS configuration initial or partial for this crash to occur.

  Workaround: Use static configuration and prevent configuration download from CNS server.

- CSCse99958

  Symptoms: A Cisco router may fail to access a flash card after formatting it, and the following error message is generated:

  ```
  *** Emulating mis-aligned load at 0x80000190 PC = 0x8001179c ... succeeded
  ```

  Conditions: The symptom is observed on a Cisco 7200 series, Cisco 7301, and Cisco 7500 series that run Cisco IOS Release 12.4(10) or Release 12.4(12) and occurs only when a flash card is accessed from the ROMmon prompt.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(8a) or an earlier release.

- CSCsf25157

  Symptoms: An IPv6 ping may fail when the **atm route-bridged ipv6** command is enabled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(22.13), interim Release 12.4(13.9), or Release 12.4(13b) and that is configured for QoS.

  Workaround: There is no workaround.

- CSCsg00173

  Symptoms: Traffic blackholing is seen in DFC-based PVLAN configuration.

  Condition: The RPF Vlan has to be programmed as secondary VLAN in the hardware tables for PVLAN to work with multicast. This condition is not satisfied in case of DFC as the primary Vlan gets programmed as RPF Vlan. The problem is not seen on the supervisor.

  Workaround: There is no workaround.

- CSCsg08751

  Symptoms: Route Switch Processor (RSP) may crash when flash card is removed from RSP slot.

  Conditions: This has been seen on RSP running Cisco IOS Release 12.4(10).

  Workaround: There is no workaround.

- CSCsg11616

  Symptoms: While restarting the iprouting process, the system crashed at redzone corruption.

  Conditions: Occurs following a switchover. The iprouting process should restart once the standby becomes active.

  Workaround: There is no workaround.

- CSCsg39754

  Symptoms: When DHCP snooping is configured on a VLAN, the redirect access list programmed in TCAM permits a wide range of UDP ports from bootps/bootpc to 65xxx.

  Conditions: UDP traffic to these destination ports (0x143, 0x243, 0xFF43) is being redirected to Route Processor (RP). If “ip dhcp snooping limit” is not configured, then RP CPU goes to 100%.

  Workaround: There is no workaround.

- CSCsg87559

  Symptoms: A client that has IPv6 for DHCP implemented may not receive a correct prefix.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as a DHCP server, that has IPv6 for DHCP implemented, and that has the **allow-hint** DHCP IPv6 interface server configuration enabled. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg92473

  Symptoms: The netflow shortcuts created are cleared before the full capacity of 128k flows (PFC3B) and 256k flows (PFC3BXL) is reached and before the reflexive ACL ageing timers expire. The full capacity is not achieved and active flows may start to get purged.

  Conditions: The symptoms are observed when either the traffic is from 128k or 256k different sources.

  Workaround: There is no workaround.

- CSCsg99677

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

  ```
  File disk#:crashinfo_20070418-172833-UTC open failed (-1): Directory entries are
  corrupted, please format the disk
  ```

  Or the crashinfo file will be stored as CRASHI~1.

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

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

Further Problem Description:

- CSCsh48919

  Symptoms: With an ATA flash card, the **dir disk0:** command will fail if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well. This situation can also occur with a compact flash (CF) card using the **dir flash:** command.

  Conditions: This symptom has been observed when using a removable flash card, such as an ATA flash car or CF card, that is formatted to use DOSFS. The removable flash card is removed from the router and inserted into a laptop that is running a version of the Microsoft Windows operating system. A “New Folder” directory is created on the flash card and the flash card is removed from the laptop and re-inserted into the router. Entering the **dir** command on the router may fail to show all of the stored files or may crash the router.

  Workaround: Remove or rename all files and directories having names with embedded spaces so that no file or directory names contains embedded spaces.

- CSCsh48947

  Symptoms: Some of the 48 power over Ethernet ports of a line card cannot be configured as “power inline static” with the maximum power capacity, 15.4 watts, that a port can support.

  Conditions: The number of supported ports depends on the power rating of the voice daughter board. One or more ports may not operate at maximum capacity.

  Workaround: There is no workaround.

- CSCsi07687

  Symptoms: Self ping to SVI fails when VLAN configurations are removed and reapplied.

  Conditions: Occurs when an interface is deleted and added again.

  Workaround: There is no workaround.

- CSCsi73982

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

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

  Workaround: There is no workaround.

- CSCsi88974

  Symptoms: While configuring a mediation device (MD), if the MediationSrcInterface is set to loopback interface, traffic will cause MALLOC failures.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: Do not use loopback0 as MD source interface.

- CSCsi93916

  Symptoms: An alignment error (i.e., spurious memory access) that causes tracebacks such as “ipnat_nbss_is_special_packet” may be observed on a Cisco router.

  Conditions: The symptoms are observed with a certain packet format, not yet identified. It is specific to the NetBios Session Service (NBSS) protocol.

  Workaround: There is no workaround.

- CSCsj34557

  Symptoms: Router displays following error message and reloads:

```
Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0
%SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000)
-Traceback=
0x6080CEB0 0x60982108 0x60982EC0 0x6098511C 0x609853BC
%SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C        0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
662B5B1C,608A6F3C        0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
%SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C        0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
662B5B1C,608A6F3C        0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6
%SYS-6-BLKINFO: Corrupted redzone blk E5D8310, words 6088, alloc 61FE2638,
InUse, dealloc 80000000, rfcnt 1 -Traceback= 0x6080CEB0 0x609681D4 0x6098211C
0x60982EC0 0x6098511C 0x609853BC
%SYS-6-MEMDUMP: 0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208
%SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638 0xE5DB2D0 0xE5D8144 0x800017C8
%SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478
```

Conditions: Occurred on a Cisco 7200 running the c7200-ik9s-mz.124-7a.bin image.

Workaround: There is no workaround.

- CSCsj35342

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

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

  Workaround: Configure “no aaa accounting gigawords.”

- CSCsj46607

  Symptoms: On Cisco 7600 routers, configuring Unicast Reverse Path Forwarding (Unicast RPF) for prefixes that are reachable via multiple paths may not set unicast RPF correctly on all paths.

  Conditions: If unicast RPF is enabled on the first path, it will show up as being enabled on all paths in **show mls cef ip** *prefix*. If it is enabled on the first path and the unicast RPF configuration of other paths is changed, the unicast RPF for the prefix is not updated.

  Workaround: There is no workaround.

- CSCsj98198

  Symptoms: The following error occurs:

  ```
  %NETFLOW_AGGREGATION-4-OER_AGG_EXPORT_ERROR: OER Error receiving TT agg export packet
  on RP
  ```

  Conditions: Errors may be seen on Cisco 6500 running as Optimized Edge Routing (OER) border router

  Workaround: There is no workaround.

- CSCsk25915

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

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

Workaround: There is no workaround.

- CSCsk39926

  Symptoms: FTP transfer fails if source interface is part of VPN routing/forwarding (VRF).

  Conditions: Occurs when the interface configured in **ip ftp source-interface** <*interface-name*> is part of a VRF or the FTP server is part of a VRF.

  Workaround: Use an interface that is not part of a VRF, and the FTP server should be known via global routing table.

  Further Problem Description: FTP client is not VRF aware. It always looks in the global routing table to reach the specified FTP server. If the specified FTP server is not known via the global routing table, the connection attempt will fail, either with a time out or destination unreachable error.

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

  This advisory is posted at the following link:
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml

- CSCsk70218

  Symptoms: RF resetting the standby CPU.

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

  Workaround: There is no workaround.

- CSCsk80250

  Symptoms: A router may reload.

  Conditions: This symptom is observed when the **show ip bgp neighbors** *x.x.x.x* **paths ^([^7][^0][^1][^8]|.|..|...|.....)+_7018_** command is issued.

  Workaround: There is no workaround.

- CSCsk83038

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

  1. High CPU. Packets sent at 1% of the line rate.
  2. Packets switched in software.
  3. VACL capture port takes a long times to start capturing packets.

  This issue not seen during the regular SSO switchover.

  Conditions: Occurs when doing the ISSU operation.

  Workaround: There is no workaround.

- CSCsk96581

  Symptoms: After loading a router for the first time or performing a switchover with a large number of BGP neighbors configured, some neighbors may send hold timer expired notifications before reaching established state.

Conditions: The problem is seen on routers with highly scaled configurations with many BGP neighbors with low hold timers configured. Typically, the problem is most likely to be seen after a switchover happens when all interfaces on the new active RP come up at approximately the same time. The sudden burst of sessions attempting to establish at the same time can cause some of the sessions to fail to be serviced in time to satisfy aggressive hold timers. Established sessions are not vulnerable to this issue; only sessions in progress to established state can experience the problem.

Workaround: BGP neighbors can be brought up in smaller groups rather than all at once to distribute the session establishment load so that no session in progress to established state will exceed their configured hold timers.

- CSCsk97295

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

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

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

- CSCsk99465

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

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

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

  Workaround: There is no workaround.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsl01427

  Symptoms: The following symptoms all relate to the same root cause:

  1. In syntax check mode, if there is a standby in SSO mode, the **cts dot1x** command does not work and the following error messages are displayed:

     ```
     RouterRP(syntax-if)#cts dot1x %ERROR: Standby doesn't support this command ^ %
     Invalid input detected at '^' marker.

     RouterRP(syntax-archive)#path disk0: %ERROR: Standby doesn't support this command
     ^ % Invalid input detected at '^' marker.
     ```

  2. After a redundancy force-switchover, the applet configuration is lost and retains only the applet name. (This is done by configuring an applet on the main RP and switchover to the Standby by issuing a redundancy force-switchover. Issue the **sh run** command on the Standby which is now the main RP.) All the action statements are lost.
  3. The Standby switch reloads by itself after going into the event manager applet configuration mode:

```
Config Sync: Line-by-Line sync verifying failure on command: event manager applet
cli-test-01 due to parser return error
```

4. The Standby switch may also reload upon removing the command **event manager applet**:

```
RouterRP(config)#event manager applet 1 EEM: Applet 1 is currently being modified
OR
RouterRP(config)#no event manager applet 1 EEM: Applet 1 is currently being
modified
```

Conditions: The symptoms are observed in syntax check mode, if there is a standby in SSO mode.

Workaround: There is no workaround.

- CSCsl04500

  Symptoms: Under certain conditions, a process called “OBFL interrupt a” may run as high as 100% for sustained periods on an individual Cisco 6700 module.

  Conditions: This was observed on a Cisco 7609 that is running Cisco IOS Release 12.2(18)SXH.

  Workaround: Apply the **hw-module reset** command to the offending module.

- CSCsl24511

  Symptoms: The problem was introduced due to the existence of multiple outgoing mcast interfaces. When ToS was changed from one interface during particle- based fastswitching, the change was carried to other interfaces, which made QoS policy perform incorrectly.

  Conditions: Fix should be applied to Cisco IOS Releases 12.2SR and 12.2SX. It is not required in haw_t and also not required by images using MRIB/MFIB.

  Workaround: Disable fastswitching and do process switching only.

- CSCsl28931

  Symptoms: On Cisco 7600 configured with VPLS, if the traffic on the ingress direction and egress direction follows different Forwarding Engines (DFC or CFC), the dynamically learned entries may not be synchronized after a line card online insertion and removal (OIR), resulting in the traffic being flooded for those MAC entries.

  Conditions: Occurs under the following scenario:

  1. The traffic flow needs to be asymmetrical, for example in a VPLS scenario, the ingress traffic comes from a switchport in a ES-20 line card (which has a distributed forwarding engine) and is forwarded to a core facing line card like SIP-400. In this flow, the ingress traffic is forwarded by the ES-20 local forwarding engine and the opposite traffic (MPLS core to access) is forwarded by the central forwarding engine.
  2. A line card OIR happens

  Workaround: Clear MAC address table dynamic entries.

- CSCsl32142

  Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with “Bad getbuffer” error may also be reported.

  Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

  Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl34523

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

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

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

Workaround: There is no workaround.

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

- CSCsl40687

  Symptoms: Router reloads due to a bus error. This occurs with the following messages:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 08:32:13 AEST Tue Nov 20 2007
  addr=0xB8, pc=0x40099888 , ra=0x44020000 , sp=0x465870E8

  08:32:13 AEST Tue Nov 20 2007: TLB (store) exception, CPU signal 10, PC = 0x40099888

  -Traceback= 0x40099888 0x402F6358 0x415102F4 0x41510C7C 0x402FF5C4 0x414F1140
  0x402FF7B8 0x41C8B8E0 0x41C8EFC0 0x41C8F064

  0x41C85260 0x421EA0C4 0x421EA224
  ```

  Conditions: This occurs after applying a Modular Quality of Service Command-Line Interface (MQC) class on a PVC.

  Workaround: Use frame relay traffic shaping (FRTS) instead of MQC under the PVC.

  Further Problem Description: MQC policy is not a supported configuration for MLPoFR connections. The above configuration is not valid. Currently, the MQC policies are configurable under MLPoFR PVCs and this results in router reload. However, the router should not crash even under those circumstances. This fix prevents MQC QOS policy from being configured on MLPoFR connections at config time when MLP may not yet be active. So, in effect, the config is blocked both if MLP is active or if MLP is just configured.

- CSCsl42113

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

  - mroute entries are correct.
  - IGMP groups are correct.
  - Receivers on the egress line card are not able to receive the multicast.
  - Interfaces counters show that the switch is receiving the multicast stream.

  Conditions: Applies to Egress multicast replication.

  Workaround: Change the multicast replication mode to “ingress”.

- CSCsl42732

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

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

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

- CSCsl51914

  Symptoms: On Cisco 7600/SIP400 supporting MLP interfaces, “priority percent” does not work.

  Conditions: The conditional police rate values will not get updated:

  1. Whenever a member link addition or deletion happens from the bundle.
  2. When all the members of the multilink are down and come back.

3. SPA / LC online insertion and removal (OIR).

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

- CSCsl52594

  Symptoms: When two routers are configured to form an IPv6 EIGRP adjacency, attempts to ping one of the loopback IPv6 addresses from the neighbor fails with the following error:

  ```
  No valid source address for destination
  ```

  Conditions: Occurs on routers running Cisco IOS Release 12.4T.

  Workaround: There are two workarounds:

  1. Disable IPv6 Cisco Express Forwarding (CEF)
  2. Enter the **clear ipv6 eigrp neighbor** command

- CSCsl57457

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) NSF may not work.

  Conditions: Occurs when router is running a modular Cisco IOS image.

  Workaround: There is no workaround.

- CSCsl65047

  Symptoms: Back-to-back ping fails after configuring “native” on subinterface.

  Conditions: Initially ping works fine, but packets go out tagged, which should not be the case. On doing a **shut/no shut** on one sub-interface with native configured cause ping to fail since the side that was flapped starts sending untagged ping packets (which is the expected behavior). The remote side that has not been flapped, expects tagged packets.

  Workaround: Do **shut/no shut** on both ends of the sub-interface.

- CSCsl65087

  Symptoms: SIP200 line card crashes due to memory corruption when high traffic passes through on a software based dLFI bundle which has ACFC/PFC configured.

  Conditions: Happens when traffic on the bundle is oversubscribed.

  Workaround: There is no workaround.

- CSCsl68327

  Symptoms: Packets may be lost during rekey.

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

  Workaround: There is no workaround.

- CSCsl71704

  Symptoms: A receive access control list (rACL) with large ACL is not applied on interface if is QoS configured.

  Conditions: Occurs when rACL with large ACL is applied on an interface. It consumes over 60% of ternary content addressable memory (TCAM) space. If the rACL is applied a second interface with QoS, the configuration fails without displaying an error message.

  Workaround: There is no workaround.

- CSCsl75136

  Symptoms: Switch with Sup32 supervisor running modular Cisco IOS software may fail to boot up after a power cycle.

Conditions: Occurs after the switch has been power cycled.

Workaround: There is no workaround.

- CSCsl86614

  Symptoms: E-OAM loopback session gets broken after SSO.

  Conditions: This issue is observed in the following scenario:

  1. Two routers are connected back-to-back and configured for e-oam.
  2. A remote loopback is created and then a switchover is performed.

  It is expected that the loopback status holds during switchover, however, the interface exits that state.

  Workaround: There is no workaround.

- CSCsl87404

  Symptoms: L2TP tunnels are not getting established.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsl94263

  Symptoms: A Cisco 7500 series router may crash.

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

  Workaround: There is no workaround.

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

- CSCsl96335

  Symptoms: When a subscriber connects and disconnects from an ASR1000 at a high level of calls per second, the system may encounter an error with the following traceback:

  ```
  ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = AAA SEND STOP EVENT
  ```

  Conditions: The symptoms are observed when an ASR1000 is functioning as LAC or LNS with ACL, QoS and uRPF features. AAA accounting is enabled for tunnel, sessions and PPP.

  Workaround: If the error is encountered persistently, consider disabling AAA accounting as temporary remedy.

- CSCsl97835

  Symptoms: The standby supervisor may crash.

  Conditions: Occurred in a system with scaled configuration with a operational rep segment. Occurred when a rep port role was configured as non-edge and then swapped to edge.

  Workaround: Shutdown the port before making changes described above.

- CSCsm01389

  Symptoms: Crash occurs after clearing auto-tunnel backup by issuing the **clear mpls traf-eng auto-tunnel backup** command.

  Conditions: Occurs with SSO and traffic engineering (TE) auto-tunnel feature enabled.

  Workaround: There is no workaround.

Further Problem Description: Crash was seen on Active SP after issuing **clear mpls tra auto-tunnel primary** followed by **clear mpls tra auto-tunnel backup** command. This crash could happen with or without a SSO switchover before issuing those commands.

- CSCsm20599

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

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

  Workaround: After creating a PVC on a P2P sub-interface, call "exit" or "end".

- CSCsm28287

  Symptoms: After shutting down a GRE tunnel interface, the active RP crashed and switchover took place. The following error message was displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 13:02:45 UTC Fri Jan 18 2008
 addr=0xD, pc=0x7144A5A0, ra=0x7209FFF8, sp=0x5ABEE90
SLOT0:01:40:03: %DUMPER-3-PROCINFO: pid = 16409: (sbin/ios-base), terminated
due to signal SIGBUS, Bus error (Invalid address alignment)
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:             zero     at
v0       v1
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:   R0   00000000  7A5FD854
EF4321F9  7A6452D0
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:             a0       a1
a2       a3
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:   R4   EF4321CD  0000000B
0000000B  00000000
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:             t0       t1
t2       t3
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:   R8   7CB96E10  00FDDBE0
00000000  EFFFFFFF
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:             t4       t5
t6       t7
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:   R12  00000000  F7E8E12F
00000000  00000000
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409:             s0
```

  Conditions: Occurred on a Cisco 7200 running an internal build of Cisco IOS Release 12.2SX.

  Workaround: There is no workaround.

- CSCsm29120

  Symptoms: PIM neighbor times out on interface that was once configured as port-channel. This happens for both IPv4 and IPv6 multicast. This issue is consistently reproducible. If PIM times out, multicast traffic will not flow on the interface.

  Conditions: Occurs under the following scenario:

  1. Configure port-channel on Ethernet interfaces.
  2. Configure IPv4 and IPv6 address on the port-channel interface. PIM neighbor will be formed.
  3. Remove Ethernet interface from the bundle interface and configure a IPv4 and IPv6 address. PIM neighbor will timeout after 1 minute 45 seconds.

Workaround: Remove the interface from the port-channel, then perform a **shut/no shut**.

- CSCsm30569

  Symptoms: Packet is not being fragmented when packet size is greater than IPSEC tunnel MTU.

  Conditions: This issue is seen on routers running Cisco IOS Release 12.4T when IPSec is configured and Cisco Express Forwarding (CEF) is enabled. When CEF is disabled this issue is not seen.

  It occurs when packet size is greater than IPSec tunnel MTU. Packet is not being fragmented, however traffic is passing successfully.

  Workaround: There is no workaround.

- CSCsm36745

  Symptoms: SSM mapping may cause slow IGMP processing.

  When SSM Mapping for mapping IGMPv1/v2 reports to PIM-SSM is configured using **ip igmp ssm-map enable**, the IGMP process may slow down and not service all incoming reports and not send out periodic queries.

  Conditions: By default, when SSM mapping is configured, the router will try to resolve via DNS any mappings that are not statically configured. When the name server does not respond timely to the DNS lookups, which could be to non- or misconfiguration, name server down etc, other incoming IGMP reports will be delayed until the lookup has timed out. This also affects IGMP reports that are not supposed to be mapped.

  Workaround:

  - Create static mappings for all reports that are to be mapped
  - Make sure that all to be mapped IGMP reports are present in the configured name server
  - Disable DNS lookup using: **no ip igmp ssm-map query dns**

- CSCsm39308

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

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

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

- CSCsm44353

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

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

  Workaround: There is no workaround.

- CSCsm45483

  Symptoms: Configuring local switching with auto-provisioned VC for an ATM interface configured with cell-packing through vc-class, results in the crash of a Cisco 7600 router.

  Conditions: This symptom is observed on an ATM interface on ATM SPA on a Cisco 7600 platform.

  Workaround: There is no workaround.

- CSCsm47417

  Symptoms: W2:setting ceExtSysBootImageList cause **write memory** to work incorrectly.

Conditions: Occurs after setting ceExtSysBootImageList to a new boot image from SNMP. The new boot image in running-config is not copied to startup-config. Instead, a variable “d” will be copied to startup-config after the **write memory**. The **show bootvar** command will show BOOT variable = d.

Example:

```
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>getmany -v2c
10.64.68.138 public
ceExtSysBootImageList
ceExtSysBootImageList.2001 = disk1:s72033-adventerprisek9_dbg-vzsm47417test
ceExtSysBootImageList.2017 = disk1:s72033-adventerprisek9_dbg-vzsm47417test
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:4>setany -v2c
10.64.68.138 public
ceExtSysBootImageList.2001 -o "disk1:"
ceExtSysBootImageList.2001 = disk1:
-----------------------------------------------
7600-11-1#
00:02:56: %SYS-5-CONFIG_I: Configured from 10.64.71.240 by snmp
```

Workaround: There is no workaround.

- CSCsm53196

  Symptoms: Crash occurs at “ip_route_delete_common”.

  Conditions: Occurs under the following scenario:

  1. A multicast BGP route exists.
  2. A unicast BGP route exists for the same prefix.
  3. Another route covered by the same majornet as the BGP route exists.
  4. There are both iBGP and eBGP sources for the BGP prefix.
  5. Redistribution of BGP routes into an IGP must be configured.

  Topology change in network causes mBGP to switch from using the iBGP sourced route to the eBGP sourced route will cause the crash.

  Workaround: If there are not both iBGP and eBGP sources for the same route the problem will not occur. If redistribution of BGP Into an IGP is not configured the problem will not occur.

- CSCsm56940

  Symptoms: Traceback seen while doing Telnet with SSH enabled.

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

  Workaround: There is no workaround.

- CSCsm64307

  Symptoms: When PPP sessions are terminated, the standby NPE may crash. This is true for both PPP sessions that are terminated naturally (from the customer end), and those that are terminated prematurely (at the provider end due to a command such as **clear pppoe sessions all**).

  Conditions: At present the conditions are unknown. It only appears to impact Cisco IOS Release 12.2(31)SB10 and related releases.

  Workaround: There is no workaround.

- CSCsm70668

  Symptoms: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel.

  Condition: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel configured. In OIR “test mbus power 6 off” and “test mbus power 6 on” are performed followed by a microcode reload on slot 6.

  Workaround: There is no workaround.

- CSCsm71537

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

  Conditions: Occurs when OER is configured.

  Workaround: There is no workaround.

- CSCsm76792

  Symptoms: A standby supervisor power cycles over and over on boot up. The following errors are seen:

  ```
  %RF-SP-3-NOTIF_TMO: Notification timer Expired for RF Client: Cat6k Power(1318)
  ```

  Conditions: This has been experienced on a Catalyst 6500 with dual supervisors running Cisco IOS Release 12.2(33)SXH2a and Cisco IOS Release 12.2(33)SXH3.

  Workaround: There is no workaround.

- CSCsm92986

  Symptoms: The commands **show disk#** and **dir disk#** may fail after boot-up

  Conditions: The symptoms are observed immediately after boot-up.

  Workaround: Using either the **format disk#** or the **fsck disk#** commands will solve the problem.

- CSCso04657

  Symptoms: SSL VPN service stops accepting any new connections.

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

  Workaround: There is no workaround.

- CSCso09170

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

  ```
  %FABRIC_INTF_ASIC-DFC11-5-FABRICSYNC_DONE: Fabric ASIC 1 Channel 1: Fabric sync done.
  DFC11: policyq_entry 0x257AC25C already present<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  %LINEPROTO-DFC11-5-UPDOWN: Line protocol on Interface IBC3/0, changed state to up
  ```

  Conditions: Occurs because of the following factors:

  1. The unqueue operation is not clean, so when a policy-map is being pushed down more than once in one port-c, the error occurs.
  2. The policy-map is pushed down more than once, even though it is only programmed in one member link in a single port-c.

  Workaround: There is no workaround.

- CSCso15740

  Symptoms: The “set metric” clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

  Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

  Workaround: Avoid using “continue” in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso27236

  Symptoms: Cisco IOS CA shows incorrect renew date (Jan 1 1979). Example:

  ```
  Before restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 2008 09:58:00
  ```

  ```
  After restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 1970 08:00:00
  ```

  Conditions: Occurs when auto-enroll is enabled and the router is reloaded.

  Workaround: There is no workaround.

- CSCso28309

  Symptoms: Ping fails from reflector during internal testing.

  Conditions: The goal of the test is to verify the successful termination of PPP/PPPoE over ATM sessions on router’s ATM interface using auto sensing. It is performed with auth_pap, process switch, and keepalive disabled. This has a functional impact as the virtual access entry is not getting added to the routing table after doing clear ip route.

  Workaround: There is no workaround.

- CSCso29361

  Symptoms: The commands given in the **interface range** command may not be synced to all interfaces configured in the range in the standby supervisor.

  Conditions: Occurs when configuration commands are entered under **interface vlan range** command. They get attached to only the first VLAN in the range in the redundant supervisor. After switchover, traffic does not flow due to the missing VLAN configuration.

  Workaround: There is no workaround.

- CSCso30649

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

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

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

- CSCso35659

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

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

Workaround: Unconfigure and clear the VLAN.

- CSCso39171

  Symptoms: When issuing the **show mac-address-table** command for an interface with REP enabled on a Cisco 7609, the Telnet session hangs and the system becomes unresponsive for long periods of time until CPU drops.

  Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1 and when REP is configured.

  Workaround: Remove REP configuration.

- CSCso39217

  Symptoms: Link flaps and causes traffic loss as well as repeated route convergence on RP.

  Conditions: Seen When ESM20 is reset. During stateful switchover (SSO), though not consistent. After a SSO switchover, we see a PORT_BOUNCED error message which indicates the cause of failure as the Consistency Check IDB was down.

  Workaround: There is no workaround.

- CSCso40612

  Symptoms: Router is crashing due to random memory corruption in parser code.

  Conditions: The crash happens on only particular sequence and timing of configuration.

  Workaround: There is no workaround.

- CSCso46337

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

  Conditions: Occurs after SSO.

  Workaround: There is no workaround.

- CSCso49064

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

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

  Workaround: There is no workaround.

- CSCso50363

  Symptoms: When AAA authentication is from RADIUS and RADIUS debugs are enabled, the password (except for last two characters) for the users trying to login to the box appears in debug messages.

  Conditions: Occurs under the following scenario:

  1. Configure RADIUS server.
  2. Configure AAA authentication for login with RADIUS.
  3. Enable RADIUS debugs.
  4. Try to telnet to the router.

  Workaround: There is no workaround.

- CSCso52598

  Symptoms: The router may crash after the **no interface ethernet** *0/0.1* command is entered.

  Conditions: It could happen on a router with more than 4000 dynamic ARP entries.

  Workaround: Do not execute **no interface ethernet** *0/0.1*.

- CSCso56038

  Symptoms: The following error message may be seen:

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

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

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

  Workaround: There is no workaround.

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

- CSCso56196

  Symptoms: Updates are not being sent or withdrawn.

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

  ```
  PE1------UUT----PE2
  ```

  On UUT there are neighbors PE1 and PE2. If PE1 and PE2 are in same update group, the **show ip bgp all update-group** command will show that.

  Now there are a lot of updates being formatted and sent in the process. The **show ip bgp all replication** command would show the messages which are enqueud for sending out for particular update groups. At this moment, one neighbor goes to idle and is not coming up, then the new updates will not be formatted until the neighbor comes up.

  Workaround:

  1. Remove the idle neighbors of the update-group and add again.
  2. Clear the IP BGP neighbor that went idle.

- CSCso57185

  Symptoms: There is an incorrect rate for dLFI when using priority.

  Conditions:

  - When queueing policy is attached without any priority feature, everything is working fine.
  - As soon as queueing policy is attached that has a priority feature, packets are dropped at the receiver side. The drops at receiver side are seen as out- of-sequence frags/lost frags.
  - This is seen even if the original size of packets sent are less than configured fragment size.

  Workaround: There is no workaround.

- CSCso57602

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

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

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

- CSCso59251

  Symptoms: An interface on ESM20G goes down.

  Conditions: Occurs when the interface has a 50 EVC on it. Seen on router using rsp72043-adventerprisek9_wan_dbg-mz.srb_throttle_033008 image.

  Workaround: A **shut/no shut** will correct the symptom.

- CSCso59974

  Symptoms: BGP session goes idle.

  Conditions: Occurs following a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCso61347

  Symptoms: A router crashes.

  Conditions: The symptom is observed on a Cisco 7600 RP using the L2WAN system testbed with ATM dLFI under traffic. The L2WAN system testbed loads 100 VT interfaces over SIP200 and another 100 VT interfaces over SIP400. The QoS policy over the VT interface is essential for this crash scenario.

  Workaround: There is no workaround.

- CSCso64050

  Symptoms: Policy-map outputs are not seen in standby router. The policy is attached to the VC in the standby, but no output is seen.

  Conditions: The symptom is observed when an ATM PVC is created and a service policy is attached to the PVC.

  Workaround: There is no workaround.

- CSCso68580

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

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

  Workaround: There is no workaround.

- CSCso71312

  Symptoms: The **ancp** command is not recognized by the Cisco IOS Software running on a Cisco 10000 Series PRE4.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SB running on a Cisco 10000 Series PRE4.

  Workaround: There is no workaround.

Further Problem Description: The “ancp” subsystem was missing in Cisco IOS Release 12.2(33)SB for a Cisco 10000 Series PRE4.

- CSCso71955

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

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

  Workaround: Disable netflow if possible.

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

- CSCso84567

  Symptoms: Non-TCP traffic passing through the device is punted to the control plane policer. When Control Plane Policing (CoPP) is configured, the bridge result is changing to policy route because WCCP is being applied to all IP packets of a WCCP service.

  Conditions: Both WCCP and CoPP must be enabled for this issue to occur.

  Workaround: There is no workaround.

- CSCso87083

  Symptoms: Router crashes.

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

  Workaround: There is no workaround.

- CSCso87916

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

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

  Workaround: There is no workaround.

- CSCso88138

  Symptoms: When there is a link flap or a reload, RSVP shows that the interface is down while actually the interface is up. Because of this, the tunnel may take a backup path even when the interface is up.

  Conditions: Unknown at this time.

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

- CSCso88616

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

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

  Workaround: There is no workaround.

- CSCso88718

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

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

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

- CSCso90058

  Symptoms: MSFC crashes with Red Zone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCso90970

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

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

  Workaround: There is no workaround.

- CSCso93296

  Symptoms: IPv6 rate limiters do not drop multicast packets

  Conditions: Occurs when multicast is not enabled.

  Workaround: Enable multicast routing.

- CSCso95426

  Symptoms: In each retransmit, the AAA client explicitly shows the radius-key in the debug output, causing security concerns.

  Conditions: Occurs when RADIUS debugs are enabled, such as **debug radius all**.

  Workaround: There is no workaround. However, this is not know to impact functionality.

- CSCso97318

  Symptoms: PPPoE over VLAN over ATM functionality is broken

  Conditions: This is resulting in both PPPoE client (Cisco PPPoE test driver) and PPPoE server caching wrong PPPoE encapsulation string (with double VLAN tag). LCP CONF request from each side is not properly processed by the peer, so the session never comes up.

  Workaround: There is no workaround.

- CSCso97695

  Symptoms: Config replace used to fail with TFTP.

  Conditions: No special conditions.

  Workaround: TFTP copy worked fine. The workaround is to copy it and then do a config replace from the disk.

- CSCsq04355

  Symptoms: Customer mistakenly modified the service module SPAN session which caused high CPU on the switch. This caused the interface to flap, bringing down Hot Standby Routing Protocol (HSRP), Open Shortest Path First (OSPF) and other protocols resulting in an outage.

  Conditions: Occurs when manipulating the service module SPAN session:

  ```
  LAB1(config)#monitor sess 1 source vl 2028
  ```

```
 % Session 1 used by service module

LAB1(config)#no monitor sess servicemodule

LAB1(config)#do sh mon

Session 2

---------

Type                   : Local Session

Source Ports           :

    Both               : Gi2/2

Destination Ports      : Gi3/2


LAB1(config)#monitor sess 1 source vl 2028

LAB1(config)#do sh mon

Session 1

---------

Type                   : Local Session

Source VLANs           :

    Both               : 2028


Session 2

---------

Type                   : Local Session

Source Ports           :

    Both               : Gi2/2

Destination Ports      : Gi3/2
```

Workaround: Do not modify or change the SPAN session related to the service module using the session number. Instead use **no mon session servicemodule** in order to remove the session.

- CSCsq05997

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

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1,

  -Traceback= 0x61013944 0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C Because
  the message is generated frequently, the log file may fill up too soon.
  ```

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

  Workaround: There is no workaround.

- CSCsq06754

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

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

  Workaround: The crash is not seen in following cases:

  1. With continuous traffic flow, shutdown the interface before OIR and give “no shut” once OIR process is over.

  2. When reloading the router with continuous traffic flow.

- CSCsq08625

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

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

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

- CSCsq14031

  Symptoms: Unable to ping IP address of session target. Packets of certain sizes (between 57 and ~63 bytes, depending on the type of packet) are corrupted when using a tunnel over a PPP multilink interface. EIGRP packets were within this range and so were dropped and caused the route to the IP address being pinged not to be added.

  Conditions: Issue may be related to encryption or Network Address Translation (NAT).

  Workaround: Disable or increase the value of **ppp multilink fragmentation**.

- CSCsq14261

  Symptoms: Downstream traffic will drop when we send IPv6 traffic over PPPoE sessions.

  Conditions: Bring up a PPPoE session over L2TP tunnel for address negotiated by IPv6, then send downstream IPv6 traffic.

  Workaround: There is no workaround.

- CSCsq15198

  Symptoms: When all uplink ports on SUP are admin down and a **no shut** is entered on any of the two uplink ports, BFD sessions running on a different LC on the chassis begin flapping.

  Conditions: This occurs whenever the first of two uplink ports is brought up.

  Workaround: There is no workaround.

- CSCsq17712

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

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

  Workaround: There is no workaround.

- CSCsq24935

  Symptoms: A switch reloads when the **distance bgp** command is configured under ipv6 address family.

  Conditions: This symptom is observed on a Cisco 3560 that is running Cisco IOS Release 12.2(44)SE2. The same symptom is also seen on a Cisco 3750. The following commands are issued:

  ```
  router bgp <>
   address-family ipv6 unicast
   distance bgp <> <>
  ```

  The router subsequently reloads because of an Instruction access Exception.

  Workaround: There is no workaround. BGP/ipv6 is not supported on such platforms.

- CSCsq29052

  Symptoms: Packets are not forwarded out from a point-to-point (P2P) interface.

  Conditions: The symptom is observed with CEF enabled and when the P2P interface is changed from an “ip unnumbered” configuration to another interface.

  Workaround: There is no workaround.

- CSCsq30261

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

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

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

- CSCsq30401

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

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

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

- CSCsq33677

  Symptoms: PPPoE sessions in relay mode got stuck in attempting state.

  Conditions: This symptom is observed on a Cisco router running an internal build of Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsq39180

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

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

Workaround: Reload the router.

- CSCsq40845

  Symptoms: Removing an IPv6 access-list via the **no ipv6 access-list** command when referencing the same ACL name using the **debug ipv6 packet access-list** command may reload the router.

  Conditions: The symptom is observed when **debug ipv6 packet access-list** is configured.

  Workaround: Disable debug “un all” before removing an access-list from the router configuration.

- CSCsq42288

  Symptoms: Scalable Ethernet over MPLS configuration and EVC configuration may not work sometimes. For Scalable EoM, the xconnect configuration has to be under SIP-400 Gig Ethernet main or sub-if.

  Conditions: Occurs under the following scenario:

  - some routes are learned from an IPv4 BGP session with the VC destination
  - the same routes are learned over an IGP session as well
  - initially the routes will be IGP because of better administrative distance
  - if the IGP session flaps, the routes will become BGP routes with VC destination being the BGP next-hop address.
  - when this happens this might break the VC connectivity.

  Workaround: Execute **clear ip route** *VC’s destination address* when the problem is seen.

- CSCsq42885

  Symptoms: Line card crashes recurrently with the “Address exception error”.

  Conditions: The issue is seen when entering the **no shutdown** command on the spatial reuse protocol (SRP) interface.

  Workaround: There is no workaround.

- CSCsq44823

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

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

  Workaround: There is no workaround.

- CSCsq48497

  Symptoms: When ingress policy map with policing action is attached to an EVC and then the **default int x/y/z** command is entered, the ingress policing does not get cleared from the hardware. When the same EVC is configured on that interface, then even without any ingress policy applied, the earlier configured policing is enabled.

  Conditions: Occurs on a ES20 interface with EVC configured. After doing the steps as above policing still works on EVC.

  Workaround: Reapply the ingress policy again on EVC, then remove the policy.

- CSCsq51378

  Symptoms: ATM PA Interface with no cables connected shows up/up after forced redundancy.

  Conditions: Occurred under the following scenario:

  - No cables attached to Fast Ethernet or ATM interface.
  - Issue **no shut** on interface.
  - The **show ip int brief** command shows interface status up/protocol down.
  - After **redundancy force** command is entered, interface shows up/up (no cables connected).

  This affects Fast Ethernet interfaces and ATM interfaces on WS-x6582-2PA/PA-2FE-TX and PA-A3-OC3-MM. It does not affect Supervisor ports or Serial Interfaces.

  Workaround: There is no workaround.

- CSCsq52836

  Symptoms: VLAN database is lost

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

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

- CSCsq53542

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

  Conditions: Occurs when multicast routing is enabled in the default mode.

  Workaround: If there are no mStatic or mBGP routes, the following configuration will avoid the problem:

  ```
  Router(config)#ip multicast rpf multitopology
  Router(config)#global-address-family ipv4 multicast
  Router(config-af)#topology base
  Router(config-af-topology)#use unicast base
  Router(config-af-topology)#
  ```

- CSCsq55691

  Symptoms: QoS with Link Fragmentation and Interleaving (LFI) over ATM does not work.

  Conditions: Occurs after a **shut/no-shut** on the ATM interface

  Workaround: Reload the line card on both ends.

- CSCsq58385

  Symptoms: Cannot ping Hot Standby Routing Protocol (HSRP) virtual address when active on ES20 card.

  Conditions: This symptom is observed on a Cisco 7600 series router with SUP720, ES20 and running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsq60016

  Symptoms: A router crashes after a long RSA key string is entered.

  Conditions: This symptom is observed when a very long hex string is entered.

  Workaround: Break the entry into shorter strings.

- CSCsq66506

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

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

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

- CSCsq68600

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

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

  Workaround: There is no workaround.

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

- CSCsq73498

  Symptoms: Three MultiOS IPC processes: ciscoipc, ipc_test_admin_proc, and ipc_test_driver_proc fail with “IPC Error: send msg[3] failed ; Error - timeout” or “RPC message timed out”.

  Conditions: This symptom occurs if an open IPC port is closed before the RPC response arrives.

  Workaround: Reload the router where IPC master is running.

- CSCsq76166

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

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

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

- CSCsq78100

  Symptoms: On a LAN card if **wrr-queue cos-map** is changed on a port that is never up, some packets are dropped on another port.

  Conditions: Occurs under the following scenario:

  1. WRED is disabled in the port that is sending traffic.
  2. Configure **wrr cos-map** on another port that is never up.

  Workaround: Configure **wrr cos-map** only after the port is **no shut**.

- CSCsq80589

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

  The following error message is seen:

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

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

Workaround: There is no workaround.

- CSCsq84238

  Symptoms: Unable to perform SVC download of post-paid tariff switch TC service.

  Conditions: On attempting to bring up a l2-connected, unclassified-mac initiated IP session and having it autologon to a TC service profile, which has post-paid tariff switching configured as part of its profile, the service is not activated.

  Workaround: There is no workaround.

- CSCsq84624

  Symptoms: A Cisco router might crash when **debug condition portbundle ip 10.1.1.1 bundle 0** is configured.

  Conditions: Occurs when this command is executed prior to configuring **ip portbundle**.

  Workaround: There is no workaround.

- CSCsq84670

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

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

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

- CSCsq89329

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

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

  Workaround: There is no workaround.

- CSCsq92440

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

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

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

- CSCsq97167

  Symptoms: IP multicast traffic drops every 100 seconds.

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

  Workaround: There is no workaround.

- CSCsq97517

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

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

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

- CSCsq98626

  Symptoms: On a Cisco 7600 configured for ATM Circuit Emulation (CEM) over MPLS, there are errors reported under the CEM circuit. This is observed using the **show cem circuit** command.

  Conditions: The error is only observed when the core-facing interface has these characteristics:

  - SVI i.e L2 (Bridge-domain and Switchport)
  - The physical interface is from a ES20 module

  Workaround: Disable MAC address aging with the **mac-address-table aging-time 0** command.

- CSCsq99447

  Symptoms: None of the BFD sessions come up.

  Conditions: The symptom is observed when BFD is configured with EIGRP for more than 32 VRFs.

  Workaround: Bring the total VRFs on which BFD is configured for EIGRP to less than 32 and reload the router.

  Further Problem Description: In EIGRP, each VRF is counted as a single BFD client whereas in other protocols, the BFD client count is shown as one per protocol. This limits the number of EIGRP/BFD sessions allowed to be configured.

- CSCsr05501

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

  ```
  "% NBAR Error: hwidb could not found"
  ```

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

  Workaround: There is no workaround.

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

- CSCsr06094

  Symptoms: A Cisco router may ungracefully reload.

  Conditions: The symptom is observed when the router is processing CoA RADIUS messages and when certain debugs are turned on.

  Workaround: Disable all debugs.

- CSCsr06707

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

  Conditions: Occurs when duplicated BGP router-id is received

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

- CSCsr08750

  Symptoms: A router may crash.

  Conditions: The router will crash with IO memory corruption when the **memory reserve critical [1-5]** command is executed.

  Workaround: Configure the **memory reserve critical** command with a much greater size.

Further Problem Description: This issue occurs only when the ratio of free processor memory and free IO memory is high (say greater than 90).

- CSCsr08921

  Symptoms: Cisco 7600 RP crashes when pseudo-wire is down for ATM over MPLS over GRE and when AAL0 encapsulation is used. The problem happens in customer-facing SIP-400 line card.

  Conditions: Configure ATM AAL0 over MPLS over GRE, then bring the pseudo-wire down.

  Workaround: There is no workaround.

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr11085

  Symptoms: A single route loop whose gateway is covered by a default route remains in the RIB after a more specific route which resolves the gateway is removed. For example, the following routes may exist in the RIB:

```
S*    0.0.0.0/0 is directly connected, Ethernet1/0
 S     192.168.0.0/16 [1/0] via 192.168.1.2
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C        192.168.1.0/24 is directly connected, Ethernet0/0
 L        192.168.1.1/32 is directly connected, Ethernet0/0
       192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C        192.169.1.0/24 is directly connected, Ethernet1/0
 L        192.169.1.1/32 is directly connected, Ethernet1/0
```

  If interface eth 0/0 goes down, then we have the following:

```
S*    0.0.0.0/0 is directly connected, Ethernet1/0
 S     192.168.0.0/16 [1/0] via 192.168.1.2
       192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C        192.169.1.0/24 is directly connected, Ethernet1/0
 L        192.169.1.1/32 is directly connected, Ethernet1/0
```

  and

```
Router#show ip route loop
 ->default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2 static 00:01:07 N
```

  In this case the route

```
S     192.168.0.0/16 [1/0] via 192.168.1.2
```

  should be removed from the RIB.

  Conditions: The default route MUST be present in order for the above behavior to be considered wrong. If a default route is NOT present then the route

```
S 192.168.0.0/16 [1/0] via 192.168.1.2
```

is a misconfiguration and must be corrected by altering the configuration. Until the configuration is corrected, the route will remain in the RIB and traffic covered by that route will be dropped.

Workaround: The one route loop can be removed from the RIB using the **clear ip route** command:

```
clear ip route 192.168.0.0
```

Further Problem Description: In the absence of the default route removal of the one route loop can lead to oscillation, which would seriously degrade the performance of the router.

- CSCsr11099

  Symptoms: Ping fails on port-channel subinterface.

  Conditions: Routers R1, R2 connected back to back and configured as shown below. When the active link goes down or is shut, the hot standby becomes active. At this point a ping between the routers fails.

  The following conditions are necessary:

  – **lacp fast-switchover** is configured on the port-channel interface
  – Either **encapsulation dot1q** or **encapsulation isl** is configured on the port-channel subinterface
  – There is only one active link

  Releases affected: Cisco IOS Release 12.2SRC

```
R1                  R2
---                  ---
gi2/0/1 ------- gi2/0/1
gi2/0/2 ------- gi2/0/2

R1 config:
interface Port-channel1
 no ip address
 lacp fast-switchover
 lacp max-bundle 1

interface Port-channel1.1
 encapsulation dot1Q 38
 ip address 10.1.3.1 255.255.255.0

interface GigabitEthernet2/0/1
 no ip address
 no mls qos trust
 channel-group 1 mode active

interface GigabitEthernet2/0/2
 no ip address
 no mls qos trust
 channel-group 1 mode active

R2 config:
interface Port-channel1
 no ip address
```

```
 lacp fast-switchover
 lacp max-bundle 1

interface Port-channel1.1
 encapsulation dot1Q 38
 ip address 10.1.3.2 255.255.255.0

interface GigabitEthernet2/0/1
 no ip address
 no mls qos trust
 channel-group 1 mode active

interface GigabitEthernet2/0/2
 no ip address
 no mls qos trust
 channel-group 1 mode active
```

Workaround: Do not configure **lacp fast-switchover**.

Further Problem Description: This occurs because the encapsulation assigned to the new active link is set to the default “native” rather than the encapsulation configured on the port-channel subinterface. Therefore, this will cause connectivity issues even with non-routed port-channel subinterfaces.

- CSCsr17660

  Symptoms: PE-CE performance degradation of 80% on initial convergence.

  Conditions: Occurs when BGP and VPNv4 are configured.

  Workaround: There is no workaround.

  Further Problem Description: Performance is not affected after initial convergence.

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This issue is observed when sending request to particular server on a server-group.

  Workaround: There is no workaround.

- CSCsr18500

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

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

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

- CSCsr18589

  Symptoms: A Virtual Router Redundancy Protocol (VRRP) group configured on a VLAN interface flaps from the backup to the master state after stateful switchover (SSO) when the existing master is still available on the network. The group will flap back to backup a short period later.

  Conditions: The problem only occurs when there are a large number of VLAN interfaces with a VRRP group configured on each interface and SSO is performed.

Workaround: Each of the VRRP groups can be configured with a larger VRRP advert timer value. Values should be varied depending on the setup, but a larger than default value is usually required.

- CSCsr20566

  Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

  Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

  Workaround: There is no workaround.

- CSCsr26025

  Symptoms: When “0.0.0.0/8 static route to null 0” is configured, the default gateway failover does not work. RIB is not updated.

  Conditions: Occurs under the following scenario:

  - Border Gateway Protocol (BGP) with two neighbors sending a default gateway.
  - Static route “0.0.0.0/8 to null 0” is configured.
  - Failover takes place and RIB is not updated.

  Workaround: There is no workaround.

- CSCsr27734

  Symptoms: The standby router crashes.

  Conditions: This symptom is observed when a service-policy map is removed from a VC.

  Workaround: There is no workaround.

- CSCsr27794

  Symptoms: BGP does not generate updates for certain peers.

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

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

- CSCsr27980

  Symptoms: When adding a class into existing policy-map and the total bandwidth exceeds system defined limits, it gets accepted in MQC. On removing another class from the same policy map, tracebacks are thrown, and the system is hogged completely.

  Conditions: This symptom is seen when the total bandwidth for the classes exceeds the platform defined limits.

  Workaround: There is no workaround.

- CSCsr29468

  Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml.

- CSCsr40433

  Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in “RSVP signaling proceeding”.

  Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

  Workaround: Use strict next hop addresses.

- CSCsr41079

  Symptoms: Error message seen after stateful switchover (SSO):

  ```
  %CHKPT-4-NOMESSAGE: Message is NULL, (Cannot get data ptr)
  ```

  Conditions: Occurs when Intermediate System-to-Intermediate System (IS-IS) NSF is configured.

  Workaround: There is no workaround.

- CSCsr43461

  Symptoms: Some configurations are missing after a reload.

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

  Workaround: There is no workaround.

- CSCsr43800

  Symptoms: Router crashes on executing **vrf upgrade-cli multi-af-mode non-common-policies vrf**.

  Conditions: Occurs when **ip vrf X** is configured on an interface and execute and the **vrf upgrade-cli multi-af-mode non-common-policies vrf X** command is entered. Observed in a Cisco 7200 running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsr44005

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

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

  Workaround: There is no workaround.

- CSCsr45502

  Symptoms: A router intermittently runs into crashes in a large scale network with active PPPoEoA sessions.

  Conditions: This symptom occurs when many active PPPoEoA sessions exist.

  Workaround: There is no workaround.

- CSCsr45986

  Symptoms: The memory of the router may become corrupted, which can lead to a crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a record that has a large packet section in it, and it is applied to capture traffic.

  Workaround: Configure Flexible NetFlow with a flow record that does not have a packet section in it.

Further Problem Description: Tracebacks are observed when the following commands are issued, which leads to a Flexible NetFlow crash.

```
configure terminal
 flow monitor mm_1
 record netflow ipv4 as
 interface Ethernet1/0
 ip flow monitor mm_1 input
 end
```

- CSCsr49316

  Symptoms: A crash happens when the **show ipv6 rpf x:x:x::x** command is given.

  Conditions: This symptom is observed only when there are more than 16 adjacencies for a single static route. The crash happens when the **show ipv6 rpf** command is given for this particular static route.

  Workaround: There is no workaround. This problem occurs as long as there are more than 16 adjacencies for single static route even if some of them are not active.

- CSCsr49701

  Symptoms: Router may reset after removing a large VPN routing/forwarding (VRF) configuration.

  Conditions: Occurred on a Cisco 10000 Series Router running Cisco IOS Release 12.2(33)XNA following the removal of a VRF with 200,000 routes.

  Workaround: The issue does not occur when a VRF of 160,000 routes was removed. Do not allow the number of routes to exceed this number.

- CSCsr50134

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

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

  - Primary path FRR cutover
  - Primary path's interface flaps
  - FRR configuration is changed

  Workaround: Avoid FRR configuration changes.

- CSCsr50821

  Symptoms: A router may crash when ARP hits through interrupt level.

  Conditions: This symptom is observed when bridging is configured, but it may also be observed when the ARP code hits by interrupt context, which is unpredictable.

  Workaround: There is no workaround.

  Further Problem Description: This defect was introduced via CSCsq05997. Cisco IOS Release 12.4 and 12.4T are not affected by this defect, but Cisco IOS Release 12.2S may be affected by this defect.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr53059

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

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

  Workaround: There is no workaround.

- CSCsr53264

  Symptoms: A software-forced crash occurs on the RP of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB2.

  Conditions: Occurs when the clear route-map counters <name> command is entered.

  Workaround: Upgrade to Cisco IOS Release 12.2(33)SRC3 or later.

- CSCsr55713

  Symptoms: A crash occurs.

  Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

  Workaround: There is no workaround.

- CSCsr55865

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

  Conditions: This symptom applies to marking using **set** command. The **police** command works as expected.

  Workaround: Use a different image.

- CSCsr55990

  Symptoms: HSRP virtual MAC is dynamic instead of static on a Cisco 7600 after a reload.

  Conditions: HSRP is configured under a routed vlan-based pseudowire:

  interface Vlan X ip address 10.0.0.1 255.255.255.0 standby 1 ip 10.0.0.254 xconnect x.y.z.w encapsulation mpls

  Occurs when fast millisecond HSRP timers are used, and an HSRP interface delay is not configured.

  Workaround: Perform a **shut/no shut** on the interface “vlan X”. Or, as a preventive action, configure **standby delay minimum 60** on the interfaces. Testing has shown that after a reboot the entry is installed correctly in the PFC/DFC.

- CSCsr56465

  Symptoms: Line card MAC notification test fails when redundancy mode is changed from RPR to SSO or SSO to RPR. SIP-400 Bus Connectivity Test failed when the following commands are issued:

  Conf t redundancy mode rpr

  Conditions: The issue observed in the Fabric Hot Sync-enabled Sup720 and RSP720 routers Cisco IOS Release 12.2(33)SRC. In the problem state, Super Santa Ana (SSA) channels are out of sync. For example, **show platform hard ssa status** will display SSA channel status from the SSA based CWAN module console.

Workaround: There is no workaround.

- CSCsr59719

  Symptoms: A router may crash soon after configuring **cns config initial**.

  Conditions: The symptom is observed when configuring **cns config initial** with an invalid IP address for the status URL, for example:

  router(confif)#cns config initial <any non-existent ip address> status http://1.1.1.1.1.1.1/junk

  When the connection to the initial server fails, the status message is posted to the status URL which will cause the router to crash if the IP address is invalid.

  Workaround: Ensure the configured ip-addresses are valid.

- CSCsr60252

  Symptoms: MPLS Layer 3 VPN with HQOS on PA-A6-OC3 with 500 ATM PVCs crashes at PEs with online insertion and removal (OIR).

  Conditions: Perform a soft OIR of PE while entering the **hw-module slot 5 start** command to observe the crash.

  Workaround: Configure with HQoS for 500 PVCs.

- CSCsr60789

  Symptoms: Occasionally a crash occurs after preemptive switchover with no traffic.

  Conditions: Unknown. Issue is not reproducible on a consistent basis.

  Workaround: There is no workaround.

- CSCsr62803

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

  Conditions: Occurs while attempting to establish a session to the processor. It fails with the following message:

  ```
  % IP routing table __Platform_iVRF:_ID00_ not accessible
  ```

  Workaround: There is no workaround.

- CSCsr64361

  Symptoms: A Standby supervisor or VSS system may continuously reload and display the following message:

  ```
  %RF-SW2_SP-3-NOTIF_TMO: Notification timer Expired for RF Client: SNMP RF Client
  The reload reason may be given as "Peer Reload Request".
  ```

  Conditions: The symptom is observed with dual supervisors or a VSS system.

  Workaround: There is no workaround.

- CSCsr65230

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

  Conditions: Occurs with SIP400 and channelized SPA interfaces.

  Workaround: There is no workaround.

- CSCsr66286

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

  ```
  Po1 : rep block port -2 vlan 6-10
  ```

```
"show int trunk" results as below.

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

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

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

Workaround: Disable boundary VLANs.

- CSCsr67177

  Symptoms: A router may experience a corner case crash if an IPv6 OSPF router is removed from the configuration.

  Conditions: The following conditions must be met before router is removed from the configuration to experience the system crash: OSPFv3 router does not run because the router-id is not available (it means that no IP address is available and/or router-id is not configured). SW interface is configured, assigned under inactive OSPFv3 router, and later removed using the **no interface** command.

  Workaround: Ensure that when the IPv6 router is configured it runs properly (if it does not start, there is a warning printed on the console advising what action to take).

- CSCsr68497

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

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

  Workaround: There is no workaround.

- CSCsr70963

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

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

  Workaround: There is no workaround.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr81271

  Symptoms: A Cisco 7600 router with PA-A3-T3 port adapter in flexwan module WS-X6582-2PA could generate following error messages with tracebacks upon a mass ATM PVCs flap:

  ```
  SLOT 2/0: %CWAN_ATM-3-VC_OR_PORT_ERR: Invalid VCD FF03 or Port: 0
  -Traceback= 403E2200 403A8C1C 40344F88 40347FD0 403481B4 403C374C 401CD170
  ```

  Slot 2/0 is the slot the port adapter is installed.

  Conditions: This seems to only occur when a large number of ATM PVCs flap, most likely from the service provider side.

Workaround: There is no workaround.

- CSCsr82003

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

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

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

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

- CSCsr82785

  Symptoms: If APS is configured on a large number of channelized sub-interfaces associated with a single controller such that a single failure can cause all of these interfaces to failover at the same time, and RIP is configured to run over these interfaces, high sustained CPU usage will be seen following the failover and reconvergence time will be lengthy.

  Conditions: Large number of APS protected interfaces fail over at the same time. RIP is the protocol running on those interfaces. IP addresses on all interfaces are covered by the same network statement.

  Workaround: There is no workaround.

  Further Problem Description: The length of the high CPU and reconvergence period will increase as the number of impacted interfaces increases.

  The length of the high CPU and reconvergence period will also increase as the number of network statements which cover the IP addresses on the affected interfaces decreases i.e. it will be worst when a single classful network (e.g. 10.0.0.0) covers all interfaces, somewhat better when multiple classful networks are impacted.

- CSCsr82895

  Symptoms: When a router has many PPPoE sessions and the router is configured as an RP-mapping agent, the router crashes following a switchover.

  Conditions: The symptom is observed when the router has 8000 PPPoE sessions and it is configured as an RP-mapping agent. Following a switchover, the issue is seen.

  Workaround: Another router that does not have as many interfaces in the network should be configured as the RP-mapping agent.

- CSCsr84639

  Symptoms: After 30 minutes, MIB synchronization failure messages appear on primary RP. Secondary RP crashes.

  Occurs under the following scenario:

  1. Bring up 1 pppox session on the L2TP network server (LNS)
  2. Pass bidirectional traffic through the LNS
  3. After 30 minutes, MIB sync failures message appear on primary RP and secondary RP crashes.

  Workaround: Enter the **no snmp mib notification-log default** command.

- CSCsr86515

  Symptoms: Router crashes due to watchdog timeout in the virtual exec process:

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (129/17),process = Virtual Exec.

  -Traceback= 40B5D8A8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
  420AA5A0 4054C05C 420570D8 40575510 41257298 41257284 %SYS-2-WATCHDOG: Process
  aborted on watchdog timeout, process = Virtual Exec.

  -Traceback= 40B5D8C8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
  420AA5A0 4054C05C 420570D8 40575510 41257298 41257284
  ```

  Conditions: This was observed on a Cisco 7600 with Supervisor 720 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

  Workaround: There is no workaround.

- CSCsr86826

  Symptoms: A standby SP may experience a memory leak in the mls-hal-agent process.

  Conditions: This has been experienced on a Cisco 7600 router with dual SUP720s running either Cisco IOS Release 12.2(33)SRC or Cisco IOS Release 12.2(33) SRC1. The router is configured for multicast.

  Workaround: There is no workaround.

- CSCsr92184

  Symptoms: Traffic drops after VLAN change on interface configured with single VLAN BCP.

  Conditions: Unconfiguring and configuring scaled single VLAN BCP configuration with heavy traffic running can cause this to happen.

  Workaround: Perform a **shut/no shut** on all interfaces.

- CSCsr96042

  Symptoms: ASR1000 Router crashes.

  Conditions: Occurs if “ip vrf” is deleted from the configuration.

  Workaround: There is no workaround.

- CSCsr97343

  Symptoms: An MSDP peer may flap randomly.

  Conditions: The symptom is observed when the device is configured with **logging host** *ip-address* ... or **logging host** *ip-address*.

  Workaround: It has been observed that removing the “logging host” configuration helps in preventing the peer-flap: **no logging host** *ip-address* **no logging** *ip-address*

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

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

- CSCsr98731

  Symptoms: If running OSPF, stale routes may be installed in the RIB. Also wrong paths (inter-area vs intra-area) are preferred.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsr99533

  Symptoms: Lawful Intercept (LI) may not work when accelerated LI feature is used and LI replication is being done by the supervisor card.

  Conditions: Occurs on a Cisco 7600 configured with a RSP720 supervisor card.

  Workaround: Use SIP400 as accelerated LI module.

- CSCsr99933

  Symptoms: Routers running Cisco IOS Release 12.2(33)SRB4 experiencing high CPU usage.

  Conditions: Occurs with high purge rate of 180/sec and above.

  Workaround: There is no workaround.

- CSCsu02975

  Symptoms: Router crashes due to memory corruption.

  Conditions: WAN router crashes when feature combination includes Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC The issue is seen only when frame-relay fragment and service-policy is part of map-class frame-relay configurations.

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configurations.

- CSCsu04360

  Symptoms: Acct-Time-Delay and Tunnel-Link-Stop records are missing from L2TP network server (LNS).

  Conditions: Occurs when using radius server for authentication.

  Workaround: There is no workaround.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4 byte CE is peered to a 2 byte capable PE using AS 23456 and the command **as-override** is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use “allowas-in” on the CE.

- CSCsu09663

  Symptoms: Router crashes when scaling DHCP sessions on Cisco Intelligent Services Gateway (ISG).

  Conditions: When the MCP-ISG is acting as DHCP Relay Agent or DHCP server, it crashes while large number of Layer 2-connected sessions are coming up.

  Workaround: There is no workaround.

- CSCsu10229

  Symptoms: cdpCacheAddress(OID:1.3.6.1.4.1.9.9.23.1.2.1.1.4) MIB is not showing GLOBAL_UNICAST address.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu12040

  Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

  Conditions:

  neighbor xxx as-override neighbor xxx send-label

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

  Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu23152

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

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

  Workaround: Reload the router and unconfigure the VFI.

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

  Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map): 1) **neighbor x.x.x.x soft-reconfiguration inbound** 2) **neighbor x.x.x.x weight** 3) **neighbor x.x.x.x filter-list in**

  If any one of the commands is not configured, then the router will not crash.

  Workaround: Configure route-map instead of filter-list for inbound direction. For example:

  `"neighbor x.x.x.x filter-list 1 in" replace with "neighbor x.x.x.x route-map` *`name`* `in"`

  where, route-map *name* permit 10 match as-path 1.

- CSCsu26315

  Symptoms: Traffic may not resume on ATM over MPLS (ATMoMPLS) connections.

  Conditions: The symptom is observed when both ATMoMPLS and ATM over LS (ATMoLS) connections are on same card and a card reset is done.

  Workaround: Reload the PXF.

- CSCsu27843

  Symptoms: Router crashes when DHCPv6 is configured on the router.

  Conditions: Router crashes when we remove the subinterface on which DHCPv6 PD request was configured.

  Workaround: There is no workaround.

- CSCsu27888

  Symptoms: IGMP v3 reports are discarded.

  Conditions: Occurs on Cisco 7200 router running Cisco IOS Release 12.4(20)T2.

Workaround: There is no workaround.

- CSCsu31954

  Symptoms: A router reloads.

  Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

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

  Workaround: Do not use EIGRP to redistribute BGP.

- CSCsu36836

  Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting “would wait forever”.

  Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

  Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu39704

  Symptoms: Unable to configure pseudowire on virtual-PPP interface. Command is rejected with the following error:

  ```
  Incompatible with ip address command on Vp1 - command rejected
  ```

  Conditions: Occurs when IPv4 address or IP VPN routing/forwarding (VRF) has already been configured on the main interface.

  Workaround: There is no workaround.

- CSCsu40667

  Symptoms: A Cisco 7600 series router may fail to install some NetFlow entries even if NetFlow table utilization is low.

  Conditions: Occurs while flows are ingressing on ES20 module.

  Workaround: There is no workaround.

  Further Problem Description: The **show mls netflow table-contention detail** command will show a heavy ICAM table utilization, while TCAM utilization is small.

  ```
  Router#<CmdBold>sh mls net table-contention det<noCmdBold>

  Earl in Module 1

  Detailed Netflow CAM (TCAM and ICAM) Utilization

  ================================================

  TCAM Utilization             :   0%
  ```

```
ICAM Utilization             :   98%

Netflow TCAM count           :   152

Netflow ICAM count           :   126

Netflow Creation Failures    :   388663

Netflow CAM aliases          :   0
```

- CSCsu42078

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

  Conditions: This happens when a service-policy is applied to an interface, and then service-policy is removed under certain conditions.

  One such condition is that “ip cef distributed” was configured on the router and the multi-link member flap triggered the service policy removal.

  The problem is that, after the policy was removed, the packet path vector was not reset correctly and still trying to access the already-removed policy internally. When traffic flows, it will cause crash.

  Workaround: For the above example, remove “ip cef distributed” from the configuration.

- CSCsu42315

  Symptoms: When the L3VPN prefix uses a tunnel with fast reroute (FRR) protection, there is traffic loss during reoptimization.

  Conditions: Not all prefix in the VRF will observe this issue. This is seen only when there are more than 250,000 prefixes.

  Workaround: There is no workaround.

  Further Problem Description: Traffic loss during re-optimization can be due to faster tunnel cleanup also. It is advisable to configure **mpls traffic-eng reoptimize timers delay cleanup** <*seconds*> to fine tune the cleanup according to the topology.

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

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

  Workaround: There is no workaround.

- CSCsu46822

  Symptoms: When account logon is done for a DHCP user, QoS policies defined in the user profile are not applied to the ISG session.

  Conditions: A DHCP session is created. User performs account logon via SESM (not CoA). User profile has QoS polices defined. Session is authenticated but policies are not applied to the session.

  Workaround: Perform account logon using CoA.

- CSCsu48898

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

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

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

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

  Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsu51245

  Symptoms: Port-channel QinQ subinterface on ESM20 and SIP600 line cards do not pass traffic after router reload and line card reset.

  Conditions: This condition is seen after router reload or member link line card reset. This is not seen when configuration is newly applied.

  Workaround: To recover from the condition, perform a **shut/no shut** on the port channel main interface.

- CSCsu54801

  Symptoms: IPv6/IPv6 Tunnel adjacency information is incomplete on the line card. This prevents IPv6/IPv6 multicast traffic on the tunnel.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu55883

  Symptoms: With MLPPP configured on OSM, the following symptoms may be observed:

  - Line card might crash.
  - Links might flap.
  - Following error message from line card might be seen:

    ```
    "SLOT 9: Sep 14 13:48:48.479 CDT: %COMMON_FIB-3-FIBIDBINCONS2: An internal
    software error occurred. Multilink1 linked to wrong idb R11_Mu1"
    ```

  Conditions: Occurs on routers running various Cisco IOS Release 12.2SR releases. Performing a **shut/no shut** on the OSM (especially on the card containing MLPPP) interfaces might trigger this issue.

  Workaround: There is no workaround.

- CSCsu57182

  Symptoms: The Cisco IOS may experience high CPU utilization.

  Conditions: ISAKMP is enabled.

  Workaround: There is no workaround.

  Further information: This issue can occur if the Cisco IOS device processes a malformed IKE message.

- CSCsu57331

  Symptoms: In a Virtual Private LAN Services (VPLS) scenario with ESM20 as core facing interface, imposition traffic might fail.

  Conditions: Occurs only when ports from Bay 1 are used as core facing interface.

  Workaround: Reset the line card.

- CSCsu57958

  Symptoms: In a scenario where a Catalyst 6500 or Cisco 7600 performs DHCP snooping + DAI functionality and a second device acts as DHCP relay, it was observed that DHCP snooping database was not populated. DHCP snooping is configured in this case on the ingress VLAN (traffic from the DHCP clients) and the DHCP server can be reached on a different egress VLAN (DHCP requests are routed).

  DHCP Replies from the server (DHCPOFFER and DHCPACK) are not snooped by the Catalyst 6500 or Cisco 7600 and so bindings are not established. Consequence is that clients will get their own IP Address but ARP Inspection will fail because bindings were not learned on the device.

  Conditions: Occurs with DHCP Snooping + DAI configured on a Catalyst 6500 or Cisco 7600 in a routed scenario (Ingress VLAN and Egress VLAN are different) and DHCP Relay performed by a different device.

  Workaround: Configure DHCP Snooping on both client and server side VLANs. Problem is applicable to both Cisco IOS Release 12.2(18)SXF and Cisco IOS Release 12.2(33)SRB.

- CSCsu59021

  Symptoms: CPU usage reaches 95 percent when adding/removing ACLs and performing an SSO.

  Conditions: The symptom occurs only when adding/removing huge ACLs and performing an SSO by using the command **redundancy force-switchover** with QOS service policy under the interface in which ACL is being used for a class-map.

  Workaround: Remove QOS policy or reboot the router.

- CSCsu62667

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

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu63884

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

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

  Workaround: There is no workaround.

- CSCsu64215

  Symptoms: Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

  Conditions: Occurs when the **ip tcp adjust-mss** command is configured on the device.

  Workaround: Disable **ip tcp adjust-mss** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsu64323

  Symptoms: The **show vpdn history failure** command should show the history of session failures due to entering incorrect password, but it does not show any history.

  ```
  Router#show vp hi fa
  ```

```
% VPDN user failure table is empty
```

Conditions: The problem was seen with Cisco 7201 running Cisco IOS Release 12.2(33)SRC1. There is no problem with Cisco IOS Release 12.4(4)XD9.

Workaround: There is no workaround.

- CSCsu65189

  Symptoms: If router is configured as follows:

```
router ospf 1
...
 passive-interface Loopback0
```

  And later is enabled LDP/IGP synchronization using command

```
Router(config)#router ospf 1
Router(config-router)# mpls ldp sync
Router(config-router)#^Z
```

  MPLS LDP/IGP synchronization will be allowed on interface loopback too.

```
Router#sh ip ospf mpls ldp in
Loopback0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required < ---- NOK
  Holddown timer is not configured
  Interface is up
```

  If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

  Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

  Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

  The problem will not occur if LDP/IGP sync is already in place and:

  - router is reloaded with image with fix for CSCsk48227
  - passive-interface command is removed/added

- CSCsu67461

  Symptoms: Router may crash when “show tracking brief” is entered if one or more tracking object have been created using the Hot Standby Routing Protocol (HSRP) CLI, such as **standby 1 track Ethernet1/0**.

  Conditions: This does not occur if all tracking objects use the new **track** command as follows:

  track 1 interface Ethernet1/0 line-protocol interface Ethernet 0/0 standby 1 track 1

  Workaround: Use **show tracking** instead, or configure tracking with the new command.

- CSCsu67637

  Symptoms: IPv6 address of loopback interface set as passive under Intermediate System-to-Intermediate System (IS-IS) router process is not present in IS-IS database.

Conditions: Issue is seen when loopback interface is set as passive under router IS-IS configuration and the IPv6 address of the interface is only added afterwards. If the **passive-interface** command is used when the loopback interface already has its IPv6 address configured, issue is not seen.

Workaround: After the IPv6 address is configured under the affected interface, remove and add the passive-interface configuration under the router IS-IS process.

- CSCsu69590

  Symptoms: After Flex Link failover, connectivity may be lost. Configured VLANs might be pruned on active link, causing VLAN interface to go down.

  Conditions: This usually happens after the second Flex Link failover.

  Workaround: Remove the Flex Link configuration from the interface, then reconfigure it.

- CSCsu71004

  Symptoms: Cisco 7600 RP crashes while executing the **copy tftp sup-bootdisk:** command. A similar crash seen upon switchover

  Conditions: Occurs when issuing a copy command from SP console on an RSP720.

  Workaround: There is no workaround.

- CSCsu71728

  Symptoms: A crash may occur while applying QOS under an MFR interface.

  Conditions: The symptoms are observed while applying QOS under an MFR interface on a PA-MC-2T3-EC in L2VPN.

  Workaround: There is no workaround.

- CSCsu74397

  Symptoms: When removing PA-MC-8TE1+ from the chassis, the router has an unexpected system reload. This reload happens when you remove the port adapter and the router is running the Cisco IOS bootloader image. Also happens when the port adapter is removed after the router finishes loading the Cisco IOS bootloader image and before it loads the complete Cisco IOS Software image.

  Conditions: This occurs on a Cisco 7200 VXR NPE-G2 Series Routers on the Cisco IOS bootloader image from the Cisco IOS Release 12.4(4)XD.

  Workaround: Remove PA-MC-8TE1+ when the complete Cisco IOS Software Image finishes loading.

- CSCsu76800

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

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

  Workaround: There is no workaround.

- CSCsu77549

  Symptoms: Protocol Independent Multicast (PIM) VPN routing/forwarding (VRF) neighbors not formed.

  Conditions: Occurs after line card reload.

  Workaround: Delete and add back the MVPN configuration.

- CSCsu78559

  Symptoms: In scaled conditions (8000 IP sessions) with SACL applied, line card memory leaks over a period of 4-5 hours. Sometimes this even results in a line card crash. The “Sacl Np Client” task occupies most of the CPU, and a large number of IP sessions (around 10% of 8k) will be in feature pending status, with ACL pending flag set.

  Conditions: Occurs under scaled conditions with approximately 8000 IP sessions, with the same SACL applied to all IP sessions.

  Workaround: There is no workaround.

- CSCsu79340

  Symptoms: Cisco router crashed while Intermediate System-to-Intermediate System (IS-IS) is coming up.

  Conditions: Occurred only on a Cisco router running Cisco IOS Release 12.2(33)SRC2 with “mpls traffic-eng multicast-intact” configured under “router isis”.

  Workaround: Disable “mpls traffic-eng multicast-intact” configuration.

- CSCsu79754

  Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

  Conditions: Unknown at this time.

  Workaround: Create an ACL to drop PIM packets to such interfaces.

- CSCsu81406

  Symptoms: Following a processor switchover in route processor redundancy (RPR) plus mode, the SM-1CHOC12/T1-SI card on the channelized serial interfaces goes down.

  Conditions: Occurs after the processor switchover in RPR plus mode.

  Workaround: Use **hw-module reset** to solve the issue.

- CSCsu81838

  Symptoms: Memory leak occurs.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- CSCsu82893

  Symptoms: Features requiring nas-port as a username determined by AAA (such as pre-auth) will not work on the standby device, causing standby sessions to be poisoned.

  Conditions: AAA calculates the IP address of the best port, which is up and active. However, on the standby device, no interface is visibly active, resulting in a best IP address defining the router to be 0.0.0.0.

  Workaround: There is no workaround.

- CSCsu83563

  Symptoms: Multicast rate-limiters stop working after a HA switchover.

  Conditions: To see this issue you have to have a HA setup with multicast rate-limiters set. In order to see this issue the rate-limiters must have been set before the standby is booted. If the rate-limiters are set after standby is up in HOT state, the issue is not seen after switchover.

  Workaround: Remove and reconfigure the rate-limiters.

- CSCsu83588

  Symptoms: After a router reload, the Flex Link configuration (**switchport backup interface Po#**) is lost.

  Conditions: Occurs when a backup interface is a port-channel interface.

  Workaround: There is no workaround.

- CSCsu87248

  Symptoms: Router crashes while adding flexible NetFlow.

  Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu87721

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

  Conditions: Occurred on a Cisco 7206VXR (NPE-G1) that was upgraded from Cisco IOS Release 12.2(31)SB11 to 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu88256

  Symptoms: Imposition traffic on a Ethernet Over MPLS (EoMPLS) VC is dropped.

  Conditions: Occurs if xconnect is configured on a EVC with switchport on another interface.

  Workaround: There is no workaround.

  Further Problem Description: When this problem happens the DMAC used by the imposition line card is that of the switchport interface instead of the router MAC address, causing the packet to be dropped.

- CSCsu89550

  Symptoms: All tagged packets on a hardware Ethernet Over MPLS (EoMPLS) VC is subjected to CoPP when the VC is down.

  Conditions: Occurs if VC is brought down by flapping core facing interface.

  Workaround: Remove the control-plane policy.

  Further Problem Description: It is applicable to only port-mode hardware EoMPLS.

- CSCsu90010

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

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

  Workaround: There is no workaround.

- CSCsu92395

  Symptoms: Router crashes.

  Conditions: This issue occurred on a Cisco 870 router running Cisco IOS Release 12.4(15)T7 and 12.4(20)T with EEM configuration like the following:

```
event manager applet RTR-MYPRIVATE_DOWN trap
 event syslog pattern "\%LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to down"
```

```
 action Mail mail server "mailaddress@cisco.com" to "mailaddress@cisco.com"
from "mailaddress@cisco.com" subject "rtr-myprivate - down" body "Sorry, I'm Down"
event manager applet RTR-MYPRIVATE_UP trap
 event syslog pattern "\%LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up"
 action Mail mail server "mailaddress@cisco.com" to "mailaddress@cisco.com"
from "mailaddress@cisco.com" subject "rtr-myprivate - up" body "Hi, I'm Active now"
```

When Virtual-Access1 interface flaps, the box crashes.

Workaround: Remove EEM action mail configuration.

- CSCsu92966

  Symptoms: Send statistics from the **show mpls l2 vc** command are not displayed.

  Conditions: Occurs on a PE when the other PE's core-facing link is flapped.

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

- CSCsu93374

  Symptoms: The group state of a slave group may unexpectedly change to Active after an RP switchover.

  Conditions: The symptom is observed when HSRP multigroup is configured such that a slave group follows the state of a master group. If the HSRP group state is Standby, then the group state of the slave group may change to Active after an RP switchover.

  Workaround: There is no workaround.

- CSCsu94379

  Symptoms: A router crashes.

  Conditions: The symptom is observed when using the **hw-module shut** command and then immediately executing the **no card** command on an ATM line card.

  Workaround: Allow for a time gap between issuing the **hw-module shut** command and the **no card** command.

- CSCsu94864

  Symptoms: The MLS shortcut for a user-traffic flow based on RADIUS Framed-IP (FIP) is not purged when the FIP sticky times out. RADIUS Load Balancing (RLB) sends out a purge request before deleting sticky and has no effect in deleting the MLS shortcut entry.

  Conditions: Occurs on a device configured with RLB and FIP sticky idle timer and with MLS aging timer configured higher than the RLB FIP sticky idle timer.

  Workaround: There is no workaround.

- CSCsu95080

  Symptoms: A router remains in the init_process state when parsing the configuration.

  Conditions: The symptom is observed when an IPv6 multicast group joins without MLD configured. When the groups unjoin, the system suspends.

  Workaround: Configure MLD.

- CSCsu95171

  Symptoms: In switches running Cisco IOS Release 12.2(33)SRC, high CPU may be seen on the SP/DFC due to NDE-IPv4 process. This may result in following unrelated problems:

- Corrupted file system(s)
- **show running** command may show “read error” etc.
- Continuous CPUHOGs automatically disabling Cisco Express Forwarding (CEF).

Log Messages reported:

```
%SYS-SP-3-CPUHOG: Task is running for (4000) msecs, more than (2000)msecs
(2/0),process = NDE - IPV4.
```

Conditions:

- Affects 12.2(33)SRC or later, but not earlier versions.
- Slow response to console commands.
- Netflow enabled on point-to-point interfaces
- High number of IPv4 routes learned via BGP.

Workaround: Downgrade to the latest release of 12.2(33)SRB. During high CPU condition, do the following:

1. Remove ALL interface level and global netflow configurations.
2. Configure global command: **cef table output-chain build favor convergence-speed**.
3. Re-apply global and interface level netflow configurations.

The **cef table ...** command mentioned above will stay in the configuration. This command should stop this issue from re-occurring.

- CSCsu95319

  Symptoms: Igmp-proxy reports for some of the groups are not forwarded to the helper. This causes members not to receive the multicast traffic for those groups.

  Conditions: The problem is seen when the igmp-proxy router is receiving UDP control traffic. That is, the router is receiving any UDP control-plane traffic on any interface.

  Workaround: There is no workaround.

- CSCsu96730

  Symptoms: Intelligent Services Gateway (ISG) traffic from one user to another may fail if the packet needs to be processed by the RP in a Cisco 7600.

  Conditions: Occurs when ISG is configured and packets are switched from one subscriber to a second subscriber.

  Other symptoms: - Counters of packet transfer might show difference between user transferring between each other - Access-list might fail to block the packet

  The 2 above symptoms will be seen when user are sending receiving on the same interface via the ISG

  Workaround: There is no workaround.

- CSCsu97934

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

  Conditions: Unknown.

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

- CSCsu99573

  Symptoms: Cisco router crashes when Open Shortest Path First (OSPF) neighbor is being configured in non-base topology and IP address of the neighbor does not fall into range of any existing interface.

  Conditions: This crash will only occur when OSPF is configured to support multi-topology routing, and neighbor statements are used in the submode for a non-base topology.

  Workaround: Configure the neighbor with this IP address in the base topology first.

- CSCsv00168

  Symptoms: Junk values are being displayed on the router when characters/commands are inputted. For example, enter “enable”, it shows “na^@^@”; enter “show version”, it shows “h ^v^@e^@^r^@^@^@^@^@”.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

  Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv01474

  Symptoms: The **ip rip advertise** command might be lost from the interface.

  Conditions: This symptom occurs in any of the following three cases:

  1. The interface flaps.
  2. The **clear ip route** command is issued.
  3. The **no network** *prefix* command and then the **network** *prefix* command are issued for the network corresponding to the interface.

  Workaround: Configure the **timers basic** command under the address-family under rip.

- CSCsv03300

  Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

  Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard GigabitEthernet interface.

  Workaround: There is no workaround.

- CSCsv04674

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

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

  Workaround: There is no workaround.

- CSCsv04733

  Symptoms: A LAC might terminate a tunnel unexpectedly.

  Conditions: This symptom is seen when the tunnel password exceeds 31 characters.

  Workaround: Use a shorter password if policy allows.

  Further Problem Description: This is seen with Cisco IOS interim Release 12.2 (34.1.3)SB1. With a customer specific special based on Cisco IOS Release 12.2 (31)SB11, it allowed 64 characters.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsv05934

  Summary: Cisco VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

  Workarounds: There are no workarounds available for this vulnerability.

  This response is posted at http://www.cisco.com/warp/public/707/cisco-sr-20081105-vtp.shtml

- CSCsv06309

  Symptoms: Link debounce down feature not working on RSP720-3C-10GE ports due to fast link feature.

  Conditions: Occurs when link debounce is configured on RSP720-3C-10GE.

  Workaround: Use “carrier-delay” instead.

  Further Problem Description: On configuring link debounce, fast link, which is enabled by default and has no CLI, needs to go off but does not.

- CSCsv06608

  Symptoms: SXP is set up between two devices but fails to initialize.

  Conditions: This symptom is observed when SXP is set up between two devices.

  Workaround: There is no workaround.

- CSCsv07188

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

  Conditions: Occurs Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsv07467

  Symptoms: When doing IP session on Layer 4 Redirect with VPN routing/forwarding (VRF) web logon scale test, subscriber tries to authenticate with 20 characters per second from test tool. MCP crashed into ROMMon.

  Conditions: Occurs only when test tool sends authentication at 20 characters per second

Workaround: There is no workaround.

- CSCsv08352

  Symptoms: Some static routes are not in the IP routing table state after a stateful switchover (SSO).

  Conditions: This only occurs following a SSO event.

  Workaround: Perform a **shut/no shut** of interface if the route does not come up automatically.

- CSCsv08528

  Symptoms: After the Resilient Ethernet Protocol (REP) topology is returned by the **rep preempt** command, MAC address table is not cleared.

  Conditions: During internal testing, this occurred approximately 3 times out of 20.

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

- CSCsv12428

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

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

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

- CSCsv13243

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

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

  Workaround: Configure subinterface in “non-native” mode.

- CSCsv13914

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

  Condition: Occurs when the interface is not up.

  Workaround: There is no workaround.

- CSCsv14818

  Symptoms: MLP on LNS bundle fails to come up.

  Conditions: The symptom is observed with MPLS applied on the core.

  Workaround: There is no workaround.

- CSCsv14963

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

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

  Workaround: There is no workaround.

- CSCsv20125

  Symptoms: PPPoE sessions over VLAN over ATM with process switch stuck at LCP stage.

  Conditions: Occurs when the **protocol pppovlan** command is configured on ATM subinterface along with **no ip cef**. PPPoE sessions are not created.

  Workaround: Use the **ip cef** command.

- CSCsv21295

  Symptoms: Due to TestLoopback diagnostic failure on RSP supervisor, the interface is placed to err-disable state.

  Conditions: This is seen when the interface is configured as RJ45 and with speed between 10 to 100mbps.

  Workaround: Configure the speed on RJ45 interface “auto” negotiation and execute the diagnostic test TestLoopback to get the port out of err-disable.

- CSCsv21403

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

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

  Workaround: There is no workaround.

- CSCsv22930

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

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Do not enable FRR between these routers.

- CSCsv23252

  Symptoms: A Cisco 7600 running Virtual Private LAN Services (VPLS) with QinQ tunnels is forwarding CDP/VTP packets from the tunnel interfaces across remote sites, even when L2TP is not enabled.

  Conditions: Occurs with a VPLS setup with QinQ tunnel interfaces facing the customer edge.

  Workaround: Use different domain names to avoid changes to VTP database.

- CSCsv23428

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

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

  Workaround: There is no workaround.

- CSCsv24179

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

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

  Workaround: There is no workaround.

- CSCsv24742

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

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

Workaround: There is no workaround.

- CSCsv24908

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

  Conditions: Occurs on a SIP-400 with SPA-2X1GE running BGP and GRE tunnels. Interface flapss on other modules are unable to resolve ARP or maintain routing neighbors. Issue seen on Supervisor 720 and Cisco 6748 CFC ports.

  Workaround: Reload the chassis.

- CSCsv25306

  Symptoms: OSPF between two customer sites over H-VPLS network with SIP600 as core facing card in the hub router fails to come up.

  Conditions: This is seen with traffic engineering (TE) and fast reroute (FRR) TE/FRR setup in the hub, and when TE tunnels have dynamic path option set.

  Workaround: Perform a **shut/no shut** on the core-facing SIP600 interface.

- CSCsv27428

  Symptoms: TCP sessions passing through a NAT router freeze.

  Conditions: The NAT router is a Cisco 7600 with RSP720. NAT translation entries keep using syn-timeout (default = 60 sec) even after TCP three-way handshake is done. Use **show ip nat translation verbose** to check timer

  Workaround: Use the **ip nat translation syn-timeout** command, which mitigates the problem to some extent.

- CSCsv27480

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

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

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

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

- CSCsv27617

  Symptoms: After reloading, NetFlow stops working and the output of **show ip interface** shows “IP Routed Flow creation is disabled in netflow table”.

  Conditions: This condition is seen on WAN main interfaces of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3 and can also be seen on Cisco IOS Release 12.2(33)SRC2.

  Workaround: Remove and reconfigure NetFlow on the affected interfaces.

- CSCsv30307

  Symptoms: ISSU does not work from Cisco IOS Release 12.2(33)SRD to Cisco IOS Release 12.2(33)SRB5.

  Conditions: When ISSU is performed from Cisco IOS Release 12.2(33)SRD image to 12.2(33)SRB5 image, ISSU is not working because of a default command introduced in 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv31342

  Symptoms: QoS does not work when a very large number of class-maps and ACLs are configured.

  Conditions: The symptom is observed on an NSE-100/NSE-150 when a large number of class-maps and ACLs are configured, so that the maximum policy-maps supported by the result table become less than 2048 (this can be checked using the **test platform acl** command). QoS does not work due to the QoS lookup table not getting updated correctly.

  Workaround: Removing and reconfiguring all the service-policies is the only workaround.

- CSCsv33977

  Symptoms: BGP peer fails to exchange the OPEN Message for negotiating capability when the neighbor router does not support any BGP capabilities.

  Conditions: The symptom is observed when the neighbor router does not support any BGP capabilities and when the capability negotiation fails due to an SSO switchover.

  Workaround: Configure “neighbor x.x.x.x dont-capability-negotiate”. Issue the **clear ip bgp *** command when the issue occurs.

- CSCsv34532

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

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

  Workaround: There is no workaround.

- CSCsv35120

  Symptoms: The ES20-GE3C/GE3CXL line card may crash if the explicit-path of an MPLS Traffic Engineering (TE) tunnel is changed so that it no longer goes out a core-facing port-channel interface.

  Conditions: Seen only when the following conditions are met:

  – Virtual Private LAN Services (VPLS) traffic passes over the MPLS Traffic Engineering tunnel.
  – Traffic going out the tunnel initially goes over a port-channel interface.
  – Five or more ports on the ES20 line card are used in the port-channel interface.
  – The explicit-path specified avoids the port-channel interface

  Workaround: Shut down the port-channel interface first before changing the tunnel’s explicit-path.

- CSCsv35571

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

  Conditions: All of the following must be true:

  – Port-channel configured with member links on ES20 line card
  – Encapsulated dot1q is configured on a service instance on the port-channel
  – Port-channel has member links on both NPUs

  - For 20-port ES20, this means ports 0-9 have at least one member link, and ports 10-19 have at least one member link.
  - For 2-port ES20, this means both ports are members of the port-channel.
  - The service instance are removed from the configuration.

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

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

- CSCsv36266

  Symptoms: E1 and SonetVT layers are down even though serial (Upper Layer) ifOperStatus is UP.

```
Serial1/0/0.1/2/1/1:1 ifOperStatus.156 = up(1)

E1 1/0/0.1/2/1/1 ifOperStatus.157 = lowerLayerDown(7

TU 1/0/0.1/2/1/1 ifOperStatus.158 = down(2)

tug 3-2 tug 2-1 e1-1:chgrp1

  AU-4 1, TUG-3 2, TUG-2 1, E1 1 (C-12 1/2/1/1) is up

  156 Se1/0/0.1/2/1/1:11500512KUP UP

  157 E1 1/0/0.1/2/1/102.05MUP <blank>

 158 TU 1/0/0.1/2/1/102.05MUP down
```

  Conditions: Occurs on serial interfaces of SPA-1XCHSTM1/OC3.

  Workaround: There is no workaround.

- CSCsv36892

  Symptoms: TCLsh mode is not exited when the session is disconnected or times out. The next user to connect and authenticate is put in TCLsh mode.

  Conditions: Occurs on high availability systems with an active and standby RP.

  Workaround: Explicitly exit TCLsh mode rather than disconnecting or allowing the session to time out.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsv41886

  Symptoms: Entering the **no ip routing** or **no router bgp xx** command yields the following error message:

  ```
  %IPRT-3-IPDB_DEL_ERROR: i_pdb delete error bgp, 4, 210074C8, 20E322E0, 0, 0
  -Process= "IP RIB Update", ipl= 0, pid= 117,
  -Traceback= 0x61FD7F58 0x62005498 0x62006D24
  ```

  Conditions: Occurs when a large number of VRFs must be configured and BGP is also configured to support these VRFs, then a **show** command, such as **show run**, is issued shortly after the **no ip routing** or **no router bgp** command.

  Workaround: There is no workaround.

- CSCsv48296

  Symptoms: The router reloads with the following error:

  ```
  SYS-6-BLKINFO: Corrupted redzone blk
  ```

  Conditions: Occurs when the **cns image** is active, and a CNS image operation is in progress.

  Workaround: There is no workaround.

- CSCsv50159

  Symptoms: Spurious access or crash seen on a router with a CEoP SPA, when bulk sync happens between RP and RPR.

  Conditions: Occurs during regular bootup.

  Workaround: There is no workaround.

- CSCsv51032

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

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

  Workaround: There is no workaround.

- CSCsv62150

  Symptoms: When cbgpPeerCapsTable is queried, it does not return the results of VPNv4 neighbors.

  Conditions: Configuration should have VPNv4 neighbors.

  Workaround: There is no workaround.

- CSCsv62960

  Symptoms: A session service policy with ‘police cir percent” configuration in the child calculates an actual “cir” of 0 bps.

Conditions: This can occur when modifying the policy map while it is attached to a session.

Workaround: Use fixed rate police “cir” rather than percent.

- CSCsv63799

  Symptoms: A router may reload if PfR is enabled and the number of flows exceeds the size of the NetFlow cache. This is a stress condition.

  Conditions: This symptom is observed when PfR is enabled (which also enables NetFlow).

  Workaround: A possible workaround is to configure the following:

  ip flow-cache timeout active 1

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv73388

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

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

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

- CSCsv73506

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

  Conditions: Unknown at this time.

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

- CSCsv73509

  Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  Conditions: Configure “no aaa new-model”, configure login local under line vty 0 4 and configure login tacacs under line vty 0 4.

  Workaround: There is no workaround.

- CSCsv73754

  Symptoms: A Cisco 10000 series router crashes. Traceback decode points to a function of bgp_vpn_impq_add_vrfs_cfg_changes.

  Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 VRFs or more are unconfigured.

  Workaround: There is no workaround.

- CSCsv76018

  Symptoms: A NSE-100 crashes after an SSO when traffic is kept on for one AToM-PPPoE circuit.

  Conditions: The symptom occurs after an SSO with traffic running for AToM-PPPoE.

Workaround: There is no workaround.

- CSCsv78555

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

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

  Workaround: There is no workaround.

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

- CSCsv79584

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

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

  Workaround: There is no workaround.

  Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining “debug ip routing” for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv79673

  Symptoms: Unicast flooding occurs for all traffic destined to VLAN SVI. MAC address for the VLAN SVI is being learned dynamically.

  Conditions: Changing the VLAN SVI configuration from IP to XCONNECT and back without shutting down the interface will result in the router MAC being learned dynamically instead of being installed as static. Normal aging occurs on the dynamic MAC, resulting in unicast flooding if the MAC is removed from the MAC address table.

  Workaround: Perform a **shut/no shut** on the affected VLAN SVI.

- CSCsv79993

  Symptoms: A Cisco 7600 may crash when a distribute-list is deleted.

  Conditions: Crash occurs when removing a distribute-list from EIGRP. The distribute-list was one of many that was sharing the same route-map and access-list. The crash only happens when multiple protocols have the same direction distribute-list configured on the same interface, as in the following example:

```
router eigrp 10

network 10.0.0.0

distribute-list 49 out Ethernet1/2.10



router rip

network 10.0.0.0
```

```
default-metric 2

distribute-list 49 out Ethernet1/2.10
```

Workaround: There is no workaround.

- CSCsv81751

  Symptoms: Cisco 7200 G2 router crashes when changing configuration of serial interfaces from PPP to SDLC and back to PPP, while running traffic.

  Conditions: This is observed on a T3 link with 56 channel groups configured on a WAN aggregation device. All the serial interfaces have service-policy configured.

  Workaround: Remove the service-policy before changing the encapsulation to SDLC.

- CSCsv86256

  Symptoms: In the pseudowire stitching configuration, if fast reroute (FRR) is enabled for link or node protection at the tunnel stitching router, then end-to-end connectivity is broken.

  Conditions: Problem happens only if a Cisco 7600 is the stitching-point router and has MPLS Fast Reroute enabled.

  Workaround: Disable FRR at the stitching point.

- CSCsv86288

  Symptoms: Sending a NETCONF hello reply which contains a “session-id” element triggers an instant crash. The device will report a reload due to a bus error.

  Conditions: This occurs when sending a hello reply which contains a session-id element. A hello without this element, one which only contains NETCONF capabilities, does not cause a crash.

  Workaround: Send a NETCONF hello without a session-id element.

- CSCsv87997

  Symptom: DHCPv6 relay process crash on Active RP.

  Conditions: Unknown at this time.

  Workaround: Unknown at this time.

- CSCsv89643

  Symptoms: If Ethernet interface configured as Open Shortest Path First (OSPF) point-to-point network then adjacency is being established using only multicast packets. As a result routes calculated over the link do not have MAC address of next-hop’s IP resolved prior to routes being installed into the routing table. This leads to delay for routes to become usable as lower-level protocols have to trigger MAC resolution. During short period of time traffic sent over the interface is lost when routes are just installed for the first time.

  Conditions: Occurs when Ethernet interface is configured for OSPF point-to-point.

  Workaround: Problem will self-correct because passing traffic triggers MAC address resolution.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsv92088

  Symptoms: BACKPLANE_BUS_ASIC-4-DEV_RESET error interrupts generated by SIP-400 module, causing traffic interruption.

  Conditions: Occurs when PPPoE traffic ingresses a SIP-400 line card on a Cisco 7600 Series router running Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCsv94471

  Conditions: On an ES-20, sometimes the interface configured as a promiscuous port does not forward the traffic to other community and isolated ports on the same private VLAN. The traffic on the promiscuous port is forwarded to all other community and isolated ports belonging to the same private VLAN. This is the expected behavior.

  Condition: Sometimes using the CLI on the interface configured in the promiscuous mode **switchport mode private-vlan promiscuous** after **switchport private-vlan mapping** *primary vlan secondary vlans* can cause traffic to be dropped. The order of these CLIs should not matter.

  Workaround: There is no workaround.

- CSCsv94485

  Symptoms: Per-user features may not get installed on the session, when other features (non per-user) are applied to the same session during account logon.

  Conditions: The issue is observed with Cisco IOS Release 12.2(33)SB3.

  Workaround: Use Cisco IOS Release 12.2(33)SB5.

- CSCsv95474

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

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

  Workaround: There is no workaround.

- CSCsv97273

  Symptoms: The SP crashes when the device receives an IP address from the DHCP server. The following error message is displayed:

  Signal = 11 Vector = 0x1400

  Conditions: Occurs on a Cisco Catalyst 6500 with RSP720-3C-GE when the **ip verify source vlan dhcp-snooping** is enabled.

  Workaround: There is no workaround.

- CSCsv99599

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

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

```
DEBUG: Packet dump: Acct-Output-Packets = 43118 Acct-Input-Gigawords = 0
Acct-Output-Gigawords = 83 Acct-Input-Octets = 4265182 Acct-Output-Octets = 41795579

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

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

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

- CSCsv99716

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The symptom is observed on a Cisco platform, when enabling the debug command **debug issu all** in the router and doing a loadversion.

  Workaround: Do not turn on ISSU debug.

- CSCsw14845

  Symptoms: An access-list with multiple ports in a single entry only programs the first port into TCAM. All subsequent ports are not processed according to the access-list entry.

  For example, the following access-list should block both SSH (TCP port 22) and Telnet (TCP port 23), but Telnet is permitted.

```
ip access-list extended deny_ssh_and_telnet
 deny   tcp any any eq 22 telnet
 permit ip any any
```

  Conditions: Occurs when there is an extended named access-list with multiple ports in a single access-list entry. This only applies to transit traffic since traffic destined to the router is process-switched and processed in software.

  Workaround: There is no workaround.

- CSCsw16157

  Symptoms: Routers using OSPF and MPLS Traffic Engineering may crash or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some cases a configuration change will cause an immediate crash, while in others memory may be corrupted resulting in problems later.

  Routers using MPLS-TE primary auto-tunnels are particularly vulnerable because those tunnel interfaces may be removed as the result of network topology changes as well as by modifying the running configuration.

  Conditions: In order to be exposed to this problem, a router must have MPLS TE tunnel interfaces that are announced to OSPF. Systems that do not run OSPF, or which do not use MPLS-TE are not affected.

  Systems that operate without “service alignment detection” enabled may crash when the following configuration commands are issued:

  Global configuration mode:

  * no interface tunnel <n>

  * no router ospf

  * no mpls traffic-eng auto-tunnel

  Interface configuration mode:

  * no ip unnumbered

  * no ip address

  Exec mode:

* clear mpls traffic-eng auto-tunnel

Note that routers running modular IOS (ION) and IOS-XE do not have alignment detection enabled.

Regardless of the state of alignment detection, removing the last MPLS-TE tunnel interface to a destination can cause problems, as can removing auto-tunnel configuration. Removal of dynamically created auto-tunnel interfaces as a result of changes in the network topology has the same effect.

Note that routers using auto backup tunnels to provide fast reroute for static MPLS-TE tunnels do not have any extra exposure to this bug because while these backup tunnels may be removed due to topology changes, the static tunnel to the same destination will not be.

Normal UP/DOWN state changes of tunnel interfaces do not cause problems.

Workaround: To remove a MPLS-TE tunnel interface, first configure it down with the "shutdown" command in interface submode.

To remove an OSPF instance, first disable MPLS-TE for the instance by configuring "no mpls traffic-eng area *n*" in router OSPF submode.

No workaround is available for MPLS-TE auto-tunnels.

- CSCsw16658

  Symptoms: "A named IPv6 access list with this name already exists" error incorrectly occurs in following scenario and we can not create ipv4 access-list:

  1. Configure **snmp-server community public RW ipv6** *access-list name* (Example. sample).
  2. Unconfigure it using **no snmp-server community public RW ipv6** *access-list name* (Example. sample).
  3. Try to create access-list name, same as ipv6 access-list name which was given in step 1.

  After step 2, we are not seeing IPv6 access-list neither in running-config nor **show ipv6 access-list**, but still we are not able to configure ipv4 acess-list.

  Conditions: Problem seen with the router loaded with c7200-adventerprisek9-mz.124-23.8.T image.

  Workaround: There is no workaround.

- CSCsw16698

  Symptoms: New DHCP clients are not able to get IP address from DHCP server via DHCP relay on the router. Existing clients are unable to renew their IP addresses

  Other Symptoms:

  1.1 When we're trying to display DHCP bindings with "show ip dhcp binding" command the following message is observed:

  % The DHCP database could not be locked. Please retry the command later.

  1.2 Command "ip dhcp database" disappeared from the running configuration.

  1.3 Output of "show run" is delayed.

  1.4 Output of "debug ip dhcp events" show the following when a new DHCP packet is received:

  DHCPD: dhcpd_receive_packet: unable to lock semaphore to check for pre-existing bindings could not lock se. DHCPD: dhcpd_timer_process could not lock semaphore. DHCPD: dhcp_server_receive could not lock semaphore.

  2.1. This bug may also cause DHCP Snooping failure. In this case, the output of the **show ip dhcp snooping database** command constantly shows these lines:

  Agent Running : Yes Delay Timer Expiry : 0 (00:00:00) Abort Timer Expiry : Not Running

Conditions: Occurs when DHCP and/or DHCP Snooping database agent is configured to store bindings on a TFTP server, and then the database files are not present or are read-only for some time on TFTP server while the router tries to write to them.

Workaround: Before the issue occurs, there are three known alternatives to avoid this problem:

1. Either configure “length 0” for line console 0;
2. Or - log in via console at least once since router startup;
3. Or - use Cisco IOS Release 12.2(33)SRD but do not enable “debug tftp packet”.

To fix the issue after it has occurred, connect to the router via console, press space bar to get rid of “--More--” prompt, then press enter to log in

- CSCsw19729

  Symptoms: Basic ping on the serial interface does not work after a reboot.

  Conditions: The symptoms occur with any encapsulation with an NSE-100 and NSE-150.

  Workaround: Explicitly do the encapsulation configuration. Even configuring the same interface will work.

- CSCsw23061

  Symptoms: The **rbe nasip** *InterfaceX* command does not work if a DHCP request comes from a QinQ interface on the BRAS/DHCP relay.

  Conditions: The symptoms are observed if a DHCP request comes from a QinQ interface on the BRAS/DHCP relay and when using the **rbe nasip** *InterfaceX* command.

  Workaround: There is no workaround.

  Further Problem Description: In a typical DSL broadband environment where DHCP option 82 is used, **rbe nasip** *InterfaceX* can be used to uniquely hardcode a BRAS interface IP into the agent-remote-id Option 82 sub-option field in case the DHCP request comes from a ATM subscriber. In modern QinQ environments, there is currently no solution. The **rbe nasip** *InterfaceX* command is ATM specific and does not work if a DHCP request comes from a QinQ interface on the BRAS/DHCP relay.

- CSCsw23945

  Symptoms: A CPU hog appears while doing an auto FPD upgrade of the SPAs.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(34)SB and with a third-party vendor’s SPA. The CPU hog is seen only when doing an auto FPD upgrade of the SPA.

  Workaround: There is no workaround.

- CSCsw24542

  Symptoms: A router may crash due to a bus error after displaying the following error messages:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
  %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
  ```

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

  Workaround: There is no workaround.

  Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

- CSCsw24611

  Symptoms: A router configured with BGP and VPN import may crash.

  Conditions: This is a hard to hit race condition. BGP imports a path from VRF-A to VRF-B. The following steps have to take place in exactly this order for the crash to occur:

  1. The next-hop for the path has to become unreachable.
  2. BGP has to re-evaluate the bestpath on the net in VRF-A and result in no-bestpath on the net (because there is no alternative path available).
  3. RIB installation has to process the importing BGP net under VRF-B.

  Step 3 will result in the crash. If, before step 3, the next-hop re-evaluation manages to process the net in VRF-B then it will clear the bestpath and there will be no crash. If, before step 3, the import code gets a chance to process the net it will clean-up the imported path from VRF-B and then there will be no crash.

  Workaround: There is no workaround.

- CSCsw24826

  Symptoms: Cisco router may crash pointing to OSPF code because of low memory access.

  Conditions: Crash is specific to the following scenario:

  1. Neighbor router performs IETF NSF restart.
  2. Software interface between routers is removed from configuration when NSF restart is undergoing, when grace LSA is present in the database of the helper router.
  3. Helper router will crash 1 hour later during max-age procedure for grace LSA. Reason is that grace LSA is associated with interface, but that interface does not exist any more.

  Workaround: If configuration changes need to be done during network changes, the following applies:

  1. Shutdown OSPF interface
  2. Check **show ip ospf da**. Can you see type-9?

     - NO => good, remove interface

     - YES => “no shutdown” interface, wait for neighbor going FULL (type-9 will be flushed during sync)
  3. Repeat Step 1.

- CSCsw25255

  Symptoms: A Catalyst 6500 or Cisco 7600 router may not send back a BPDU with agreement flag in response to a proposal on its root port, causing slow convergence on the designated bridge.

  Conditions: This is seen on Catalyst 6500 switches running any version of Cisco IOS Release 12.2(33)SXH. This is seen on Cisco 7600 routers running any version of Cisco IOS Release 12.2SR.

  Workaround: The problem does not occur if **debug spanning-tree event** is enabled. This can be a suitable workaround in an environment with a small number of VLANs if the debug does not impact CPU usage.

- CSCsw26414

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

  ```
  %DIAG-SP-6-TEST_RUNNING: Module 6: Running TestSPRPInbandPing{ID=2} ...
  %DIAG-SP-6-TEST_OK: Module 6: TestSPRPInbandPing{ID=2} has completed successfully
  ```

Conditions: Device goes into BAD state for unknown reason.

Workaround: There is no workaround.

- CSCsw27711

  Symptoms: GE SPA does not come up after performing multiple times **shut** and **no shut**. The following error message is shown:

  ```
  %SPA_ETHER-3-SEND_MSG: Subslot 4/0, 2xGE SPA Failed to notify driver process about a
  line state change in one of the SPA interfaces
  ```

  Conditions: The symptom occurs after performing multiple times **shut** and **no shut** and having around 1000 SPA-GIG subinterfaces.

  Workaround: Perform **hw-module slot** *slot-number* **stop/start** to bring up the interface.

- CSCsw28082

  Symptoms: SNMP messages are not seen.

  Conditions: When the BRI interface is down on a remote router, and **no ppp link reset** is configured on device, SNMP trap message shows “down” instead of “keepalive failed”.

  Workaround: There is no workaround.

- CSCsw28139

  Symptoms: PBR stops working after stateful switchover (SSO). All traffic that should be policy routed is dropped instead.

  Conditions: This usually happen after several switchovers between supervisors. Usually problem occur after about 10 switchovers, however, it could happen after first one.

  Workaround: Remove and add policy on the interface.

- CSCsw31019

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed if the **frame-relay be 1** command is issued under “map-class frame-relay *name*” configuration.

  Workaround: There is no workaround.

- CSCsw35155

  Symptoms: When using denies in ACLs in crypto maps, the VPN SPA or VPN SM crashes.

  Conditions: Occurs when configuration uses denies in ACLs with crypto maps that causes too many entries in the Ternary Content Addressable Memory (TCAM).

  Workaround: Enter the **crypto ipsec ipv4 deny clear** command.

- CSCsw35638

  Symptoms: When a Cisco router is the Merge Point (MP) for a protected TE tunnel, and FRR is triggered, two things happen:

  – The primary LSP goes down, and traffic is lost on the protected tunnel.

  – Any PLR that is downstream of the failure will lose its backup.

  Conditions: When a competitor’s router is a point of local repair (PLR) and a Cisco router is a merge point, then when FRR is triggered, the Cisco router drops the backup tunnel (in some cases immediately and in other cases after 3 minutes). This causes the primary tunnel that is protected by this backup to go down. The issue has been identified as related to the fact that session attribute flags (link/node protection desired) are being cleared by the competitor PLR when the Path is sent over the backup tunnel.

Workaround: There is no workaround.

- CSCsw36872

  Symptoms: VPN-NUM in VLAN-RAM TCAM wrongly provisioned after reconfiguration of Layer 3 port-channel. This changes member link mapping, and VRF membership changes on Layer 3 port-channel. Also discrepancy in L3MGR info between RP and SP for affected port-channel/internal vlan representation observed.

  Conditions: When the command **channel-group** *number* **mode active** is configured on the member link before the respective Port-channel is configured, this causes the member link interface to go admin down. When the port-channel is configured, the port-channel first comes up and then the member link. This may cause the port-channel to take up the same VLAN which was previously assigned to the member link. If this happens, the symptom is seen.

  Workaround: One workaround is to configure the port-channel first and then activate the channel-group on the member link interface. Another workaround is to create a dummy interface so that it takes up the member link's previous VLAN and the port-channel will be assigned a new one, in which case this problem is not seen.

- CSCsw37053

  Symptoms: Traffic with aggregate label was forwarded in wrong VPN, causing the mis-forwarding, as the IP prefix was not present in the VPN routing/forwarding (VRF) table.

  Conditions: Occurs under the following scenario:

  1. Aggregate label should not be using the VPN CAM.
  2. The recirculation VLAN has the wrong VPN number.

  Workaround: Manually correct the wrong **mls vlan-ram entry**.

  Further Problem Description: If there are multiple aggregate labels on a given VRF, there might be a chance of seeing this issue.

- CSCsw37635

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The active router crashes when doing load version with "debug issu all" turned on.

  Workaround: Do not turn on ISSU debug.

- CSCsw43211

  Symptoms: Following errors are seen:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0xFFFFFFFF)

  -Traceback= 60476EBC 60477400 60491664 616C5834 616C7EEC 61AB72CC 61AC2E64 61AC2EBC
  60FE4274 60FDEFA4 60FD4180 60FD4874 60FD4BBC 60FD275C 60FD27A0 60FC8F74
  ```

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

  Workaround: There is no workaround.

- CSCsw43272

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

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

  Workaround: Use IP pool instead of DHCP pool.

- CSCsw43948

  Symptoms: A Cisco 3845 router that is running Cisco IOS Release 12.4(13) may bounce the frames (which are not destined for itself) on the same interface that receives them.

  Conditions: The symptom is observed if there is bridging configured on an ethernet subinterface in the following way:

```
ip cef
 !
 bridge irb
 !
 interface GigabitEthernet0/1
  no ip address
  no sh
 !
 !
 interface GigabitEthernet0/1.100
  encapsulation dot1Q 100
  ip address x.x.x.x x.x.x.x
  no ip redirects
  no ip unreachables
  no ip proxy-arp
  ip rip advertise 10
 !
 interface GigabitEthernet0/1.509
  encapsulation dot1Q 101
  bridge-group 1
```

  Workaround: If the command **bridge-group 1** is removed from the sub-interface, it will behave as expected.

- CSCsw45694

  Symptoms: Cisco 10000 PRE3 and PRE4 routers use nested policy. You can apply service-policy with higher shape rate than the actual available BW to the POS or ATM interfaces.

  This problem applies to both the **shape average** *bps* and the **shape average percent** *percent_value* commands.

  The child policy will use the configured shape rate to calculate the priority police value. This will result in higher police rate.

  Conditions: This symptom occurs when shape rate is configured higher than the actual BW.

  Workaround: Configure shape rate to the actual available BW.

- CSCsw47210

  Symptoms: Range PVCs fail to come up on the interface when a VC-class with create-on-demand is detached from the ATM interface.

  Conditions: The symptoms are observed when a VC-class with create-on-demand is detached from the interface.

  Workaround: Remove create-on-demand from the VC-class instead of removing the VC-class itself.

- CSCsw47475

  Symptoms: Cisco 7600 router has multiple E1s that randomly flap.

  Conditions: Occurs on a router with RSP720, SIP-200 and 8xCHT1/E1 SPA installed.

  Workaround: There is no workaround.

- CSCsw50608

  Symptoms: With the traffic flowing between a promiscuous port and a port belonging to a community VLAN of the same primary VLAN, if the user adds or removes any other secondary VLAN under the same private VLAN using the following configuration under “int gi” for the promiscuous port.

  Conditions: The issue was seen upon using the following CLI on the interface configured in the promiscuous mode.

  switchport private-vlan mapping *primary-vlan* **add/remove** *secondary-vlan*.

  Workaround: There is no workaround.

- CSCsw51210

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

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

  Workaround: Avoid configuring MFR with the Cisco 7304 platform.

- CSCsw52698

  Symptoms: The following error message is displayed:

  ```
  %BACKPLANE_BUS_ASIC-4-DEV_RESET: Backplane Bus Asic reset, interrupt [0x062D]=0x0008
  ```

  Conditions: Symptom reported by 7600-SIP-400 cards on 7600 Series Routers when PPPoE connections are terminated via the 7600-SIP-400 cards.

  Workaround: There is no workaround.

- CSCsw53404

  Symptoms: FR-FR and FR-Ethernet connections configured for anything over MPLS (AToM) interworking do not work with the combination of SIP400 and channelized SPAs.

  Conditions: Occurs with Frame Relay AToM configurations with SIP400 and channelized SPAs.

  Workaround: There is no workaround.

- CSCsw62823

  Symptoms: Encapsulation is not getting inherited from the VC-class for the final VC.

  Conditions: The symptom is observed when changing encapsulation from the console without exiting from the applied encapsulation under VC-mode on a VTY session.

  Workaround: Apply encapsulation from single terminal at the same time (either from console or from VTY).

  Further Problem Description: Only the last VC is not getting updated with encapsulation.

- CSCsw69366

  Symptoms: When sending packets that exceed specified MTU, packets are received as giants in PA-T1/E1 IMA card instead of being fragmented.

  Conditions: It happens only after changing sub-interface MTU and after stateful switchover (SSO).

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

- CSCsw70125

  Symptoms: A Cisco 7600 SIP-400 with POS interfaces encapsulated with IETF frame-relay may incorrectly set 0x800 as Network Layer Protocol Identifier (NLPID) for hardware assisted multicast IP packets. The correct value is 0xCC.

  Conditions:

  1. IP unicast packets in hardware path do not have this problem.
  2. IP multicast or unicast packets in software path do not have this problem.
  3. Problem is reproducible in Cisco IOS Release 12.2(33)SRA2, 12.2(33)SRA7, and 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw71208

  Symptoms: Cisco 7600 does not respond properly to Link Control Protocol (LCP) echo requests, causing PPP sessions to renegotiate between the router and non-Cisco devices.

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

  Workaround: Disable keepalives on the non-Cisco device.

- CSCsw72030

  Symptoms: A NSE-100/150 crashes when you configure and bring up an L2TP xconnect circuit over a GRE tunnel.

  Conditions: The symptom occurs when you configure an L2TP circuit over a GRE tunnel and bring up the circuit by making the xconnect interface up.

  Workaround: There is no workaround. You can disable PXF via the configuration command **no ip pxf** to avoid this problem. The downside being all traffic will be RP-switched at a much slower rate than PXF-switching.

- CSCsw72677

  Symptoms: Router crashes with “no bba-group pppoe”.

  Condition: Happens after unconfiguring “bba-group”.

  Workaround: There is no workaround.

- CSCsw73863

  Symptoms: IDs allocated from DHCP are leaked, causing the device to reload.

  Conditions: Device is configured as Cisco Intelligent Services Gateway (ISG) DHCP with 24000 sessions flapping every 10-12 minutes.

  Workaround: There is no workaround.

- CSCsw75589

  Symptoms: If you have configured Netflow and also have “ip flow-cache mpls label-positions”, you are very likely to run in a bus error crash with info similar to what is seen here:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20

  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20

  10:28:28 UTC Sat Dec 20 2008: TLB (store) exception, CPU signal 10, PC = 0x61CB7180
  ```

  Conditions: Problem is platform independent but specific to Cisco IOS release. This problem is seen in Cisco IOS Release 12.2(33)SRC1 and possibly affects Cisco IOS 12.4T releases as well.

Workaround: Consider removing MPLS netflow configuration by removing the **ip flow-cache mpls label-position 1** command.

- CSCsw76113

  Symptoms: Unable to reuse a sub-interface as main-interface.

  Conditions: Occurs when we configure **no virtual-template subinterface** when all of the Interface Descriptor Blocks (IDB) that platform supports are used as “subif-vaccess”. No more “vaccess” can be created.

  Workaround: Do not configure **no virtual-template subinterface** at run time. Check **show vtemplate** output. If there are more IDBs used by subinterface, then do not configure **no virtual-template subinterface**.

- CSCsw76692

  Symptoms: PXF crashes when traffic is sent for an L2TPv3 circuit which has been configured over a GRE tunnel.

  Conditions: The symptom occurs when the core-facing interface is ATM and the peer router is a non-PXF.

  Workaround: There is no workaround.

- CSCsw76910

  Symptoms: Supervisor reloads on configuring or verifying firewall farm commands.

  Conditions: Occurs before and after compliance testing on the firewall farm commands.

  Workaround: There is no workaround.

- CSCsw77205

  Symptoms: ES20 line cards crashing in a loop while using a anything over MPLS (AToM) VC with Cisco Intelligent Services Gateway (ISG).

  Conditions: The issue is seen on all the ES20 cards installed in a Cisco 7609 router running Cisco IOS Release 12.2(33)SRC2.

  Workaround: Manually shutdown the AToM interfaces and ISG interfaces to stop the crashes.

- CSCsw78396

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

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

  Workaround: There is no workaround.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/sub-interface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw79787

  Symptoms: MQC incorrectly calculates bandwidth percentage on POS link.

  Conditions: The symptom is observed on a SPA-2XOC3-POS inserted into a Cisco 7300 series router with an NSE-150 that is running Cisco IOS Release 12.2(33)SB2.

  Workaround: There is no workaround.

- CSCsw81485

  Symptoms: Issuing **no** form of IPX configuration commands on an interface crashes the switch.

  Conditions: Occurs when IPX routing is enabled on the device but not on the interface.

  Workaround: Do not issue **no** form of IPX configuration commands on an interface where IPX is not enabled.

- CSCsw82462

  Symptoms: A connected prefix from the global routing table has a VPN routing/forwarding (VRF) interface as outgoing interface.

  Conditions: This condition occurs after a **clear ip route x.x.x.x** for the prefix x.x.x.x.

  Workaround: **Shut** the VRF interface, clear the prefix from the routing table, then **no shut** the VRF interface.

- CSCsw87061

  Symptoms: A Cisco 7304-NSE100 router crashes when configured with NAT and a large number of ACLs.

  Conditions: This symptom occurs when configuring NAT with a large number of ACLs. A malloc failure will occur and will be followed by the router crash. This happens only on NSE100 and not on NSE150.

  Workaround: There is no workaround.

- CSCsw88324

  Symptoms: The ESM20G, 7600-ES20-GE3CXL, indicates Major error on show module.

  Conditions: No special configuration conditions are needed to reproduce. The online diagnostics status indicates “Major Error”. The major error can be observed following a forced switchover using the **redundancy force-switchover** command.

  Workaround: No workaround known. Only reloading the router may cause the ESM20G to recover and pass online diagnostics.

- CSCsw89574

  Symptoms: Under certain circumstances when a route entry containing a repair path is updated or deleted, the repair path may not be properly removed. This may result in the repair path being orphaned in memory consuming a 60 byte memory block.

  Conditions: Occurs with mVPN/TE and multicast enabled on a BGP speaking router. All images based on Cisco IOS Release 12.2(33)SR may be impacted by this problem.

  Workaround: There is no workaround.

- CSCsw89720

  Symptoms: When we perform SNMP query (getmany) on cbQosPoliceStatsTable and cbQosREDClassStatsTable, CPU utilization reaches 99% with a single SSH session. If we query cbQosPoliceStatsTable and cbQosREDClassStatsTable from 18 SSH sessions, CPU-HOG error message are seen

Conditions: Occurs with a large number of policies defined on a GigE subinterface (~4k).

Workaround: No workaround, other than stopping the query.

- CSCsw90777

  Symptoms: With LFI enabled, the average latency does not show much improvement, compared with LFI disabled.

  Conditions: The symptom is observed on a PRE4 with a CHSTM1 line card with LFI enabled and with 128K and 384K circuits.

  Workaround: There is no workaround.

- CSCsw91320

  Symptoms: A crash occurs with the following footprint:

```
Address Error (store) exception, CPU signal 10,
PC = 0x4330E8E0

0x432DF9F0 ---> dlink_rmqueue+30
0x432DFAEC ---> dlink_dequeue+2C
0x40DF73BC ---> nrp_service_notification_queue+26C
0x40DF7D8C ---> network_redist_process+210
```

  Conditions: Occurs when a multicast protocol is configured on at least one interface. Intermediate System-to-Intermediate System (IS-IS) is configured to run on one of the interfaces on which the multicast protocol is enabled. For example:

```
interface TenGigabitEthernet1/1
 ip address 10.10.1.21 255.255.255.252
 ip router isis
 ip pim sparse-mode
```

  IS-IS interface configuration is removed from the interface on which the multicast protocol is configured. If a unicast route owned by IS-IS changes shortly after the multicast interface configuration is removed, the crash may occur.

  Workaround: The following multicast configuration can be used to avoid the risk of a crash:

```
Router(config)#ip multicast rpf multitopology
Router(config)#global-address-family ipv4 multicast
Router(config-af)#topology base
Router(config-af-topology)#use unicast base
```

- CSCsw91422

  Symptoms: Crash occurs on Cisco 7206VXR/NPE-G1 running Cisco IOS Release 12.2(31)SB12.

  Conditions: Occurs under general use. No error messages appear in logs.

  Workaround: There is no workaround.

- CSCsw96484

  Symptoms: An interface that has been error disabled by an OAM remote link failure will not be recovered even if OAM link failure error disable recovery has been configured.

  Conditions: Occurs when Ethernet OAM is configured on the interface and a remote failure is detected.

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

- CSCsw99846

  Symptoms: With mLDP over a P2P tunnel, traffic drops in multiple cases.

  Conditions: The traffic drops when there is a change in path set entries, which can happen when you perform a **shut** and **no shut** the TE tunnel or toggle MPLS traffic-tunnel or use the **clear mpls traffic-eng auto-tunne** command.

  Workaround: There is no workaround.

- CSCsx05672

  Symptoms: High CPU utilization occurs on the new active supervisor after a stateful switchover (SSO).

  Conditions: Occurs when large numbers of logical interfaces (such as port-channel sub-interfaces or interface VLANs) are configured and earl policing policies applied (uflow policing or aggregate policing) on all the logical interfaces. The CPU utilization on the active supervisor aggravates on each switchover.

  Workaround: There is no workaround.

- CSCsx06457

  Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

  Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

  Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx07317

  Symptoms: Static NAT translations can fail after a reload or crash.

  Conditions: The trigger seems to be a high number of static translations (~100 translations). Once the router is rebooted for any reason, the translations will fail.

  Workaround: Remove and reapply static translations in the configuration.

- CSCsx08294

  Symptoms: A Cisco 6500 running Cisco IOS Release 12.2(33)SXH may encounter a bus error due to OSPF processes.

  Conditions: Occurs when the device is configured for OSPF Incremental SPF and Virtual Links.

  Workaround: Do not use Incremental SPF.

- CSCsx09221

  Symptoms: According to **show pxf cpu buffers** on a Cisco 10000 series router, the PXF CPU buffer might go down to zero.

  Conditions: The symptom is observed when:

  – The router connects to the other end of a router via 6CT3 line card.

  – Repeating the commands **shutdown** and **no shutdown** on controller T3 on the other end of the router and, after that, monitoring with **no shutdown** for several hours.

  Workaround: Reset the ESR-6CT3 line card by issuing the **hw-module slot** *slot#* **reset** command.

- CSCsx09353

  Symptoms: Switched Port Analyzer (SPAN) is not capturing traffic in both directions. It only captures traffic in one direction.

  Conditions: Occurs when running Cisco IOS Release 12.2(33)SRC or later and with a ES-20 card.

  Workaround: Use another method of packet capture if possible. See VACL capture for details. Removing the SPAN configuration and reapplying it also helps in getting the feature working.

- CSCsx12378

  Symptoms: A Cisco 7304 router may crash.

  Conditions: The symptom is observed on a Cisco 7304 router with an NSE-100 engine while doing multicast ping.

  Workaround: There is no workaround.

- CSCsx13929

  Symptoms: The following error is observed when you flap the Native gig interface through which an L2TP circuit over a GRE tunnel is configured and when traffic is passing:

  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: SROC packet length missmatch

  Conditions: The symptom occurs when PFX is enabled and traffic is passing through the circuit.

  Workaround: There is no workaround.

- CSCsx15841

  Symptoms: The **BGP aggregate-address** command configured on active RP does not auto-sync to the running configuration of the standby RP.

  Conditions: Occurs when BGP is configured on active/standby redundant RP system.

  Workaround: Configure BGP aggregate-address and reboot the system, forcing both active and standby to load from startup configuration.

- CSCsx16152

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

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

  Workaround: No workaround except turning off DHCPv6 relay.

- CSCsx17619

  Symptoms: Connectivity between the multilink bundles is lost.

  Conditions: Occurs upon configuration of DLFI over ATM and trying to clear the virtual-access created for multilink using the **clear ppp interface virtual-access** *no* command.

  Workaround: There is no workaround.

- CSCsx18270

  Symptoms: Admin tag is being advertised by the neighbor router. This tag is not showing up in the local router. This causes route filtering based on admin tag to fail.

  Condition: Occurred on a Cisco ASR1000 running Cisco IOS Release 12.2(33)XNB. Other devices and releases of Cisco IOS are affected.

  Workaround: There is no workaround.

- CSCsx20147

  Symptoms: The delay value to destination computed is different between IPv4 and IPv6.

  Conditions: Occurs when EIGRP for IPv6 is configured.

  Workaround: There is no workaround.

- CSCsx21482

  Symptoms: The following commands executed from the console result in a device reload: **write**, **copy running-config startup-config** or **show run**.

  Conditions: The symptom is observed when a large number of interfaces (200+) have been configured for RIPv6 and are active. Interfaces which are down will not contribute to the problem.

  Workaround: There is no workaround.

- CSCsx21606

  Symptoms: On a Cisco 10000 series router that is running Cisco IOS Release 12.2(28)SB11, the serial interface becomes stuck in an up/down state and the multilink interface in a down/down state. The debugs indicate:

  ```
  Se7/0/0.10/17:1 PPP: Missed a Link-Up transition, starting PPP
  Se7/0/0.10/17:1 PPP: Updating buffered PPP packet
  Se7/0/0.10/17:1 PPP: Starting timer for fast-start
  Se7/0/0.10/17:1 PPP: Handle allocation failure
  ```

  Conditions: The symptom is observed when new T1s are added to the router. The triggers are an SSO configuration and when the router runs for a long time. The new T1s cause a lot of flapping of links.

  Workaround: Reload the router or perform a PRE failover on the Cisco 10000 series router.

- CSCsx23419

  Symptoms: The SFP ports are shown in the ENTITY MIB even though the SFPs are not inserted.

  Conditions: The symptom is observed with an NPE-G2 and NSE-150 card running Cisco IOS Release 12.2(31)SB10.

  Workaround: There is no workaround.

  Further Problem Description: In both (shut/no shut) states the issue occurs. With the ANA model, the device operates correctly the first time when the SFP is inserted (SFPmodule ==> SFP container ==> port). But once the SFP is pulled out, the port goes under the container (incorrectly, as the port should not go there). When we insert the SFP, the same port comes under the module. Since ANA will not delete a DC (the port, in this case) the same port gets two parents which ANA will not accept. With this fix the “PORT” entry will not be populated by the ENTITY MIB unless XCVR exists.

- CSCsx25316

  Symptoms: A device may reload because of a crash after the command **clear ip route *** is executed.

  Conditions: The trigger for this issue is executing the **clear ip route*** command in the presence of a default route. If an RIP update is received by the router while the routing information base is being cleared, the update will be processed causing RIP to check the state of the default route in the routing information base. This combination has the potential to cause a crash.

  The probability of the crash occurring is proportionate to the size of the routing table. The larger the routing table, the greater the chance of encountering the problem.

  Workaround: It is recommended to avoid using the **clear ip route *** command. If the prefix in question is known, then use **clear ip route** *prefix* instead.

Further Problem Description: This problem was observed in Cisco IOS Release 12.2(33)SRC3. All Cisco IOS SR33-based images (SRB, SRC, SRD and SB33) are vulnerable to this problem. The problem will be seen only when using the **clear ip route *** command and is platform independent. Other commands like **clear ip ospf**, **clear ip bgp**, **clear ip isis** or **clear ip route** *prefix* are not vulnerable.

- CSCsx27659

  Symptoms: L3 traffic is blackholed after online insertion and removal (OIR) of Distributed Forwarding Cards (DFCs).

  Conditions: After an OIR, some of the adjacencies (recirculation) may not be correctly programmed when they go online.

  Workaround: Use the **clear adjacency** command to reprogram the adjacencies correctly. This will impact traffic on the router.

  Further Problem Description: Use the **show mls cef adjacency entry** *x* **detail** command to diagnose. A display of "vlan=0" on recirculation adjacencies indicates this problem.

- CSCsx28221

  Symptoms: A router crashes.

  Conditions: The symptoms are seen when configuring range PVCs on a point-to-point subinterface and creating PPPoA sessions.

  Workaround: There is no workaround.

- CSCsx28442

  Symptoms: Spurious memory access may be observed with a Cisco 7304 (NPEG100) router when PA-CC is booting up with any channelized PAs, such as PA-MC-T3/PA-MC-E3/PA-MC-8TE1/PA-2CT3+/and other channelized PAs.

  Conditions: The symptom is observed when booting up a Cisco 7304 (NPEG100) RP which has PA-CC with channelized PA, or when the PA-CC with channelized PA is inserted. It is seen with the latest Cisco IOS 12.2(33)SB images (after release 12.2(33)SB3).

  Workaround: There is no workaround.

- CSCsx28948

  Symptoms: Packet leak is observed on Cisco 7200 router running Cisco IOS Release 12.2(33)SRC.

  Conditions: Multicast packet is forwarded to the tunnel interface, causing memory leak. Even packet is dropped, memory leak is observed. Multicast data having less then 64 byte size is dropped at the driver. Leak is not happening with interface other then tunnel interface.

  Workaround: There is no workaround.

- CSCsx33622

  Symptoms: Flapping BGP sessions are seen in the network when a Cisco IOS application sends full-length segments along with TCP options.

  Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the non-fixed Cisco IOS device. ICMP unreachables toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

  Workaround: Any value lower than the advertised MSS from the peer should always work.

Setting the MSS to a slightly lower value (-20 to -40) is sufficient to avoid the issue. This number actually accounts for the length of TCP options present in each segment. The maximum length of TCP option bytes is 40.

If the customer is using MD5, Timestamp, and SACK, the current MSS should be decreased by 40 bytes. However, if the customer is using only MD5, the current MSS should be decreased by 20 bytes. This should be enough to avoid the problem. For example:

1. If the current MSS of the session is 1460, New MSS = 1460 - 40 = 1420 (accounts for maximum TCP option bytes; recommended).
2. If the current MSS of the session is 1460, New MSS = 1460 - 20 = 1440 (accounts for only the MD5 option).

- CSCsx33961

  Symptoms: SNMP engine consumes 100% CPU and device does not respond to SNMP polls.

  Conditions: Occurs when ATM SPA subinterface counters, such as ifInOctets and ifOutOctets are being polled with multiple Varbinds in single SNMP PDU.

  Workaround: There is no workaround.

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

  Conditions: The symptom is observed on a Cisco 7200 series router and Cisco 7301 router with an NPEG1 processor.

  Workaround: Change the MDL of operation to PULL using the command **dma enable pull model**.

- CSCsx35306

  Symptoms: Router crashes at “t3e3_ec_safe_start_push”.

  Conditions: The crash is seen immediately after removing the channel-group of the PA-MC-2T3/E3-EC card.

  Workaround: There is no workaround.

- CSCsx37313

  Symptoms: When using encapsulation PPP on a POS SPA OC192POS-XFP in a SIP-600, the protocol comes up on both sides and IP Control Protocol (IPCP) is open for PPP. Pinging the remote side fails due to corruption of the PPP frame.

  Conditions: Occurs when using encapsulation PPP on a POS SPA OC192POS-XFP

  Workaround: Use High-Level Data Link Control (HDLC) encapsulation.

- CSCsx37431

  Symptoms: CE-to-CE ping for packet size less than 48 bytes fails or applications like telnet fail.

  Conditions: Occurs with ATM SPA on SIP200. ATM PA on FW2 should be one of the CEs facing, while other PEe should be 7200

  Workaround: There is no workaround.

- CSCsx39405

  Symptoms: When unconfiguring multicast distribution tree (MDT) and VPN routing/forwarding (VRF), SP crashes.

  Conditions: The problem occurs on scale setup. When number of entries is large on PI multicast side, the PI process can get suspended during delete operation

  Workaround: There is no workaround.

- CSCsx40675

  Symptoms: Router crashes

  Conditions: Occurs during xconnect L2TP session configuration.

  Workaround: There is no workaround.

- CSCsx40747

  Symptoms: A specific configuration of “ip casa” followed by a subsequent use of the command **show running-config** can cause the router to go into an infinite loop and hang.

  Conditions: The symptom is observed when “ip casa” is configured and you enter into config-casa mode. The command **show running-config** will cause the router to hang.

  Workaround: There is no workaround.

  Further Problem Description: This issue is specific to the usage of ip casa. If you do not use casa, you are not vulnerable to the issue described here.

- CSCsx41877

  Symptoms: ATM PVP CLI become inaccessible to the command-line interface.

  Conditions: The commands disappear after configuring l2transport VCs on ATM interface.

  Workaround: Execute default on ATM interface before configuring any L2VC or L2VP.

- CSCsx43644

  Symptoms: Policy-name remains unchanged after renaming.

  Conditions: The symptom is observed only with an ATM interface.

  Workaround: There is no workaround.

- CSCsx43897

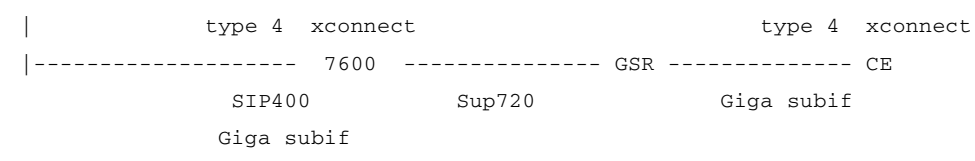
  Symptoms: CPU utilization goes high when a third session is allowed to be created through SNMP. Also occurs with applications that use SNMP to create sessions, such as NAM GUI.

  Conditions: Perform the SNMPSet on the service module session (this will fail). Now try to create another local session via SNMPSets sequence.

  Workaround: Use CLI to create the sessions.

- CSCsx47554

  Symptoms: With a topology like this:

  The packets above 1496 are not passing through end-to-end.

  The MTU on the edge-facing interfaces is 1500, the one on the core-facing interfaces is 1600.

  Conditions: The GSR on the other side seems not to have a similar behavior. The bug has been reproduced in Cisco IOS Release 12.2(33)SRB3 and SRC3.

  Workaround: Increase the MTU on the edge-facing interface end-to-end

- CSCsx49444

  Symptoms: PVCs associated with an F4 OAM VP remain in an “INAC” state after the interface flaps.

  Conditions: The symptom is observed with F4 OAM management configured on a VP.

  Workaround: Use the commands **shut** followed by **no shut** again.

- CSCsx49573

  Symptoms: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml

  Conditions: See “Additional Information” section in the posted response for further details.

  Workarounds: See “Workaround” section in the posted response for further details.

- CSCsx56263

  Symptoms: The **clear counter** command resets all the if-mib Object Identifiers (OIDs).

  Conditions: The symptom is observed when the **clear counter** command is issued. It is seen with Cisco IOS Release 12.2(33)SB3 and with an HHGIGE line card.

  Workaround: Reload the router.

- CSCsx56369

  Symptoms: Connectivity breaks on SPA based multilink bundles with ACFC/PFC configured when one of the member links go down.

  Conditions: Occurs on a Cisco 7600. Multilink must be SPA based with ACFC/PFC configured. The output of **show ppp multilink** on the RP would show **multilink in hardware**.

  Workaround: Adding back the link or bringing the link back up makes it work.

- CSCsx57465

  Symptoms: On a Cisco 7600-SIP-200 / SPA-2XOC3-ATM running the c7600s72033-adventerprisek9-mz.122-33.SRB4 image, an ATM interface may suddenly cease processing ingress packets resulting in all VC sharing the physical interface being shut down.

  Conditions: Occurs when the ATM SPA interface is configured for LFI.

  Workaround: There is no workaround.

- CSCsx58183

  Symptoms: A Cisco router might not successfully recreate a session on standby when Accounting and L4Redirect are installed.

  Conditions: The symptom occurs with PPPoE sessions in HA scenarios where Accounting along with other ISG features are deployed.

  Workaround: There is no workaround.

- CSCsx58861

  Symptoms: A router crashes.

  Conditions: The symptom is observed after the application of a multicast configuration.

  Workaround: There is no workaround.

- CSCsx58889

  Symptoms: Calls fail intermittently with cause “47: no resource available” error.

  Conditions: Occurs when router is under load test.

  Workaround: There is no workaround.

- CSCsx60939

  Symptoms: Standby crashes on deletion of a port-channel.

  Conditions: The problem is seen only when **lacp fast-switchover** is configured on the port-channel.

  Workaround: Shut the port-channel before deleting it.

- CSCsx62080

  Symptoms: Cisco ASR crashes into ROMmon when doing DHCP renew from client PC when Cisco Intelligent Services Gateway (ISG) is configured as DHCP relay.

  Conditions: Occurs when ISG is acting as DHCP relay and without port-bundle host key (PBHK) enabled.

  Workaround: Disable ping using the **ip dhcp ping packets 0** command.

- CSCsx64198

  Symptoms: Intercepted LI packets are not updated in MIB counter.

  Conditions: This symptom is observed when creating time based ACL for taps.

  Workaround: There is no workaround.

  Further Problem Description: Intercepted packet count is based on packets sent to MD. For time based ACL, it is not getting incremented although MD is receiving the packets. Due to this time based ACL script for LI, count fails.

- CSCsx65525

  Symptoms: SIP reloads with the following error messages:

  ```
  %C7600_PWR-SP-4-DISABLED: power to module in slot 2 set off (Module Failed SCP dnld)
  %CWAN_RP-6-CARDRELOAD: Module reloaded on slot 2/0
  ```

  Conditions: Occurs during switchover from slot6 to slot5 with RSP720.

  Workaround: There is no workaround.

- CSCsx67931

  Symptoms: The **no l2tp tunnel authentication** command does not work at LNS.

  Conditions: This symptom happens when the VPDN group that is used has a **virtual-template** *x*.

  Workaround: Configure the **no l2tp tunnel authentication** command under virtual template.

- CSCsx76308

  Symptoms: Cisco 6500 crashes with Breakpoint exception, CPU signal 23.

  Conditions: An attempt to free unassigned memory is seen before the crash:

  ```
  00:01:25: %SYS-2-FREEFREE: Attempted to free unassigned memory at 50D9D260, alloc
  40CC9960, dealloc 40CC9A90
  -Traceback= 41044F88 40CC9A98 40CC88C0 40CC20E4 40CCF5B0 406AF1AC 4069A834 4101848C
  41018478
  ```

  Workaround: There is no workaround.

- CSCsx78763

  Symptoms: When deny ACL is active, packets are intercepted and is expected to be 0. However it intercepts 20 packets and sends MD and CE1 routers.

  Conditions: LI replication occurs when deny ACL is active.

  Workaround: There is no workaround.

- CSCsx78789

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

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

  Workaround: Use netflow random samplers.

- CSCsx78826

  Symptoms: ES20 cards crash due to an address error after a remote Label Distribution Protocol (LDP) session is shut. This is also seen when the remote router is reloaded.

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

  Workaround: There is no workaround.

- CSCsx79111

  Symptoms: MPLS packets that need a swap label may get punted to CPU because the outgoing interface/label has wrong MTU value in hardware (MLS). Once the packet is punted to CPU, it is forwarded correctly, as Cisco Express Forwarding (CEF) in software has correct info. If the traffic rate is high, this causes high CPU.

  -**show mls status** can confirm the MTU failure increasing.

  -**remote command switch show mpls platform vlan** shows wrong MTU for outgoing interface.

  -**show mls cef mpls label X detail** will show the MTU as 0.

  -**show mpls forwarding-table interface X detail** shows good MRU value.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB5.

  Workaround: Re-stating the **mtu** command or **mpls ldp mtu ...** does not make any difference. You need to either bounce the affected interface or reload the switch.

- CSCsx82880

  Symptoms: MAC security on ESM20 ports stop working after unrelated configuration changes are done to any other ports on the same ESM20.

  Conditions: On ESM20 ports having service instances configured with MAC security on them, traffic stops flowing on those EVCs when unrelated configuration changes are done on other ports on that ESM20.

  Workaround: Perform a **shut/no shut** on the affected port.

- CSCsx94400

  Symptoms: All traffic through ES line cards stops after a RSP failover. The line cards are powered down and never recover.

  Conditions: Occurs occasionally when a **redundancy force-switchover** is executed on a router containing ES line cards with an N-PE redundancy configuration that looks like the following under a VPLS VFI:

  ```
  l2 vfi vfi101 manual
  vpn id xxx
  ```

```
forward permit l2protocol all
```

Workaround: Reload the router. If this does not help, reduce the number of possible core-facing MPLS interfaces that the VPLS pseudowire could possibly take.

- CSCsy04594

  Symptoms: When a Cisco 7600 is connected to a different MST region and has a port with root guard configured on the MST boundary port, all VLAN interfaces flap each time a superior BPDU is received on this port. This behavior was observed with Cisco IOS Release 12.2(33)SRB4 and Cisco IOS Release 12.2(18)SXF14.

  Conditions: It was observed in the following context:

  1. The switch is connected to a different MST region
  2. It has a port configured as root guard on MST region boundary

  Workaround: Shut down blocked port or remove root guard configuration from the port and the VLAN interfaces stop flapping.

- CSCsy07789

  Symptoms: QoS classification is broken with two user-defined classes.

  Conditions: The symptom is observed on a Cisco 7300 (NSE-100) and 7300 (NSE-150) router.

  Workaround: There is no workaround.

- CSCsy07830

  Symptoms: All traffic through ES line cards stops after a RSP failover. The line cards fail diagnostics and never recover.

  Conditions: Occurs periodically when a **redundancy force-switchover** is executed on a router containing multiple RSPs and ES line cards.

  Workaround: Reload the router.

- CSCsy07953

  Symptoms: Any attempt to copy a file from a router to an FTP server will fail. The FTP error is “No such file or directory”.

  Conditions: This is only a problem with FTP and only when transferring to an FTP server. Transfers from an FTP server work as expected.

  Workaround: Use a different file transfer protocol, such as TFTP.

- CSCsy10610

  Symptoms: LACP L3 POCH members flap, getting unbundled and bundled back again.

  Conditions: Global native VLAN tagging has to be enabled, and L3 POCH interface should have a subinterface configured under it.

  Workaround: Disable global VLAN tagging.

- CSCsy14633

  Symptoms: Packets are not getting intercepted.

  Conditions: The symptoms are observed when using radius-based LI.

  Workaround: There is no workaround.

- CSCsy15227

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsy24676

  Symptoms: On occasion, a false positive is returned on a file system failure. File operation is deemed successful when, in fact, it has failed.

  Conditions: This problem occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converted to a success code. This problem is likely to show up if there is a device error during the write. The device error may be due to bad media or an OIR (although it is very unlikely during an OIR).

  Workaround: There is no workaround.

  Further Problem Description: This is possible during any file system operation where a file system device is unable to complete the operation and an error is returned. This error is not passed down to the file system stack but is converted to a success code. Other clients which are dependent on previous file system operations fail on successive file system calls and possibly result in a crash.

- CSCsy26370

  Symptoms: Router carshes at af_policer_get_class_drops.

  Conditions: Router crashes while attaching policy under another policy.

  Workaround: There is no workaround.

- CSCsy27394

  Symptoms: Users who can execute a **show ip interface** command can see that an LI tap is in progress.

  Conditions: No specific conditions are necessary to trigger this problem.

  Workaround: There is no workaround.

- CSCsy28296

  Symptoms: A PPP aggregator may erroneously remove a per-user static route downloaded from RADIUS when the first member link of a multilink group goes down.

  Conditions: Issue observed on Cisco 7200/NPE-G1 running Cisco IOS Release 12.2(33)SRC3 and earlier SRC releases. Also occurs in Cisco IOS Release 12.2(33)SRD.

  Workaround: Clear interface virtual-access (for the MLP bundle). You can also downgrade to Cisco IOS Release 12.2SB.

- CSCsy32368

  Symptoms: An 8192 hold-queue value for the port-channel is invalid.

  Conditions: The symptom is observed when two interfaces, each with a hold-queue of 4096, are configured and then added to the port-channel interface. The hold-queue value of the port-channel is 8192 which is invalid.

  Workaround: There is no workaround.

- CSCsy34805

  Symptoms: Police rate configuration is lost after reload.

  Conditions: The following configuration:

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

  is saved in the router configuration as:

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

  This configuration is invalid and is rejected.

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

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

- CSCsy42615

  Symptoms: Entries for ABRs and ASBRs are missing from the OSPF route table. This results in inter-area and external routes being omitted from the Routing Information Base (RIB).

  Conditions: The bug will only be seen when MPLS-TE tunnels are being used. Also, specifying non-default SPF timer values with **timers throttle spf** will increase the risk of hitting this bug.

  Workaround: There is no workaround.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** may cause a router to crash.

  Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

  Workaround: There is no workaround.

- CSCsy49524

  Symptoms: A Cisco 7304 router may crash due to memory corruption.

  Conditions: The symptoms are observed with an Any Transport over MPLS (AToM) tunnel being transported over a Generic Routing Encapsulation (GRE) tunnel. LDP is enabled on the tunnel and routes to the LDP neighbor are known via the tunnel interface. The crash usually occurs during initial bootup when the remote LDP neighbor comes up, but has also been observed after a period of normal operation (specifically seen while transporting ATM over MPLS).

  Workaround: There is no workaround.

- CSCsy54440

  Symptoms: A standby, which is running Cisco IOS Release 12.2(31)SB, will crash while upgrading to Cisco IOS Release 12.2(33)SB, after using the command **issu runversion**.

  Conditions: The symptom is observed while upgrading from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(33)SB after using the command **issu runversion** and when there is one or more PPPoE sessions present.

  Workaround: Ensure there are no PPPoE sessions present while upgrading.

- CSCsy55362

  Symptoms: Console may hang.

  Conditions: Occurs when the TACACS+ server is being used as AAA server and the *single-connection* option is configured.

  Workaround: Remove the single connection option.

- CSCsy55455

  Symptoms: Device running Cisco IOS Release 12.2(33)SRD1 with SAA/SNMP crashes due to bus error.

  Conditions: Occurs when an SNMP poll for IPSLA/SAA values is performed.

  Workaround: There is no workaround.

- CSCsy58115

  Symptoms: In a router running BGP, the BGP process may hold increased amounts of memory over time without freeing any memory. This may also be seen from the output of **show proc mem sort** and in the output of **show ip bgp sum** or **show ip bgp vpnv4 all sum** and looking at the number of BGP attributes which may be increasing over time in relation to the BGP prefixes and paths which may remain roughly the same.

  Conditions: Some BGP neighbors are not in established state and exchanging prefixes. The issue is observed on all platforms running the following releases of Cisco IOS:

  - 12.2(31)SB14
  - 12.2(33)SB1b
  - 12.2(33)SB2
  - 12.2(33.05.14)SRB
  - 12.2(33.02.09)SRC
  - 12.2(33)SRC3
  - 12.4(20)T2
  - 12.4(22)T1
  - 12.2(33)SXI or later releases.

  Workaround: Remove the configuration lines related to the inactive neighbors (neighbors in Idle or Active states).

- CSCsy58886

  Symptoms: Router crash is seen during ISSU with **mls qos** enabled.

  Conditions: Occurs when user does ISSU from Cisco IOS Release 12.2(33)SRC2 to SRC3 or from 12.2(33)SRD1 to later SRD release.

  Workaround: Disable QoS globally using the **no mls qos** command.

- CSCsy59142

  Symptoms: The port in the line card cannot create a PPPoE session. The **show controller atm** *1/0/0* command shows that the counter “non-existent VC” is increasing.

  Conditions: The symptom is observed with a Cisco 10000 series router with ATM PPPoE sessions.

  Workaround: Reconfigure the interface.

  Further Problem Description: For the multiport OC3ATM card, having any physical interface in shut state with non default MTU configured on any of its subinterfaces or the physical interface itself, the following sequence of operations can cause a SAR corruption and traffic failure:

  - hw-module reset of the card or router reload.
  - no-shut the physical interface.

  After the no-shut event, all the VCs under other physical interfaces of the multiport card may drop traffic.

- CSCsy61277

  Symptoms: A router may crash when using the **show cef int** command in parallel with removing per-user ACL via radius.

  Conditions: The symptom is observed when using the **show cef int** command in parallel with removing per-user ACL via radius.

  Workaround: There is no workaround.

- CSCsy61367

  Symptoms: A router crashes when removing the VPN service from the PVC.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS interim Release 12.2(33.01.23)MCP04.

  Workaround. Do not enable VPN service for PTA service.

- CSCsy70524

  Symptoms: A router crashes upon deleting range PVCs with PPPoE sessions and with bandwidth configured through DBS.

  Conditions: The symptom is observed when deleting the range PVCs with PPPoE sessions.

  Workaround: There is no workaround.

- CSCsy74334

  Symptoms: Sticky-ARP entries are refreshed forever even after the client is removed from the network.

  Conditions: This issue is seen after an upgrade from Cisco IOS Release 12.2(33)SRB5 to Release 12.2(33)SRD1.

  Workaround: There is no workaround.

- CSCsy75718

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The issue appears to be Day 1, reported on a Cisco 7200/NPE-400 and 7200/NPE-G2 that is running Cisco IOS Release 12.4T, 12.4M, or 12.2SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server and if a lease is found only to exist on PPP aggregator, use the command **clear interface virtual-access** to recover.
  2. Manual: use the command **clear interface virtual-access**.

  Further Problem Description: The issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire when the PPP user's virtual access interface changes.

  Note: Use case fixed via CSCsy39667:

  1. PPP session with userid "jerry", VAI 100, and va_swidb "X" goes down.

2. New PPP session with userid “jerry”, VAI 100, and va_swidb “Y” is negotiated within 5 seconds of 1.

Fix Overview: DHCP looks for match on PPP userid and VAI number (not va_swidb) to reclaim DHCP Lease.

Use-case still requiring a fix:

1. PPP session with userid “jerry” and VAI 100 goes down.
2. New PPP session with userid “jerry” and VAI 200 is negotiated within 5 seconds of 1.

- CSCsy81362

  Symptoms: Port-channel VLAN sub-interfaces stop forwarding traffic after an SSO.

  Conditions: The symptom is observed after an SSO. One of the member links is getting removed from the port-channel bundle.

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

- CSCsy83691

  Symptoms: While migrating STS from VT to T3 mode, PRE crashes.

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (42/38),process = C10K Card Event Process.
  -Traceback= 6011F8E4 60111414 606DC7D0
  ```

  Conditions: This symptom is seen only while converting VT controller to T3 controller on CHSTM1 and CHOC12 line cards.

  Workaround: There is no workaround.

- CSCsy83830

  Symptoms: Router crashes when we send multiple access packets for same username when configured for RADIUS Load Balancing (RLB).

  Conditions: Occurs with the following topology

  ```
  CLIENT----->RLB----->SERVER
  ```

  Client sends multiple access retry packets to server and router crashes after a period of time. This issue will be seen in cases where multiple access requests are seen for the same username, and 60 seconds expire since the arrival of the first of such access requests, before an accounting start for the same username is seen.

  Workaround: If RLB do not see multiple access packets we wouldn’t see any crash.

- CSCsy86078

  Symptoms: Router crashes with memory corruption.

  Conditions: Occurs when BFD is configured on 10GigE interfaces and constant link flaps.

  Workaround: There is no workaround.

- CSCsy86441

  Symptoms: The PIM process shows a high CPU usage.

  Conditions: The symptom is observed when several PIM-enabled interfaces are coming up at the same time.

  Workaround: There is no workaround.

- CSCsy87385

  Symptoms: For IPv6 adjacencies, MTU is incorrectly programmed.

Conditions: Occurs with simple IPv6/6PE setup.

Workaround: There is no workaround.

- CSCsy88640

  Symptoms: A core dump may fail to write, with the following errors seen on the console:

```
current memory block, bp = 0x4B5400A0,

 memorypool type is Exception

 data check, ptr = 0x4B5400D0

 bp->next(0x00000000) not in any mempool

 bp_prev(0x00000000) not in any mempool

 writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z

  [Failed]

 writing compressed ftp://10.0.0.1/testiomem.Z

  [Failed]

 writing compressed ftp://10.0.0.1/test.Z

  [Failed]

 %No memory available
```

  Conditions: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.

  Workaround: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.

- CSCsy92895

  Symptoms: When SIP-400 is configured as Lawful Intercept service module, after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when SIP-400 is configured as Lawful Intercept service module on a Cisco 7600.

  Workaround: After line card OIR, select the SIP400 again as the LI service module using the command **li-slot list <sip400 slot number>**.

- CSCsy95540

  Symptoms: L2TP tunnel not coming up for ATM attachment circuit.

  Conditions: The problem is seen on Cisco 7200 router running Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsy96108

  Symptoms: OSPF neighborship establishment will not progress past the EXSTART state on a Cisco 10000 series router.

  Conditions: The symptom is observed under the following conditions:

  - OSPF peering over an ATM PVC sub-interface on an ESR-1OC12ATM line card. - a service-policy attaching a policy-map to the ATM major interface. - the policy-map must contain a class map that matches **ip dscp** *cs6*. - router is running Cisco IOS Release 12.2(33)SB1.

  Workaround:

  1. Removing the policy-map from the major interface, or removing the DSCP-CS6 class-map from the policy allows OSPF peering to complete successfully.
  2. Moving the policy-map from the major interface to a sub-interface.

  Note: configuring “ip ospf ignore-mtu” on the affected PVC interface is not a work-around.

  Further Problem Description: This issue is not seen in Cisco IOS Release 12.3(7)XI7b, only after upgrade to Cisco IOS Release 12.2(33)SB1.

- CSCsz00624

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

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

  Workaround: There is no workaround.

- CSCsz01313

  Symptoms: A router crashes with the following message:

  ```
  MET-DST: %SYS-2-INTSCHED: 'may_suspend' at level 7
  -Process= "AAA SEND STOP EVENT", ipl= 7, pid= 230
  -Traceback= 406ED098 406CEF8C 409E6A48 409E71F4 409E7CBC 406A1218 40875D20 40875D98
  400E89F0 40180A78 406F2708 406F2A00 406E88A0 406D7AE4 406E7A14 406E3B08
  ```

  Conditions: The symptom is observed under normal operation.

  Workaround: There is no workaround.

- CSCsz01484

  Symptoms: When using CBR-ATM traffic class on a ESR OC12 or OC3 line card for PPPoATM over MLP over MultiVCs, only half of the VAI sessions come up active in the bundle. If VBR-NRT is used, the problem does not occur.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB or later.

  Workaround: For the ESR-4OC3ATM-SM-LR a possible workaround would be to use VBR-NRT. However, this is not an option for the 1oc12atm-1 card since CBR and VBR-NRT use a different SAR scheduler.

- CSCsz05181

  Symptoms: A router may reload unexpectedly.

  Conditions: The symptom is observed when the router has Bidirectional Forwarding Detection (BFD) configured and is actively sending keepalives. The crash has multiple possible triggers:

  – It can be triggered by certain show commands (**show bootvar** and **show c7200** are known to cause the problem). The issue will not be seen on every invocation of the commands. It is a rare timing condition, so the probability of the crash increases as the commands are run more frequently.

  - It can also be triggered by large scale BFD deployments (hundreds of sessions on a single router).

  Workaround: Unconfigure BFD.

- CSCsz07569

  Symptoms: The session ID changes between “interim” and “stop” accounting records.

  Conditions: The symptom has been observed on Cisco IOS Release 12.2(31)SB12 with “radius-server attribute 44 extend-with-addr” in the configuration.

  Workaround: Do not configure “radius-server attribute 44 extend-with-addr”.

- CSCsz10073

  Symptoms: SPA-4XOC3-ATM can stop forwarding ingress traffic after cell packing timer is changed.

  Conditions: Occurs when MPLS is configured over a tunnel interface and the cell packing timer is changed.

  Workaround: There is no preventive workaround to this issue. Once the card is in the problem state, the FPGA is hung and to recover from this state, the SPA has to be reloaded.

- CSCsz11384

  Symptoms: The following error is logged:

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

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

  Workaround: There is no workaround.

- CSCsz14873

  Symptoms: Auto-RP messages are not forwarded from a Cisco 10000 series router PE to any attached CE in MVPN.

  Conditions: The symptom is seen with an MVPN setup, when Auto-RP routes have both an L and H flag.

  Workaround: There is no workaround.

- CSCsz21640

  Symptoms: A router may crash with BusError when sending an AccountingStop record.

  Conditions: Just before the crash, the following error messages are seen:

  ```
  %IDMNGR-7-ALLOCFAIL: Warning: Failed to allocate memory for keylist in event_init
  %IDMNGR-7-ALLOCFAIL: Warning: Failed to allocate memory for client request data in
  request_init
  ```

  The system is configured for ISG-services.

  Workaround: There is no workaround.

  Further Problem Description: This was seen in a customer specific special based on Cisco IOS Release 12.2(31)SB13.

- CSCsz30049

  Symptoms: A router may crash with memory corruption or with one of the two following messages:

  ```
  %SYS-6-STACKLOW: Stack for process HQF Shaper Background running low, 0/6000
  %SYS-6-STACKLOW: Stack for process PPP Events running low, 0/12000
  ```

In the case of memory corruption, a corrupted block will be in an address range very close to process or interrupt level 1 stack (this information is available in the crashinfo file).

Conditions: The symptom is observed on routers running Cisco IOS Release 12.2SB when ALL of the following conditions are met:

1. The router is configured for VPDN/L2TP.
2. There is a mixture of PPPoVPDN and "MLP Bundle" users.
3. QoS service policy with queuing actions (bandwidth guarantee or shaper) is applied to virtual access interfaces for both types of users.

Here is a way to find out if there is normal PPP users or MLP users:

```
PPP User via CLI:
 Router#sh user | inc PPP.*00 [1-9]
   Vi4          user#wl-cp03-7k2#4 PPPoVPDN     00:00:00 30.3.0.47

 MLP via CLI:
 Router#sh user | inc MLP.*00 [1-9]
   Vi8          user#wl-cp04-7k2#5 MLP Bundle   00:00:00 30.4.0.54
```

Workaround:

1. Allow only PPPoVPDN (i.e.: prevent "MLP Bundle" creation).
2. Disable QoS for "MLP Bundle" users or all users.

- CSCsz34356

  Symptoms: After a disk is formatted with a Cisco IOS Release 12.2(33)SRC image, "dir" and "boot" from the disk will fail at the rommon prompt and the following error messaged is generated:

  ```
  rommon 1 > dir disk1:

  Initializing ATA monitor library...
  open(): Open Error = -1
  dir: cannot open device "disk1:"
  rommon 2 >
  ```

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: Format the disk under an image that does not exhibit the problem.

- 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.

- CSCsz40677

  Symptoms: PRE crash caused by DHCP internal function.

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

  Workaround: There is no workaround.

- CSCsz43627

  Symptoms: Traceback and alignment corrections are seen from MLPoLNS.

Conditions: This symptom occurs while doing a **shut** in a GigE interface.

Workaround: There is no workaround.

- CSCsz43691

  Symptoms: If TAL subscribers attempt to logon when the Cisco ASR 1000 series router RADIUS service download requests a time-out, some sessions will get stuck in “Attempting” state during user/service authorizations. Once 200 sessions are stuck in this state, no subscriber will be able to login until all the sessions (those that are active and those that are stuck in “Attempting” state) are manually cleared using the **clear subscriber session all** command.

  Conditions: The symptom is observed when TAL subscribers attempt to logon while the Cisco ASR 1000 series router RADIUS service download requests a time-out.

  Workaround: Use the **clear subscriber session all** command to manually clear all sessions. This may be, however, service disruptive and impractical in a production network.

- CSCsz45683

  Symptoms: A Cisco 10000 series router reloads when the command **clear sss session all** is used.

  Conditions: The symptom is observed on a PRE2 with Cisco IOS Release 12.2(33)SB onwards and only when L4R is applied.

  Workaround: There is no workaround, except to avoid using L4R.

- CSCsz48040

  Symptoms: A router may crash when performing an ISSU upgrade.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRC3. It is seen when performing an ISSU upgrade if “mls qos” is configured on the router.

  Workaround: Unconfigure “mls qos” before performing the ISSU upgrade.

- CSCsz50620

  Symptoms: Bus error crash at an invalid address.

  Conditions: The symptom is observed when running Cisco IOS Release 12.2(31)SB with SSS configured.

  Workaround: There is no workaround.

- CSCsz56805

  Symptoms: Different IPs are seen on the same session between Active and Standby PRE cards and the number of in-use IP addresses on Standby is more than that on the Active.

  Conditions: The symptom is observed with the frequent connect/disconnect of sessions and when IP addresses are allocated from the local pool.

  Workaround: Reload the Standby card frequently.

- CSCsz71654

  Symptoms: Accounting records do not show the correct username.

  Conditions: The symptom is observed when account-logon (authentication) happens after failed Transparent Auto-Logon (TAL).

  Workaround: There is no workaround.

- CSCsz73470

  Symptoms: When there are more than 8000 DHCP sessions on a Cisco 7600 ISG, a few dangling sessions are sometimes observed.

Conditions: This symptom occurs when there are more than 8000 DHCP sessions on a Cisco 7600 ISG. ISG is configured as a DHCP relay.

Workaround: Clear the sessions using the **clear ip subscriber dangling** command.

- CSCsz75180

  Symptoms: The router may crash upon deleting a subinterface.

  Conditions: This symptom is observed if an ethernet interface is configured as follows:

```
router(config)#int Ethernet1/1.1
router(config-subif)#encap dot1q 1001
router(config-subif)#mpls ip
router(config-subif)#end
```

  Next, the subinterface is removed with “no interface Ethernet1/1.1”.

  The router may crash.

  Workaround: Do not delete the subinterface.

- CSCsz82825

  Symptoms: When relaying to multiple servers, from an unnumbered interface, the Cisco IOS DHCP relay sends packets to all servers, even for packets where the client in a RENEWING state unicasting to attempt to reach a single server.

  ARP entries are retained for all OFFERed addresses, even if the client ultimately is using a different address. These extra ARP entries persist for several hours.

  Conditions:

  1. When relaying a DHCP packet on an unnumbered interface, and the DHCP client is in a renewing state (as determined by the fact), send it to the DHCP server that allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions.
  2. When the client is in any other state, or if we do not get a response from the DHCP server, send to all helper-addresses.

  Workaround: There is no workaround.

  Further Problem Description: Only retain an ARP entry for the address that the DHCP client acknowledges. Do not retain addresses offered by DHCP servers that the client did not use in the ARP table.

- CSCsz82950

  Symptoms: A peer RP reloads.

  Conditions: If any configurations are done using NMS for DCTM MIB, this symptom occurs when unconfiguring the configuration that is created by DCTM MIB configuration.

  Workaround: There is no workaround.

  Further Problem Description: DCTM was not HA supported before. HA is supported now. If configurations are not done by using NMS, there will not be any issues.

- CSCsz87003

  Symptoms: Memory leaks are seen with MLP on LNS bundle.

  Conditions: Memory leaks are seen with MLP on LNS bundle on flapping the member-links.

  Workaround: There is no workaround.

- CSCsz89319

  Symptoms: Free memory is going down because SSS Manager is growing.

  Conditions: This symptom is observed on a Cisco 7600 that is used for ISG and that is running Cisco IOS Release 12.2(33)SRC3 under high network activity.

  Workaround: There is no workaround. Reload the router to free memory.

  Further Problem Description: The speed of the memory leak depends on the network activity. The more stress on the router, the faster the leak.

- CSCsz94698

  Symptoms: Router crashes while giving the **no igmp static- group** *add* **source ssm-map** command.

  Conditions: This issue is seen in Cisco 7300 (NSE100), Cisco 7300 (NPEG100), and Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsz95137

  Symptoms: The last 5000 VCs are not synced to standby when the box is configured with 62000 VCs.

  Conditions: This symptom occurs during a PRE3 HA setup.

  Workaround: There is no workaround.

- CSCsz97358

  Symptoms: A router crashes due to memory corruption.

  Conditions: The symptom is observed on a Cisco 7300 series router (with an NSE-150) that is running Cisco IOS Release 12.3(31)SB14.

  Workaround: There is no workaround.

- CSCta00720

  Symptoms: Attempting an auto proxy logon causes a crash.

  Conditions: This crash is seen only with auto proxy service download.

  Workaround: If services are activated by CoA service logon, this issue will not be seen.

  Further Problem Description: Attempting authentication of the proxy service causes a crash with traceback in description when the user profile is similar to:

```
simulator radius subscriber 1
 framed protocol ppp
 service framed
 authentication rouble-auto password cisco
 vsa cisco 250 Aproxy_service;proxy_user;welcome
 vsa cisco generic 1 string "accounting-list=default"
!
```

- CSCta05617

  Symptoms: A router crashes after executing the **show pxf cpu queue** *GigE main i/f* command.

  Conditions: This symptom occurs after removing a VLAN match class from the VLAN group QoS service policy, which was attached to a GigE main interface.

  Workaround: There is no workaround.

- CSCta08472

  Symptoms: When using PRE2 on a Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB4, ACL applied to interface fails to reject the unwanted traffic.

  Conditions: This symptom occurs when using PRE2 on a Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB4 and applying an ACL to a dot1q interface. Apply ACL to interface.

```
Access-group DENY_169 in
ACE  defined. ..
ip access-list extended DENY_169
 deny   ip 169.0.0.0 0.255.255.255 any
 permit ip any any
```

  Workaround: There is no workaround.

- CSCta15074

  Symptoms: A 2-level hierarchical policy-map does not get attached to the interface.

  Conditions: If we try to attach a 2-level hierarchical policy-map, in which the parent class has no police action but the child policy-map has a police action, the process to attach the policy-map fails.

  Workaround: There is no workaround.

- CSCta17933

  Symptoms: When NAT is done on UDP encapsulated ESP packets, the UDP checksum of the packets is incorrect.

  Conditions: This is observed on a Cisco 7300 router with PXF (NSE-100 or NSE- 150).

  Workaround:

  - Disable PXF (this may have significant performance impact).
  - Disable UDP checksum on IPSEC endpoints.

- CSCta26071

  Symptoms: A Cisco IOS platform can crash when authorizing Radius profiles. The issue is due to an invalid terminal sync change that updated the incorrect enumeration structure, leading to one enumeration having 1 too many entries and another one too few.

  When parsing the “protocol” or “service” field, the AAA code may walk beyond the boundaries of a string array associated with the above mentioned enumerations. This will cause platforms such as the Cisco ASR to crash.

  Conditions: This crash has been observed on a Cisco ASR1004 (RP2) that is running the Cisco IOS-XE version Cisco IOS Release 12.2(33)XNC1t.

  Workaround: This crash will occur if an invalid protocol or service field is provisioned in a Cisco VSA. However, even when valid protocols or services are used, it is possible that certain enumeration walking code may also trigger a crash. However, Cisco has not been able to validate that situation. As a consequence, when using branches such as Cisco IOS Release 12.2(33)SB or Release 12.2XNC, without this fix, it is critical that no invalid Cisco VSA be used.

- CSCta34812

  Symptoms: The offered rate and bandwidth allocated for all the user classes are the same, although different percentages are configured. The output rate failed to guarantee its minimum bandwidth setting.

  Conditions: The data rate for QoS bandwidth is not meeting its minimum requirement.

  Workaround: There is no workaround.

- CSCta39570

  Symptoms: A router that is running Cisco IOS Release 12.2(33)SB5 may reload by TLB (store) exception.

  Conditions: This issue was first reported on a Cisco 10000 series router using PRE3 and running Cisco IOS Release 12.2(33)SB5.

  Workaround: There is no workaround.

- CSCta73054

  Symptoms: When using passive FTP with NAT VRF, the connection is broken after NAT in the Cisco 7300. The port numbers are not consistent.

  The source port is translated from “X_PORT” to “Y_PORT”, but after NAT to the outside, the port still remains the same. This breaks the passive FTP session.

  Conditions: This issue is observed when using Cisco IOS Releases 12.2(31)SB11, 12.2(31)SB14, 12.2(33)SB3a and 12.2(33)SB5 when using VRF NAT and trying to establish passive FTP connections across the Cisco 7300.

  Workaround: No issues are observed when Cisco IOS Release 12.2(25)S11 is used. The passive FTP session and NAT behave as expected.

- CSCta89550

  Symptoms: On a Cisco 10000 series router with LI done with session brought up via radius and using SNMP session ID taps, LI is not working.

  Conditions: This happens only for using session ID taps in SNMP and bringing up sessions via radius

  Workaround: There is no workaround.

- CSCta95359

  Symptoms: Parallel **write memory** commands on two VTY sessions erase stby-nvram.

  Conditions: With latest Cisco IOS Release 12.2(33)SB image, on performing parallel **write memory** commands on two different VTY sessions, stby-nvram is completely erased.

  Workaround: With “nvbypass” configured, the problem is not seen.

Resolved Caveats—Cisco IOS Release 12.2(33)SB6

Cisco IOS Release 12.2(33)SB6 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB6 but may be open in previous Cisco IOS releases.

- CSCsh23312

  Symptoms: A Cisco 10000 series may drop MPLS packets from an ingress interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB or a later release after an FSU has occurred on a neighboring router.

  Workaround: Enter the **microcode reload pxf** command on the Cisco 10000 series.

- CSCsk04318

  Symptoms: Under the BGP router configuration mode, removing an address-family configuration and then immediately reapplying the same configuration may cause the standby RP of a dual-RP router to reload unexpectedly. Typically, the following configuration sync error will be reported:

```
Config Sync: Line-by-Line sync verifying failure on command: address-family ipv4 vrf
NAME due to parser return error
```

Removing and replacing the RD configuration under a VRF may also trigger the same type of sync error behavior, although the command listed as failing line-by-line sync will be different.

Conditions: Removal of a BGP address-family configuration triggers background cleanup processing that occurs asynchronously after the command is entered by the user. The background cleanup runs on both the active RP and the standby RP, although the cleanup may happen at different times on the active and standby. Because such background processing does not usually run in lockstep on the two RPs, a window exists after entering an address-family deconfiguration command where the active RP and standby RP are not in the same state. If the user tries to reconfigure the address-family command before both RPs have completed processing and are again in the same state, line-by-line sync may fail and cause the standby RP to reload.

Workaround: The line-by-line sync error can be avoided by allowing adequate time for the standby RP to complete background processing and arrive in an identical state as the active RP. If configuration commands are applied when both RPs are in a consistent state, the configuration sync error will not occur and the standby RP will not reload. The background processing normally happens at 60-second intervals, so waiting 2 minutes between deconfig/reconfig attempts for the same command should prevent the issue in all cases.

The line-by-line sync error and standby RP reload should not cause any service impact, as only the standby RP is affected. The active RP remains fully functional and continues traffic forwarding as usual while the standby RP reloads.

- CSCsr17660

  Symptoms: PE-CE performance degradation of 80% on initial convergence.

  Conditions: Occurs when BGP and VPNv4 are configured.

  Workaround: There is no workaround.

  Further Problem Description: Performance is not affected after initial convergence.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

  Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr96042

  Symptoms: A Cisco ASR1000 router crashes.

  Conditions: This symptom occurs if “ip vrf” is deleted from the configuration.

  Workaround: There is no workaround.

- CSCsv95474

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

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

  Workaround: There is no workaround.

- CSCsw24611

  Symptoms: A router configured with BGP and VPN import may crash.

Conditions: This is a hard to hit race condition. BGP imports a path from VRF-A to VRF-B. The following steps have to take place in exactly this order for the crash to occur:

1. The next-hop for the path has to become unreachable.
2. BGP has to re-evaluate the bestpath on the net in VRF-A and result in no-bestpath on the net (because there is no alternative path available).
3. RIB installation has to process the importing BGP net under VRF-B.

Step 3 will result in the crash. If, before step 3, the next-hop re-evaluation manages to process the net in VRF-B then it will clear the bestpath and there will be no crash. If, before step 3, the import code gets a chance to process the net it will clean-up the imported path from VRF-B and then there will be no crash.

Workaround: There is no workaround.

- CSCsw45694

  Symptoms: Cisco 10000 PRE3 and PRE4 routers use nested policy. You can apply service-policy with higher shape rate than the actual available BW to the POS or ATM interfaces.

  This problem applies to both the **shape average** *bps* and the **shape average percent** *percent_value* commands.

  The child policy will use the configured shape rate to calculate the priority police value. This will result in higher police rate.

  Conditions: This symptom occurs when shape rate is configured higher than the actual BW.

  Workaround: Configure shape rate to the actual available BW.

- CSCsw63003

  Symptoms: Memory increase occurs in “BGP Router” process due to BGP path attributes. Memory used by this process increase every day and so do the BGP path attributes while the number of routes is not increasing.

  Conditions: This symptom occurs on a provider edge (PE) router that is running Cisco IOS Release 12.2(31)SB, 12.2(33)SB, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, 12.4, 12.4T. Problem is seen with continuous churn in the network such that BGP never manages to converge and when the paths churning are not reusing existing path attributes. That will cause those paths to allocate new paths attributes.

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

- CSCsx21606

  Symptoms: On a Cisco 10000 series router that is running Cisco IOS Release 12.2(28)SB11, the serial interface becomes stuck in an up/down state and the multilink interface in a down/down state. The debugs indicate:

  ```
  Se7/0/0.10/17:1 PPP: Missed a Link-Up transition, starting PPP
  Se7/0/0.10/17:1 PPP: Updating buffered PPP packet
  Se7/0/0.10/17:1 PPP: Starting timer for fast-start
  Se7/0/0.10/17:1 PPP: Handle allocation failure
  ```

  Conditions: The symptom is observed when new T1s are added to the router. The triggers are an SSO configuration and when the router runs for a long time. The new T1s cause a lot of flapping of links.

  Workaround: Reload the router or perform a PRE failover on the Cisco 10000 series router.

- CSCsx23000

  Symptoms: Configurations on an ATM card are not removed. Tracebacks and error messages are displayed, and the router may crash.

  Conditions: This symptom is observed when you have range-pvc configured under p2p atm subifs, irrespective of the card type. With scaling configurations like 8k range VCs on each port of 4oc3atm card, the router may crash.

  ```
  hw-module slot<> shut
    no card <>
  ```

  Workaround:

  - Reload the box when the problem occurs.
  - To avoid the problem from happening, if you have p2p interface with range- pvc configurations, remove all those configurations using the **no interface** command before doing “no card”.

- CSCsx56263

  Symptoms: The **clear counter** command resets all the if-mib Object Identifiers (OIDs).

  Conditions: The symptom is observed when the **clear counter** command is issued. It is seen with Cisco IOS Release 12.2(33)SB3 and with an HHGIGE line card.

  Workaround: Reload the router.

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-2009092

- CSCsy07555

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ip

- CSCsy57066

  Symptoms: cbQosCMDropByte64 is a 64-bit counter, but it rolls over at 32-bit boundary. Due to the problem with cbQosCMDropByte64, cbQosCMPostPolicyByte64 also becomes incorrect. The counter seems to add additional 2^32 (4294967297) bytes to the counter.

  Conditions: This symptom is observed when cbQosCMDropByte64 rolls over 32-bit boundary.

  Workaround: There is no workaround.

- CSCsy58115

  Symptoms: In a router that is running BGP, the BGP process may hold increased amounts of memory over time without freeing any memory. This may also be seen from the output of **show proc mem sort** and in the output of **show ip bgp sum** or **show ip bgp vpnv4 all sum** and looking at the number of BGP attributes which may be increasing over time in relation to the BGP prefixes and paths which may remain roughly the same.

  Conditions: Some BGP neighbors are not in established state and exchanging prefixes. The issue is observed on all platforms running the following releases of Cisco IOS:

  - 12.2(31)SB14
  - 12.2(33)SB1b
  - 12.2(33)SB2
  - 12.2(33.05.14)SRB
  - 12.2(33.02.09)SRC
  - 12.2(33)SRC3
  - 12.4(20)T2
  - 12.4(22)T1
  - 12.2(33)SXI or later releases.

  Workaround: Remove the configuration lines related to the inactive neighbors (neighbors in Idle or Active states).

- CSCsy82158

  Symptoms: A corrupt multicast packet may crash the PXF on a Cisco 10000 series router with the following exception error:

  ```
  "PXF DMA Error -Small Packet Handle Creating a Large Descriptor, Restarting PXF"
  ```

  Conditions: The issue is seen when a padded multicast packet is switched by the PXF and the IP length, from the IP Header, does not include this padding.

  For example, a multicast packet where the IP length is 124 bytes and there is 436 of unaccounted padding can crash the PXF with a “PXF DMA Error”.

  Workaround: There is no workaround.

- CSCsy86078

  Symptoms: Router crashes with memory corruption.

  Conditions: Occurs when BFD is configured on 10GigE interfaces and constant link flaps.

  Workaround: There is no workaround.

- CSCsy93187

  Symptoms: CHSTM1/CHOC12 line card is crashing due to watchdog reset.

  Conditions: CHSTM1/CHOC12 line card is receiving FDL message storm from the far end just before the crash.

  Workaround: Disable the FDL interrupts permanently by writing into the interrupt enable registers of CHSTM1/CHOC12 using “poke” commands (line card CLI to write into the registers). The FDL messages are ignored completely by disabling the FDL interrupts.

- CSCsz14417

  Symptoms: The 4XCHT3 input CRC counter does not work.

  Conditions: This symptom is observed when input CRC counters do not increment when CRC is mismatched.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB5

Cisco IOS Release 12.2(33)SB5 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB5 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsy32510

  Symptoms: BGP pending prefixes may remain on the router and occupy memory even after those prefixes are withdrawn.

  Conditions: This symptom occurs when the UUT is a HA router in SSO mode.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB4

Cisco IOS Release 12.2(33)SB4 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB4 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCeg00338

  Symptoms: A high CPU utilization may occur at the interrupt level on a Cisco 10000 series when CLNS traffic is forwarded.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with an PRE-1 and that runs Cisco IOS Release 12.0(24)S6.

  Workaround: There is no workaround.

- CSCsk46534

  Symptoms: Channel over-subscription may cause a CHSTM1/CHOC12 linecard crash.

  Conditions: The symptom is observed only with over-subscribed traffic.

  Workaround: There is no workaround.

- CSCso90058

  Symptoms: MSFC crashes with RedZone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCso90970

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

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

  Workaround: There is no workaround.

- CSCsq06754

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

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

  Workaround: The crash is not seen in following cases:

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

- CSCsr75700

  Symptoms: In very rare cases, a Cisco 10000 series router crashes with a log similar to:

  ```
  %Software-forced reload Breakpoint exception, CPU signal 23, PC = 0x408FAFC0
  Possible software fault. Upon recurrence, please collect crashinfo, "show tech" and
  contact Cisco Technical Support.


  -Traceback= 408FAFC0 408F8B78 41990010 419910E0 41992DB8 42158AF4 41992EC0 41953F8C
  41956C1C
  ```

  (Note that the hex values of the traceback may be different.)

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB1.

  Workaround: There is no workaround.

  Further Problem Description: The occurrence of the problem so far has been rare. The decode of the traceback points to a BGP issue. The confirmation of whether a crash is due to this bug in BGP or not can only be made after the traceback from the crash has been decoded by Cisco support engineers.

- CSCsu42078

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

  Conditions: This happens when a service-policy is applied to an interface, and then service-policy is removed under certain conditions.

  One such condition is that “ip cef distributed” was configured on the router and the multi-link member flap triggered the service policy removal.

  The problem is that, after the policy was removed, the packet path vector was not reset correctly and still trying to access the already-removed policy internally. When traffic flows, it will cause crash.

  Workaround: For the above example, remove “ip cef distributed” from the configuration.

- CSCsu64215

  Symptoms: Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

  Conditions: Occurs when the **ip tcp adjust-mss** command is configured on the device.

  Workaround: Disable **ip tcp adjust-mss** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsv08352

  Symptoms: Some static routes are not in the IP routing table state after a stateful switchover (SSO).

  Conditions: This only occurs following a SSO event.

Workaround: Perform a **shut/no shut** of interface if the route does not come up automatically.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv73388

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

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

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

- CSCsv73509

  Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  Conditions: Configure “no aaa new-model”, configure login local under line vty 0 4, and configure login tacacs under line vty 0 4.

  Workaround: There is no workaround.

- CSCsv73754

  Symptoms: A Cisco 10000 series router crashes. Traceback decode points to a function of bgp_vpn_impq_add_vrfs_cfg_changes.

  Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 VRFs or more are unconfigured.

  Workaround: There is no workaround.

- CSCsv99653

  Symptoms: PXF may crash.

  Conditions: The symptom is observed when multicast traffic is sent over VRF on MFR subinterface.

  Workaround: There is no workaround.

- CSCsw16133

  Symptoms: SWIDBs are not cleared, even after removing the subinterfaces. Deleted subinterfaces are considered to be inactive VCs which block the configuration of the maximum number of IDs on the interface.

  Conditions: The symptom is observed when subinterfaces are created using the **range pvc** command. If the subinterfaces are deleted, this is not updated in the SWIDBs.

  Workaround: Reload the router.

- CSCsw37635

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The active router crashes when doing load version with “debug issu all” turned on.

  Workaround: Do not turn on ISSU debug.

- CSCsx25316

  Symptoms: A device may reload because of a crash at ip_ndb_owned_by_pdb after the command **clear ip route *** is executed.

  Conditions: The trigger for this issue is executing the **clear ip route*** command in the presence of a default route. If an RIP update is received by the router while the routing information base is being cleared, the update will be processed causing RIP to check the state of the default route in the routing information base. This combination has the potential to cause a crash.

  The probability of the crash occurring is proportionate to the size of the routing table. The larger the routing table, the greater the chance of encountering the problem.

  Workaround: It is recommended to avoid using the **clear ip route *** command. If the prefix in question is known, then use **clear ip route** *prefix* instead.

  Further Problem Description: This problem was observed in Cisco IOS Release 12.2(33)SRC3. All Cisco IOS SR33-based images (SRB, SRC, SRD and SB33) are vulnerable to this problem. The problem will be seen only when using the **clear ip route *** command and is platform independent. Other commands like **clear ip ospf**, **clear ip bgp**, **clear ip isis** or **clear ip route** *prefix* are not vulnerable.

- CSCsx28446

  Symptoms: PXF crash when MLPPP on LNS sends traffic through Priority Queue (PQ) Level 1.

  Conditions: The symptom is observed with MLPPP on LNS with a QoS policy applied with PQ1. No traffic passes through the virtual-access interface and if any packets match the class for PQ1 then PXF crashes. This only occurs when “ppp multilink interleave” is defined on the virtual template interface.

  Workaround: Remove “ppp multilink interleave” from the configuration in the virtual template.

- CSCsx29123

  Symptoms: An E1 flaps due to LOF/RAI alarms.

  Conditions: The symptom is observed after an upgrade to Cisco IOS Release 12.0(30)SZ from Release 12.0(28)S5.

  Workaround: Toggle the E1 clock source from line to internal or internal to line.

Alternate Workaround: Apply a local loopback then remove the loopback.

- CSCsx31786

  Symptoms: A Cisco 10000 series router that is running Cisco IOS Release 12.2(31)ZV2a may reboot or lose communication with all line cards (displaying an "IPCOIR-3-TIMEOUT" message).

  Conditions: The symptom is observed after a PPPoE session establishment and when IGMP joins to one multicast stream with many receivers.

  Workaround: There is no workaround.

- CSCsx49924

  Symptoms: On a Cisco 10000 series router with a PRE3, the throughput of a PVC (referred to as "impacted PVC") may degrade when there is too much priority traffic going through another PVC (referred to as "background PVC"). The background PVC must also have SCR below 800 kbits/s in order to impact the impacted PVC.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)SB, 12.2(33)SB1, 12.2(33)SB2 and 12.2(33)SB3.

  Workaround 1: Configure PCR greater than SCR on the impacted PVC.

  Workaround 2: Configure Maximum Burst Size(MBS)=40 on all possible background PVCs: PVCs whose SCR is below 800 kbits/s and who have a priority class (i.e., all PVCs that can trigger the issue if too much priority traffic goes through). This is the recommended workaround.

- CSCsx58335

  Symptoms: When relaying to multiple servers from an unnumbered interface, the DHCP relay sends packets to all servers, even for packets where the client is in a RENEWING state unicasting to attempt to reach a single server. ARP entries are retained for all offered addresses, even if the client is ultimately using a different address. These extra ARP entries persist for several hours.

  Conditions: The symptom is observed under the following conditions:

  1. When relaying a DHCP packet on an unnumbered interface and the DHCP client is in a renewing state (as determined by the fact that the packets are sent to the DHCP server which allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions).
  2. When the client is in any other state, or if we do not get a response from the DHCP server, the packets are sent to all helper-addresses.

  Workaround: Use Cisco IOS 12.4T images.

  Further Problem Description: Only retain an ARP entry for the address that the DHCP client ACKs. Do not retain addresses offered by DHCP servers which the client did not use in the ARP table.

- CSCsx73770

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

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

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

- CSCsx97071

  Symptoms: Multicast packets are not getting accounted.

  Conditions: The symptom is observed when sending multicast traffic. The packets are received properly, but they are not getting accounted.

  Workaround: There is no workaround.

- CSCsy22215

  Symptoms: Multicast traffic drops in MVPN setup. Mroute entry in ingress PE stays in "Registering" state.

  Conditions: The symptom is observed in an MVPN setup.

  Workaround: Configuring "ip pim fast-register-stop" in the router that is configured as RP will fix the problem in most cases.

Open Caveats—Cisco IOS Release 12.2(33)SB3

Cisco IOS Release 12.2(33)SB3 is a rebuild release for Cisco IOS Release 12.2(33)SB. This section describes a severity 2 caveat that is open in Cisco IOS Release 12.2(33)SB3. There are other open caveats in Cisco IOS Release 12.2(33)SB3. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsr75700 is an exception.

- CSCsr75700

  Symptoms: In very rare cases, a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB1 crashes with a log similar to the following:

```
%Software-forced reload
   11:00:00 bst Fri Aug 1 2008: Breakpoint exception, CPU signal 23, PC =
 0x408FAFC0
  ----------------------------------------------------------------------
     Possible software fault. Upon recurrence, please collect
     crashinfo, "show tech" and contact Cisco Technical Support.
  ----------------------------------------------------------------------
-Traceback= 408FAFC0 408F8B78 41990010 419910E0 41992DB8 42158AF4 41992EC0
 41953F8C 41956C1C
```

  Note that the hex values of the traceback may be different. The decode of the traceback points to a BGP issue.

  Conditions: The issue has not been reproducible in Cisco and not seen recently in the customer network either. No trigger has been identified. The confirmation of whether a crash is due to this bug in BGP or not can only be made after the traceback from the crash has been decoded by Cisco support engineers.

  Workaround: There is no workaround identified at this point.

Further Problem Description: The occurrence of the problem so far has been rare. After the traceback decode, Cisco support engineers can compare the decode information with what we know and have documented in this ddts to confirm it is the same issue.

Resolved Caveats—Cisco IOS Release 12.2(33)SB3

Cisco IOS Release 12.2(33)SB3 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB3 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCeb69473

  Symptoms: Device crashes with a segmentation violation (SegV) exception.

  Conditions: Occurs when the **connect** *target_ip* **[login|513] /terminal- type** *value* command is entered with a large input parameter to the *terminal-type* argument such as the following:

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa


Trying 192.168.0.1...Open
login:


*** System received a SegV exception ***
signal= 0xb, code= 0x1100, context= 0x82f9e688
PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

  Workaround: AAA Authorization AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

  For a complete description of authorization commands, refer to the following links:

  Configuring Authorization
  http://www.cisco.com/en/US/docs/ios/12_4/secure/configuration/guide/schathor.html

  ACS 4.1 Command Authorization Sets
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/SPC.html#wpxref9538

  ACS 4.1 Configuring a Shell Command Authorization Set for a User Group
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/GrpMgt.html#wp480029

  Role-Based CLI Access The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that

is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices. The following link provides more information about the Role-Based CLI Access feature:

Role-Based CLI Access
http://www.cisco.com/en/US/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.shtml

Device Access Control Due to the nature of this vulnerability, networking best practices such as access control lists (ACLs) and Control Plane Policing (CoPP) that restrict vulnerable device access to certain IP addresses or Subnetworks may not be effective. Device access best practices provide some mitigation for these issues by allowing systemic control of authenticated and unauthenticated users. Device access best practices are documented in:

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access
http://www.cisco.com/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd804ac831.pdf

Improving Security on Cisco Routers http://www.cisco.com/warp/public/707/21.html

- CSCec51750

  Symptoms: A router that is configured for HTTP and voice-based services may reload unexpectedly because of an internal memory corruption.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.3 T.

  Workaround: There is no workaround. Note that the fix for this symptom prevents the router from reloading and enables the router to generate the appropriate debug messages. The internal memory corruption is addressed and documented in caveat CSCec20085.

- CSCec72958

  Symptoms: A Cisco router that is configured for Network Address Translation (NAT) may reload unexpectedly because of a software condition.

  Conditions: This symptom can occur when the router translates a Lightweight Directory Access Protocol (LDAP) packet. NAT translates the embedded address inside the LDAP packet. This problem is strictly tied to NAT and LDAP only.

  Workaround: There is no workaround.

- CSCee63182

  Symptoms: A Cisco router may crash or may stop responding.

  Conditions: This has been always seen with an atm interface only when a rate-limit command is enabled on the interface. The crash occurs when an interface that is configured with a **rate-limit** command is deleted by entering the **no interface** command and then reenabled by entering the **interface** command.

  Workaround: Remove the rate-limit configuration from the interface before deleting the interface.

  Further Problem Description: Happens under very specific circumstances and the crash is seen randomly.

- CSCeg86665

  Symptoms: DSCP value is not being preserved when the ingress packet is encapsulated with a GRE header. The DSCP value will be rewritten to 0 as the packet egresses the router.

  Conditions: The router must be a tunnel endpoint and packets must be marked for this behavior to trigger.

Workaround: Configuring the **mls qos marking ignore port-trust** command will cause egress packets to be marked correctly.

- CSCeh75136

  Symptoms: If a user fails to successfully establish a SSH connection on the first attempt, subsequent attempts may also fail.

  Conditions: Occurs when a Cisco router is configured to authenticate SSH connections using TACACS+. The rem_addr field in the TACACS+ header may be empty if the user does not successfully authenticate on the first attempt. This may cause authentication or authorization failures if rem_addr information is required by the TACACS+ server.

  Workaround: Configure **ipssh authentication-retries 0**.

- CSCek75694

  Symptoms: A router running Cisco IOS 12.4T may reload unexpectedly

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCsb98906

  Symptoms: A memory leak may occur in the “BGP Router” process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCsc87117

  Symptoms: Bidirectional designated forwarder flaps, and packets are looped in the network for up to 20 seconds.

  Conditions: Occurs when two bidirecitonal-enabled routers are servicing the last-hop receivers on 10 or more VLANs. There should be receivers on all 10 VLANs for a minimum of 1,000 groups. When the Reverse Path Forwarding (RPF) link of active designated forwarder (DF) is shut or when the link is brought back up, DF on the receiver VLAN needs to change from one box to another box. During DF-transition, the DF-election flaps and multicast packets are looped up to 20 seconds.

  Workaround: Configure the **mls ip multicast Stub** command on the receiver VLANs on both boxes.

- CSCsc94969

  Symptoms: After configuring **import ipv4 unicast map #name** under **ip vrf #name**, all existing routes (except direct connected) under the VPN routing/forwarding (VRF) table disappear.

  Conditions: Occurs when router is configured with MPLS, VRF, and import IPv4.

  Workaround: There is no workaround.

- CSCsd04608

  Symptoms: When removing policy from interface, the router crashes.

  Conditions: Occurs when policy is hierarchical with child and grandchild policy.

  Workaround: There is no workaround.

- CSCsd80349

  Symptoms: In a MPLS Traffic Engineering Fast Reroute environment, if the line protocol on the protected link goes down due to mismatched keep-alives on the link (or too many collisions), the forwarding plane does not switch traffic for protected label switched paths (LSP) to their respective backups.

Conditions: Occur under the following scenario: - A Cisco router running a Cisco IOS Release 12.2S - Router acting as a Point of Local Repair (PLR) for MPLS Traffic Engineering Tunnels that request Fast Reroute protection - Mismatched keep-alives or excessive collisions on the protected link.

Workaround: There is no workaround.

- CSCsd82457

  Symptoms: The EapOverUDP protocol cannot detect Cisco IP conference stations and wireless phones, resulting in the policy configured locally on the box for IP phones not being applied.

  Conditions: This symptom is observed with a normal EapOverUDP configuration that is used for applying the NAC policies for IP phones.

  Workaround: There is no workaround.

- CSCse23950

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

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

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

  Workaround: Disable bridging or HW encryption.

- CSCsf21629

  Symptoms: In a system with a redundant Supervisor 720 Engine, the etherchannel member ports may flap after SSO.

  Conditions: The symptoms are observed when running LACP and on the first SSO only.

  Workaround: There is no workaround.

- CSCsg21394

  Symptoms: A router reloads unexpectedly because of malformed DNS response packets.

  Conditions: This symptom is observed when you configure name-server and domain lookup.

  Workaround: Configure the **no ip domain lookup** command to stop the router from using DNS to resolve hostnames.

- CSCsg27783

  Symptoms: When an SVI is configured with VLAN ACL and Reflexive ACL and then an ingress policy-map is applied on the same SVI, SP TCAM in ingress is programmed correctly but DFC TCAM is programmed incorrectly.

  Conditions: The symptoms are observed on a Cisco Catalyst 6000 Series Switch, or a Cisco 7600 series router that is running Cisco IOS Release 12.2SX, Release 12.2(33)SX, Release 12.2SR or Release 12.2(33)SR and that has a DFC line card.

  Workaround: Entering the **shutdown** command on the VLAN followed by the **no shutdown** will bring the VLAN to the correct state.

- CSCsg72678

  Symptoms: TCAM entries are not displayed for the interface when using the **show tcam interface acl** command.

Conditions: The symptom is observed after online insertion and removal (OIR) of the DFC module in the switch.

Workaround: There is no workaround.

- CSCsg99677

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

  File disk#:crashinfo_20070418-172833-UTC open failed (-1): Directory entries are corrupted, please format the disk

  Or the crashinfo file will be stored as CRASHI~1.

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

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

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

- CSCsh29217

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

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

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

- CSCsh37276

  Symptoms: A switch with MSFC may crash when removing SVI interfaces from the configuration.

  Conditions: The symptom is observed on a Cisco Catalyst 6000 Switch or Cisco 7600 series router that is running Cisco IOS Release 12.2SX, Release 12.2(33) SXH, Release 12.2SR or Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsh39541

  Symptoms: Traffic via ATM interface is software switched.

  Conditions: The symptom is observed if the ATM interface has both IPv4 and IPv6 addresses configured.

  Workaround: There is no workaround.

- CSCsh88532

  Symptoms: Unable to change QoS trust settings on WiSM interfaces from trust CoS.

  Conditions: When certain networks need to trust DSCP or IP-precedence, WiSM could not set qos-trust values.

  Workaround: Use manual LAG configuration to set the individual gigabit interfaces and port channels to set the QoS trust to DSCP or IP-precedence instead of WiSM default CoS.

- CSCsi54333

  Symptoms: RP inlet and outlet temperatures may display as “N/A”.

Conditions: The conditions are observed when attempting to display the environment status with the command **show environment status**. With Cisco IOS Release 12.2(18)SXF7, the RP inlet/outlet temperature sensor value displays a value of 32.

Workaround: There is no workaround.

- CSCsi57031

  Symptoms: On a pseudowire that is configured on an OC-12 ATM interface, when you delete the **oam-ac emulation-enable** command, enter the **write memory** command, and then initiate an SSO switchover, the new standby PRE continues to reboot because of a configuration mismatch with the new active PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when the new active PRE has the **oam-ac emulation-enable** command in its configuration but the new standby PRE does not, causing a configuration mismatch. The symptom may not be platform-specific.

  Workaround: Reload the new active PRE, then remove the **oam-pvc manage 0** command from its configuration.

- CSCsi57927

  Symptoms: A Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections that are hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when a **copy** *source-url* **ftp:** command is executed and the FTP server fails to initiate the FTP layer (no banner) but does set up a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

  The CLI command will time out, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and time itself out, and close the TCP connection, but the router will not clean up the TCP resources at this time.

  Workaround: Manually clear TCP resources using the **clear tcp** command, referencing the **show tcp brief** command output.

- CSCsi68795

  Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

  Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

  Workaround: There is no workaround.

  Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsi69342

  Symptoms: Whenever Netflow is enabled on interface, all packets start getting process switched and CPU utilization goes up in IP INPUT process.

  Condition: If ip route-cache flow is enabled, it causes packets to be punted to process switching.

  Workaround: Remove Netflow commands from the configuration.

- CSCsj25315

  Symptoms: When a /128 IPv6 route is added and withdrawn, CPUHOG may occur on a router.

  Conditions: The symptom is observed with the following conditions: 1. A Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB. 2. Where there are a number of prefix-length /128 routes. 3. Where there are more than two summary routes covering above the /128 routes. 4. Where there is a routing flap with a summary route that is has a longer prefix.

  Workaround: Reduce the number of /128 routes.

  Alternate workaround: Prevent a summary route flap by configuring the static summary route to Null interface.

- CSCsj49293

  Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

  Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

  Workaround: There is no workaround.

  Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsj58223

  Symptoms: Crash due to a bus error after the **show memory** command is entered.

  Conditions: Occurs on a WS-C6509-E running Cisco IOS Release 12.2(18)SXF8. It happens very rarely.

  Workaround: Do not use the **show memory** command.

- CSCsj87744

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

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

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

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

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

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

- CSCsj88665

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

  The device may also display Spurious Memory Accesses.

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

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

- CSCsk03336

  Symptoms: Interface counters on line cards may show incorrect packet input statistics in the output of the **show interface** command.

  Conditions: Occurs when the "CEF LC IPC Backg" process causes the line card CPU to exceed 90%. This is seen when an unstable network causes excessive CEF updates.

  Workaround: There is no workaround.

- CSCsk05653

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

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

  c10k-6#hw-module standby-cpu reset c10k-6# Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT) Aug 13
  14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary removed Aug 13
  14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug
  13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
  (PEER_REDUNDANCY_STATE_CHANGE) Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST:
  Standby processor fault (PEER_NOT_PRESENT) Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug 13 14:49:31.813
  PDT: %REDUNDANCY-3-IPC: cannot open standby port no such port Aug 13 14:49:32.117 PDT:
  %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 => 0x1421) Aug 13 14:49:32.117 PDT:
  %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
  (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

  Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411) Aug 13
  14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary removed Aug 13
  14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C Aug 13 14:51:33.822
  PDT: CONFIG SYNC: Images are same and incompatible

  Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer uid (2)
  is the same -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C Aug 13
  14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing Incompatibility.
  Please check full list of mismatched commands via: show issu config-sync failures mcl

  Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file: aaa group server
  radius RSIM ! <submode> "sg-radius" - ip radius source-interface GigabitEthernet6/0/0
  ```

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

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

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

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

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

- CSCsk21328

  Symptoms: Router crashes during shutdown or deletion of interface.

  Conditions: Occurs on interfaces on which IPv6 is enabled.

  Workaround: There is no workaround.

- CSCsk24854

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

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

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

  Workaround: There is no workaround.

- CSCsk25046

  Symptoms: For a policy applied to an interface with an ifindex of 14, the corresponding entry will not appear in cbQosServicePolicyTable. This is impacting device monitoring.

  Conditions: The following two conditions are required for the issue to exist:

  - There should be an interface with an ifindex of 14 with a policy applied.
  - There should a be a policy applied on the control plane.

  Workaround: Remove the policy on the control plane.

- CSCsk25838

  Symptoms: When congestion control is enabled, some CMs may get sent out of order. The actual send window size may be smaller than what is allowed by congestion control algorithm, and yet when the send window size reduces it is treated as if its size did not change.

  Conditions: The symptoms are observed at any time when congestion control is not disabled and the congestion window changes its size due to a change in network latency or processing rate.

  Workaround: There is no workaround other than disabling congestion control.

- CSCsk28361

  Symptoms: 4000 virtual-template (VT) takes high CPU during system load configuration.

  Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

  Workaround: There is no workaround.

- CSCsk39022

  Symptoms: Broadcast may not be forwarded between VLANs.

  Conditions: The symptom is observed only on Modular IOS. It is seen with Cisco IOS Release 12.2(18)SXF10, when executing the command **ip directed-broadcast**.

  Workaround: There is no workaround.

- CSCsk63794

  Symptoms: Crash may happen under regular operations as well as when changes to QoS policies are being made.

  Conditions: Occurs on a Cisco 7600 with enhanced FlexWAN module and PA-2T3+ with about 70 frame-relay PVCs in point-to-point topology.

  Workaround: Shut the interface instance before applying/removing the policy.

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsk66339

  Symptoms: A Cisco 7600 router running Cisco IOS Release 12.2(18)SFX6 may encounter a condition such that when intermediate system-to-intermediate system (IS-IS) and traffic engineering (TE) are configured, IS-IS should remove the native path from its local RIB and call RIB code to remove the path from global RIB but fails by either not passing the “delete” msg to RIB properly or RIB does not react when it received the “delete” call.

  Conditions: The **show mpls traffic-engineering tunnel** command output may indicate “Removal Trigger: setup timed out” status.

  Workaround: Perform a **shut/no shut** on the interface or change the metric temporarily to force an update with the **tunnel mpls traffic-eng autoroute metric 1** command.

- CSCsk75986

  Symptoms: A multilink bundle may go down when ACFC and PFC configurations are applied.

  Conditions: The symptoms are observed under a multilink interface on CPE and virtual-template on LNS.

  Workaround: There is no workaround.

- CSCsk80250

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

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

  Workaround: There is no workaround.

- CSCsk83505

  Symptoms: Under various circumstances, UDP input queues can grow to much larger than their intended size. This can result in memory allocation errors if the application that services a UDP input queue is unable to do so quick enough to keep up with incoming traffic. UDP needs to drop received packets, once a given input queue has reached its limit.

  Conditions: This symptom is observed with RIPv6 with a large number of neighbors in both Cisco IOS and ION images.

  Workaround: There is no workaround.

  Further Problem Description: The root cause is that several pieces of code are enqueuing packets to ipsocktypeinq without checking its size, and without updating statistics.

- CSCsk84925

  Symptoms: Platforms, such as the Cisco Catalyst 6500, are capable of dropping multicast traffic in hardware. However, in order to do so, they require that mroute entries be created by software. In the case of SSM mroutes on a first-hop router, software does not always create such entries and so this traffic cannot be dropped in hardware, resulting in high CPU utilization on the route-processor.

Conditions: This symptom will be encountered in the following scenario:

1. There are no receivers present for a given SSM (S,G) flow
2. (S1,G) has already been created
3. A directly-connected source (S2,G) starts sending traffic

That is, the first flow (S1,G) will be created and will be properly dropped in hardware if no receivers for that flow are present. Subsequent flows to the same group G will not be created and will impact the route-processor CPU.

Workaround: There are several possible workarounds to this issue:

1. Disable the mroute-cache on the incoming interface using the interface-mode command **no ip mroute-cache**. On platforms such as the Catalyst 6500, this will have no impact for hardware-switched flows.
2. Ensure that all SSM source traffic is sent to unique groups.
3. Ensure that receivers are present for all anticipated traffic.

- CSCsk86150

  Symptoms: When EIGRP goes down, BGP installs the major network in the routing table. When EIGRP comes up again, it installs the subnet routes in the routing table, while the BGP major network remains in the routing table. Also, the BGP local source route is not installed in BGP table.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(10b) and 12.4(13c) Enterprise Services images.

  Workaround: Reconfigure the network command

- CSCsk91267

  Symptoms: There are two symptoms:

  1. When you reset a WS-X6708-10GE card, you may see the following message:

  ```
  %OIR-SW2_SP-6-PWRFAILURE: Module 3 is being disabled due to power converter failure
  0x3
  ```

  2. When you turn off a power supply or due to a temporary power supply glitch, user may see a similar message:

  ```
  00:09:16: %OIR-SP-6-PWRFAILURE: Module 1 is being disabled due to power convertor
  failure 0xF
  ```

  OR

  ```
  %OIR-SP-6-PWRFAILURE: Module 2 is being disabled due to power convertor failure 0x8
  ```

  When you turn on a power supply, you do not see “power supply 1 online” message.

  Conditions: Occurs when a WS-X6708-10GE card is reset or when power is interrupted.

  Workaround: There is no workaround.

- CSCsk92854

  Symptoms: Traceback may be seen while testing L2TP scaling 32k functionality on a Cisco 10000 series router.

  Conditions: The symptom is seen with scaling scenarios and with a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCsk95969

  Symptoms: A HA router in SSO mode with both IPv6 unicast and IPv6 multicast configurations may crash while configuring IPv6.

Conditions: The symptoms is observed on an HA router in SSO mode with both IPv6 unicast and IPv6 multicast configurations, when both configurations are removed completely and then configured again.

Workaround: There is no workaround.

- CSCsk98751

  Symptoms: A router may crash after the command **mpls traffic-eng backup-path tunnel** is issued.

  Conditions: The symptom is observed when a backup tunnel is configured on PLR, which is a mid point router for a protected primary tunnel.

  Workaround: There is no workaround.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsl14450

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

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

  Workaround: There is no workaround.

- CSCsl16323

  Symptoms: Traceback with the following message displayed:

  ```
  PST: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb VRF_0_vlan1020 (if_number 132).
  ```

  Conditions: This traceback is seen after doing stateful switchover.

  Workaround: There is no workaround.

- CSCsl19708

  Symptoms: Fabric Channel may not go into sync on bootup.

  Conditions: Can occur in any environment, but error is only seen during bootup.

  Workaround: There is no workaround.

- CSCsl28246

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

  Conditions: This symptom is observed under TC sessions.

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

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

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

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

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

- CSCsl32122

  Symptoms: VPN client users using a certificate to connect to a Catalyst 6000 or Cisco 7600 with VPN blade fail to connect. IPSec negotiation fails during mode configuration.

  Conditions: Conditions are unknown at this time.

  Workaround: Preshared key authenticated VPN clients can connect without problem.

- CSCsl34481

  Symptoms: Router crashes due to IPv6 multicast routing.

  Conditions: This happens after applying multicast routing configurations, and again while unconfiguring.

  Workaround: There is no workaround.

- CSCsl40705

  Symptoms: The following tracebacks may occur on a VPDN under stress situations:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0x63249A94)
  -Traceback= 604721D4 60472718 6048C7B8 616C8CEC 616C9BA8 61AB48C4 61AB79A8 61AB8C48
  61AB8CAC 616C51DC
  ```

  Conditions: The symptom is observed in stress situations when a Call Disconnect Notification (CDN) is received immediately after a connect request.

  Workaround: There is no workaround.

  Further Problem Description: This traceback is harmless.

- CSCsl42732

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

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

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

- CSCsl44170

  Symptoms: Lawful Intercept tapped PPPoE LCP/PPP control packets originating from the router contain incorrect payload.

  Conditions: This symptom is observed on a Cisco 10000 router with radius based Lawful Intercept.

  Workaround: There is no workaround.

- CSCsl48075

  Symptoms: The floating static route behaves incorrectly in a v6 VRF. In a situation where there are two static routes via different interfaces in a v6 VRF and the Administrative Distance (AD) of one route is increased (floating static route), instead of installing the route with lesser AD as expected, the route with higher AD is installed in the routing table.

  Conditions: The symptoms are observed when there are two static routes via different interfaces in a v6 VRF and the AD of one route is increased.

  Workaround: There is no workaround.

- CSCsl48153

  Symptoms: When the CNS image retrieve operation is performed, the router may not download the associated image from the image server.

  Conditions: The symptom is observed when Image Server holds a valid image for the device.

Workaround: There is no workaround.

- CSCsl51380

  Symptoms: Sup720 has periodic consistency checker for TCAM and SSRAM, from shadow to hardware which write to hardware when an inconsistency is detected between shadow and actual hardware. However, on a Sup720 and a Sup32 there is no verification to check whether the write was successful, and no syslog or notification is given to notify persistent hardware entry failures.

  Conditions: The symptoms are observed on a Sup720 and Sup32.

  Workaround: There is no workaround.

- CSCsl57023

  Symptoms: PVC recreation may fail after a switch-over occurs on a Cisco 7600 series router and a new active is reset.

  Conditions: The symptom is observed when a switch-over occurs on a Cisco 7600 series router from active to standby.

  Workaround: There is no workaround.

- CSCsl60092

  Symptoms: Router crashes as the client is trying to return a fragmented message but not the last fragment.

  Conditions: Seen on a system running stress test with Layer 3 unicast/multicast and Layer 2 traffic with 5K OSPF, 20K BGP routes, 10K IGMP groups, 98K mac addresses. Running a script to **shut/no shut** VSL control port every 5 seconds and wait 10 seconds between different ports on both the active and the standby, the crash was seen on active SP about 3 hours into the test.

  Workaround: There is no workaround.

- CSCsl61806

  Symptoms: When the sum of EIRs of all BW queues under an ESM20 line card exceeds 549Gbps, the following message may be produced: "EXCEEDEXCESSQRATE".

  Conditions: The symptom is observed in an environment which has a large configuration with 1000 EVCs with WRED-configured policymaps under a PC interface. When the WRED is removed from a class which has a shape rate, a number of exceed excess error messages are seen. When the **shutdown** command is executed followed by the **no shutdown** command on the PC interface, most of the queues go to pending state with the exceed excess error message flooding the screen.

  Workaround: Changing either the shape rate or adding the WRED back to the class-map will resolve the problem. Reloading the line card will also recover this problem.

- CSCsl62076

  Symptoms: Configuring IPv6 RIP on a router may cause the router to crash.

  Conditions: The symptom is observed on a Cisco 10000 series router when configuring IPv6 RIP.

  Workaround: There is no workaround.

- CSCsl62341

  Symptoms: The configuration command **ip summary-address rip** is not applied by radius configuration as part of the lcp:interface-configuration.

  Conditions: This symptom is observed only when the lcp:interface- configuration is used in combination with other AVPairs that perform an interface-specific configuration. For example, the last four AVPairs shown below use a mix of lcp:interface-configuration and interface-specific AVPairs: xxxxx@xxxx2001 Password = "xxxx" Service-Type = Framed-User, Framed-Protocol =

PPP, Framed-IP-Address = 10.17.1.1, Framed-Routing = listen, av-pair = "ip:description=sub-VAI ppp1", av-pair = "ip:vrf-id=X2001", av-pair = "ip-unnumbered=Loopback2001", av-pair = "lcp:interface-config=ip summary-address rip 10.17.1.0 255.255.255.0"

Workaround: If you require a summarized address to be advertised via RIP to CPEs, ensure that the lcp:interface-configuration command/attribute is used for all interface specific configurations, as this issue occurs when the interface specific commands/attributes are mixed between the AVPairs and the lcp:interface-configuration commands. The interface profile should be applied before applying any IP configuration profiles.

- CSCsl62344

  Symptoms: If a contact phone number is configured to be 12 digits long, the configuration will fail. If the configuration is already in the running- configuration, the call-home configuration will lost after reload.

  Conditions: The symptom is observed when the call-home contact phone number is configured to be 12 digits long.

  Workaround: Add a white space in the contact phone number to make it at least 13 digits long.

- CSCsl63212

  Symptoms: L2TP network server (LNS) router crashes while establishing virtual private dial-up network (VPDN) and shutting down client interface.

  Conditions: Occurs while making call from client to LNS with specific configurations.

  Workaround: There is no workaround.

- CSCsl63311

  Symptoms: On a Cisco Catalyst 6500 Series Switch, NAT traffic may be software switched. This may result in high CPU utilization.

  Conditions: The symptom is observed when the NAT traffic egress on an interface is configured as an ISL L3 sub-interface.

  Workaround: Use DOT1Q instead of ISL.

  Alternate Workaround: Make the connection a Layer 2 ISL trunk and create an SVI for each sub-interface.

- CSCsl63494

  Symptoms: AAA server does not count active user sessions correctly. User authentication may be denied by the AAA server because max session limit has been reached.

  Conditions: This may occur with AAA authentication, when max session limit is configured on Cisco Secure ACS server (may happen with other AAA servers too). When user initiates X.25,ssh,rsh,rlogin or telnet sessions and later disconnects them, AAA server does not decrement active sessions counter due to wrong attributes present in the accounting records sent by the device. Eventually, the misbehaving counter may reach max session limit, and user will be denied a login.

  Workaround: Removing max session limit can be considered.

- CSCsl65179

  Symptoms: Setting priority queue limit for PFC QoS configurations resets non- priority queue limits to default values.

  Conditions: The symptom is observed when changing the priority queue limit for PFC QoS to the default setting. If CoS values are mapped to queues with default queue limits of zero, then traffic with these CoS values will be dropped until non-default configuration is reapplied.

  Workaround: After changing the priority queue limit, reapply non default non- priority queue limits.

Further Problem Description: Setting the priority-queue queue-limit to the default values via the **no priority-queue queue-limit** or **default priority-queue queue-limit** commands sets the WRR queue limits to default values. This action has the side effect of dropping all traffic mapped to queues 4 and 5 until the WRR queue limits are reconfigured.

- CSCsl65327

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

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

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

- CSCsl70722

  Symptoms: A router running Cisco IOS may crash due to watchdog timeout.

  Conditions: Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

  Workaround: There is no workaround.

- CSCsl70963

  Symptoms: Whenever there is member link updates and/or parent class policy-map modification which involves bandwidth change, the bandwidth change will not be reflected on the SIP2 line card.

  Conditions: The symptom is observed on any hardware switching platform/line card, such as SIP-400.

  Workaround: Use priority and with absolute-value (explicit) policer.

- CSCsl72285

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

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

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

- CSCsl77067

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

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

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

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

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

  and then:

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

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

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

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

- CSCsl80682

  Symptoms: VPN SPA crashes when encryption ACLs are modified.

  Conditions: Was seen happening when GRE takeover configured (GRE acceleration being done by SPA):

  crypto engine gre vpnblade

  Workaround: Configure GRE acceleration to be done by supervisor:

  crypto engine gre supervisor

- CSCsl80870

  Symptoms: While bringing up 20 MLPoATM bundles with 10 member links, a few member links fail to come up.

  Conditions: This symptom occurs when some of the member links are inactive when the bundles come up.

  Workaround: There is no workaround.

  Further Problem Description: The cause for this issue is the bundle auth type does not match with the current links auth type. The current link name does not match the bundle first link name. CONFREJ is sent, and the member is removed from the bundle.

- CSCsl83212

  Symptoms: Traceback error message is shown every 10 seconds in the log on both Active and Standby RPs:

  ```
  *Dec 17 20:48:47.342: assert failure: NULL!=tinfo: ../const/common-
  rp/const_macedon_tunnel.c: 3875: macedon_tunnel_check_takeover_criteria
  ```

  ```
  *Dec 17 20:48:47.342: -Traceback= 42C53118 42C59EB0 42C61938 42C621CC
  ```

  Conditions: This symptom is observed when an autotemplate interface is deleted from router configuration.

  Workaround: Recreating the same autotemplate interface that is being deleted will stop this traceback error message.

- CSCsl86316

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

  Conditions: The symptoms are observed in an L2TP scenario

  Workaround: There is no workaround.

- CSCsl87404

  Symptoms: L2TP tunnels are not getting established.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsl87935

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

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

  Workaround: There is no workaround.

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

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

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

- CSCsl92316

  Symptoms: Router may experience mwheel CPUHOG condition.

  Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

  Workaround: There is no workaround.

- CSCsl95609

  Symptoms: When a VRF which has BGP multipath that has been defined using the **address-family ipv6 vrf** *vrf-name* command is deleted, alignment tracebacks may be seen on the console.

  Conditions: The symptom is observed on a VPNv6 with BGP multipath defined.

  Workaround: There is no workaround.

- CSCsl96254

  Symptoms: If an EIGRP distribute-list that is applied to an interface allows a route, the route will be installed into the routing table without first checking to see if the global distribute-list allows it as well. All platforms are affected.

  access-list 1 permit any access-list 2 deny any

  router eigrp 1 network 192.168.1.0 0.0.0.255 distribute-list 1 in FastEthernet0/0 distribute-list 2 in no auto-summary

  The configuration above should deny all routes by virtue of access-list 2. Instead, all routes are allowed per access-list 1.

  Conditions: Running EIGRP with interface distribute lists and a global distribute list. All platforms are affected.

  Workaround: Currently the only workaround is to apply the global distribute list to each interface distribute list.

- CSCsl96370

  Symptoms: A CPUHOG message may be seen.

  Conditions: This symptom is observed when the following three conditions are met:

  1. HSRP debugs are enabled.

  2. The router is logging to console.

  3. An interface with more than 50 HSRP groups is shut down.

  Workaround: There is no workaround.

- CSCsl97384

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

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

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

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

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

- CSCsl99156

  Symptoms:

  1. The No_Global bit (0x10) for MOI flag is incorrectly set for iBGP when it becomes best path.

  router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions: MOI flags = 0x16 <-------MOI flags 0x10 is incorrectly set for iBGP when it becomes best path, correct flag should be 0x4, 0x5, 0x6 ... correct now.

  2. The No_Global bit (0x10) for MOI flag for iBGP path was incorrectly unset when eBGP becomes best path.

  router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions: MOI flags = 0x5 <-------MOI flags 0x10 is incorrectly clear for ibgp path when eBGP becomes best path, correct flag should be 0x14, 0x15, 0x16... correct now.

  Conditions: This symptom sometimes happens after BGP path update.

  Workaround: Issue the **clear ip route vrf** *vrf name* **x.x.x.x/y command.**

- CSCsm00570

  Symptoms: FlexWAN card crashes after a service policy is attached to sub-interface in which mulitlink is configured, followed by **shut/no shut**.

  Conditions: This problem requires both a QoS configuration change and an interface flap to happen at the same time. It is not likely to happen in production environments.

  Workaround: There is no workaround.

- CSCsm01126

  Symptoms: The standby fails to come up in SSO. The following message is seen on the active:

  %FILESYS-4-RCSF: Active running config access failure (0) <file size>

  Conditions: This symptom is observed when the router has a configuration greater than 0.5 megabytes.

  Workaround: There is no workaround.

- CSCsm01577

  Symptoms: When an OC-3 CEoP SPA has a large IMA configuration, a SPA Online Insertion and Removal (OIR) will sometimes cause a number of groups to remain down. A SIP-400 OIR is required to bring the groups up.

  Conditions: The symptom is observed when OC-3 CEoP SPAs are configured with IMA in a back-to-back connection, and traffic is passing. In this situation, a SPA OIR will cause IMA groups to remain down.

  Workaround: Perform an OIR on the SIP-400.

- CSCsm04442

  Symptoms: Delete an interface which has ip summary-address rip configured. The router crashes.

Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm14833

  Symptoms: All incoming ISDN calls are rejected.

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

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

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

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

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

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

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

- CSCsm15350

  Symptoms: The VPNSPA may crash with an assert failure.

  Conditions: The symptom is observed when B2B is configured and when creating 8000 remote access sessions.

  Workaround: There is no workaround.

- CSCsm17066

  Symptoms: One of the GLBP forwarders for a group may experience a state flap between two of the group members.

  Conditions: The symptom is observed after SSO occurs on a router in which the pre switch-over state for GLBP is "LISTEN". The forwarder which is assigned to this group member will experience the flap. It will only occur on setups where there are more than two GLBP group members.

  Workaround: There is no workaround.

- CSCsm21126

  Symptoms: A Cisco 7600-SSC-400 may not recover from a fabric error.

  Conditions: The symptom is observed when an error is present in the fabric channel. The fabric errors can be observed by executing the command **show platform hardware** *ssa fabric-monitor history.*

  Workaround: There is no workaround.

- CSCsm21435

  Symptoms: Clock accuracy goes out of conformance when the reference clock is reverting from the secondary source to the primary after a switchover.

  Conditions: Occurs when dual Circuit Emulation over Packet (CEoP) cards are receiving reference clock via each one’s BITS-IN.

Workaround: There is no workaround.

- CSCsm23160

  Symptoms: The standby RP may unexpectedly reload and issue the following traceback: %SCHED-2-SEMUNLOCK: rf task attempted to unlock semaphore owned by interrupt.

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

  Workaround: There is no workaround.

- CSCsm23560

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

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

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

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

- CSCsm26130

  Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.

  Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

  Workaround: There are four possible workarounds:

  1) Use an "aggregate-address" configuration instead of the static route to generate the summary. 2) Remove auto-summary from the BGP process. 3) Enter the **clear ip bgp *** command. 4) Remove and reconfigure the BGP network statement for the summary route.

- CSCsm26610

  Symptoms: A router running Cisco IOS may unexpectedly reload.

  Conditions: This is specific to platforms with powerpc processors, such as the npe-g2 and 2600xm series routers. It requires either the legacy rate-limit config or MQC style policer configured on an interface.

  Workaround: There is no workaround.

- CSCsm37834

  Symptoms: ES20 or SIP600 cards may reset with the following error:

  ```
  %EARL-DFC7-2-SWITCH_BUS_IDLE: Switching bus is idle for 5 seconds. The card grant is 0
  ```

  Conditions: The symptom is observed when performing an RPR switchover or "test crash" on the active supervisor. It is seen in HFS-enabled chassis (such as S-chassis or infinity chassis).

  Workaround: There is no workaround.

  Further Problem Description: The problem occurs because of a loss of synchronization on the switch fabric. This results in the loss of EARL heartbeat packets causing the EARL recovery process to complain that a bus stall has occurred when it finds that no heartbeat packets have been received.

- CSCsm40666

  Symptoms: Using the **excute-on** command on SUP to PPC may cause the device to hang in some cases.

  Conditions: This happened when the SUP process is busy with CLI process, including the case where CLI-intensive management application is running.

  Workaround: Open another Telnet session enter the same **execute-on** command. This will release the first hung **excute-on**.

- CSCsm41873

  Symptoms: Device crashes when VPN routing/forwarding (VRF) is unconfigured.

  Conditions: MCP Router crashes while unconfiguring **ip vrf vrf name** with a script.

  Workaround: There is no workaround.

- CSCsm44147

  Symptoms: The standby WS-SUP720-3BXL failed to boot into SSO mode because of MCL check failure with the FPD configuration command: **upgrade fpd path sup-bootdisk:**

  Conditions: The problem happens when "sup-bootdisk:" is used as the FPD image package directory path argument in the **upgrade fpd path** *pkg-dir-path* configuration command for an active WS-SUP720-3BXL that supports "sup-bootdisk:" filesytem, but the same fiilesystem is not support by the standby WS-SUP720-3BXL.

  Workaround: For systems that have a mixture of old and new WS-SUP720-3BXL, please do not use "sup-bootdisk:" as the filesystem in the **upgrade fpd path** *pkg-dir-path* configuration command, instead use the "sup-bootflash:" filesystem as this filesystem exist on both old and new WS-SUP720-3BXL.

  Further Problem Description: The **show module** EXEC command can be used to identify the HW revision of the WS-SUP720-3BXL, if it does not have a version above 5.x then it won't have the support of the "sup-bootdisk:" filesystem.

- CSCsm44620

  Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

  Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

  Workaround: Remove the following configurations:

  a. rpm-xfh10-z135 - shut & remove interface Switch1.4073 b. rpm-xfh09-z134 - shut & remove interface Switch1.4073 c. rpm-xfp11-l172 - remove interface Switch1.3172 d. rpm-xfp13-z074 - remove interface Switch1.4074 e. rpm-xfp04-l171 - remove interface Switch1.3171

- CSCsm44905

  Symptoms: CPU Hog messages may be seen when QoS is configured on a number of subinterfaces

  Conditions: The symptom is observed in a scaled configuration with 4,000 subinterfaces having QoS applied, when a "match" statement is dynamically added or removed from the QoS class-map.

  Workaround: There is no workaround.

- CSCsm45390

  Symptoms: A Cisco IOS software crash may occur when receiving a specific malformed DHCP packet.

  Conditions: An IOS device configured for DHCP Server and receives a DHCP-request from a DHCP relay device. A specific malformed option in the packet packet may induce a software traceback or crash. The specific packet will not occur without manual modification.

  Workaround: There is no workaround.

- CSCsm46170

  Symptoms: Upon the execution of the **test crash** command on the active supervisor in an HFS capable chassis, the new active fabric channel may go out of synchronization, the line card shows up minor errors with the **show mod** command, the traffic stops passing through the line card, and the following error message may be seen: %FABRIC_INTF_ASIC-5-FABRICSYNC_REQ: Fabric ASIC 0: Fabric sync requested after 3 sync errors

  Conditions: The symptoms are observed on an HFS-capable chassis and are triggered by the **test crash** command on the active supervisor. It is seen with both SIP200 and SIP400.

  Workaround: There is no workaround. The only way to come out of the problem state is with a line card reset using the **hw-module module** *slot* **reset** command.

- CSCsm48357

  Symptoms: When FlexWAN card configured for Frame Relay over MPLS (FRoMPLS) is subjected to online insertion and removal (OIR), the standby will crash when FRoMPLS is unconfigured.

  Conditions: Occurs when FRoMPLS is unconfigured following an OIR.

  Workaround: There is no workaround.

- CSCsm50317

  Symptoms: Service policy counters stop updating after applying a service policy.

  Conditions: The symptom is observed when applying service policy with ACL to virtual template. The policy-map counters become stuck at zero.

  Workaround: Remove the policy and reapply.

- CSCsm50741

  Symptoms: When a non-DC router is removed from a DC enabled area and the area becomes DC enabled, some of the LSAs are not refreshed correctly with DoNotAge (DNA)bits set. Crash may happen when customer deploys iptivia probes in the network. Fixed in CRS.

  Conditions: The symptom is observed when a router without DC capability is removed from a DC enabled area.

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

- CSCsm53035

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

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

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

- CSCsm61571

  Symptoms: When the optical RX level changes such that is out of the supported threshold or a mismatched combination of XFPs used at ends (eg: ZR to LR, SR to LR etc), then the line card CPU utilization becomes very high at the interrupt level. This greatly contributes to exhaustion of line card CPU resources and results in failure to process heartbeat keepalives. As a result, line card is eventually reset by the SP to attempt recovery. Cause of the CPU being so frequently interrupted are the continuous interface state transitions which are triggered by the line card.

  Passing CLIs to the line card fail:

  7600#remote command module 2 sh proc cpu sort No response from remote host 7600#

  SP fails to receive heartbeat checks from the ES20 LC and eventually crashes

  %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 30 seconds [2/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 60 seconds [2/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 90 seconds [2/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 120 seconds [2/0] %CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 150 seconds [2/0] %OIR-3-CRASH: The module in slot 2 has crashed

  When unplugging the fibers, LC becomes responsive, but shows high CPU in interrupt:

  7600# 7600#remote command module 2 sh proc cpu sort | e 0.00% 0.00% 0.00%

  CPU utilization for five seconds: 99%/96%; one minute: 36%; five minutes: 23% PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process 124 59128 542 109092 2.19% 2.17% 2.30% 0 Vlan Statistics 134 221872 1057 209907 0.42% 8.74% 10.38% 0 CFIB LC STATS Ta 127 24072 3340 7207 0.18% 0.20% 0.17% 0 BW Stats Poll 213 1628 177 9197 0.12% 0.07% 0.05% 0 sip10g Stats Bac 173 7208 634 11369 0.12% 0.01% 0.00% 0 TCAM Manager pro 193 1240 177 7005 0.12% 0.05% 0.05% 0 MFI LFD Stats Pr 172 2488 373 6670 0.12% 0.08% 0.09% 0 QoS SP Process 104 440 87 5057 0.12% 0.04% 0.01% 0 xcvr RPC process

  Conditions: Occurs on a Cisco 7600 router with a XFP-10GZR-OC192 housed in a ES20, where the optical fiber has its RX level out of the specified range for the given XFP being used.

  Workaround: Verify the optical properties of the fiber using the **sh hw-module subslot X/Y transceiver Z stat** command. If out of range, replace with optical fibers for which the optical transmission properties are within the specified range for the given XFP being used.

- CSCsm61726

  Symptoms: Adaptive clock stays in HOLDOVER state and does not get to an ACQUIRED state.

  Conditions: The symptom is observed when using adaptive clock through an MLPPP interface. The same configuration with POS interfaces (instead of an MLPPP interface) will allow the adaptive clock get to an ACQUIRED state.

  Workaround: There is no workaround.

- CSCsm62179

  Symptoms: MPLS pseudowire ping for SVI Mode Ethernet over MPLS over GRE (EoMPLSoGRE) may fail.

  Conditions: The symptom is observed if EoMPLSoGRE is configured with SVI mode.

Workaround: There is no workaround.

- CSCsm63632

  Symptoms: Watermark and XDR error messages indicating a failure to create IPC buffers are seen, such as: %XDR-6-XDRIPCPEER: XDR IPC error occurred for peer in slot 3/0 (3) due to inability to create an IPC buffer. %IPC-5-WATERMARK: 1123 messages pending in xmt for the port Slot 3: FAST.control.RIL(2030000.11) from source seat 2160000

  Conditions: The symptom is observed when the router is under stress by route flaps and linecard resets (DFC enabled) to create repeated downloads of the CEF tables to the linecard(s). This creates large amounts of IPC traffic. Only releases prior to Cisco IOS Release 12.2(33)SRB3 are affected by this issue.

  Workaround: There is no workaround, but XDR will recover from the situation gracefully without losing any messages.

  Further Problem Description: It is not clear if other applications that fail to get IPC buffers during this period will recover gracefully or not.

- CSCsm69981

  Symptoms: ISG is not allocating the next free port in the cyclic order as expected.

  Conditions: The symptom is observed on PC clients using a web-portal. It is observed when the browser is shutdown and a new one started within 60 seconds and when the web-server timeout is set for 60 seconds.

  Workaround: Adjust the web-server TCP port allocation timers to match that of the ISG and PC clients.

  Further Problem Description: ISG allocates a free port in a port-bundle when a subscriber sends a TCP SYN packet. The port is freed after around 60 seconds. After this, if the same subscriber sends a TCP SYN packet (in order to establish a new session), ISG allocates the freed port and not the next free port in the cyclic order.

- CSCsm70774

  Symptoms: The router crashes when a kron policy-list is modified from the console after that kron policy-list has been deleted by another user on a different vty.

  Conditions: This symptom can be observed on a Cisco router when the **kron policy-list** *word* is issued from the console and removed from the VTY. Using the command **cli** *abcd* in the console, while still in the **kron policy-list** *word* mode, causes the router to crash.

  Workaround. There is no workaround.

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

  Workaround: There is no workaround.

  Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

  pseudowire-class ER1_to_HR1_EoMPLS no preferred-path interface Tunnel501331 disable-fallback ! interface tunnel501331 shutdown ! no interface tunnel501331

- CSCsm73602

  Symptoms: High CPU load due to VTEMPLATE Backgr process.

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

  Workaround: There is no workaround.

- CSCsm74143

  Symptoms: INTR_MGR-DFC7-3-BURST: msg seen when PMAP is removed from subinterface.

  Conditions: Occurs on a ES20 LC with subinterface having a HQoS policy applied. The steps are:

  1) Remove the child policy from the parent class.

  2) Remove the service-policy from the subinterface.

  Workaround: Apply the service-policy again in the interface and remove the policy.

- CSCsm77558

  Symptoms: A "NODESTROYSUBBLOCK" error message is seen when the SWIDB is being reused and subblocks are still attached to the SWIDB.

  Conditions: The symptom is seen typically in thrashing situations or whenever sessions are being disrupted.

  Workaround: There is no workaround.

- CSCsm78184

  Symptoms: The standby router may reload unexpectedly during synchronization, after a synchronization failure.

  Conditions: The symptom is observed during the MIB synchronization to standby.

  Workaround: There is no workaround.

- CSCsm78539

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

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

  Workaround: There is no workaround.

- CSCsm82382

  Symptoms: A memory leak is seen on the Standby RP. If the memory leak is very high, CEF gets affected and finally gets disabled due to lack of memory. (It may take a few thousand such operations before the CEF gets disabled.)

  Conditions: The symptom is observed on a Cisco Catalyst 6500 series switch and the Cisco 7600 series router and while using 6348 linecards. The leak is seen in some port operations, such as port mode and port state changes.

  Workaround: There is no workaround.

- CSCsm83961

  Symptoms: BFD for eBGP neighbors may not be enabled after an SSO switchover. Specifically, BFD sessions for eBGP neighbors that are up before an SSO switchover may not be present after an SSO switchover.

Conditions: The symptom is observed with NSR peers on platforms that do not yet support BFD for SSO. When **neighbor** *ip- address* **ha-mode sso** and **neighbor** *ip-address* **fall-over bfd** are both configured for a neighbor, BFD is only enabled on the active RP. The fact that BFD has been enabled may be lost after issuing a forced switchover (even though the configuration is present and correct).

Workaround: Configuring/re-configuring the **neighbor** *peer-ip-address* **fall-over bfd** command after the switchover will enable BFD for eBGP NSR peers. Rebooting the router will also have the same effect.

Further Problem Description: Note that since BFD SSO is not yet supported, using both BFD and NSF for BGP simultaneously may cause BGP sessions to go down (and come back up) after an SSO switchover.

- CSCsm85197

  Symptoms: CE routes learned through a GRE tunnel may not be installed in the VRF routing table.

  Conditions: The symptom is observed when the GRE tunnel configurations are changed from unnumbered to numbered and back to unnumbered.

  Workaround: There is no workaround.

- CSCsm87634

  Symptoms: In the police flow command, the burst value may be different from the value that was inputted.

  Conditions: The symptom is observed when using the higher ranges of burst values, since the value is right-shifted before making a capability check.

  Workaround: There is no workaround if values closer to the upper limit are used. Additionally, if cir=128000, the issue will not occur as cir%8000 is 0 and hence the police factor is 0, so the right-shift does not take effect.

- CSCsm87702

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

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

  Workaround: There is no workaround.

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

- CSCsm87721

  Symptoms: Dialer Cisco Express Forwarding (CEF) with IP accounting fails with packet counters returning zero for the member interface.

  Conditions: This happens when **ip accounting output-packets** configured on NAS. The NAS is being checked for **show adjacency detail** which returns 0 packets and 0 bytes for the member interface.

  Workaround: There is no workaround.

- CSCsm87959

  Symptoms: An HSRP IPv6 address may become :: if the IP address of an interface is changed.

  Conditions: At least one HSRP IPv4 group should exist on the interface.

  Workaround: Delete the group completely from the configuration, and then reconfigure it.

Once the problem occurs, the HSRP IPv6 group must be deleted and re-added.

- CSCsm89526

  Symptoms: When a new class-map configuration is added to policy-map, packet (which belongs to another existing class) drop issue will be observed.

  Conditions: Occurs on a Cisco 7600 router with ES20 and running Cisco IOS Release SW 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsm89795

  Symptoms: The router keeps reloading and complaining about unavailability of memory.

  Conditions: This symptom is observed if the router is directly connected to a DHCP server or if an attack is made by flooding DHCP replies.

  Workaround: There is no workaround.

- CSCsm93068

  Symptoms: A large number of interfaces (10,000 or more) in a VRF might lead to long boot-up times and CPU hogs.

  Conditions: The symptom is observed if there is a large number of interfaces in a VRF.

  Workaround: There is no workaround.

- CSCsm93513

  Symptoms: Cannot configure queue-limit if more than one class has priority (with different priority levels) configured.

  Conditions: This is a new feature. Initially there was only one priority level supported, so only one queue was maintained. Queue-limit configurations were blocked if there were more than one priority class in the policy. Now that additional priority levels are supported, this configuration should be supported.

  Workaround: There is no workaround.

- CSCsm95129

  Symptoms: The **no ip next-hop-self eigrp** command does not work after mutual redistribution with BGP (either iBGP or eBGP).

  Conditions: This has been observed on any platform. The combination RIP/EIGRP or OSPF/EIGRP works instead.

  Workaround: There is no workaround.

- CSCsm95145

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

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

  policy-map type control RULEB class type control MATCH_PRE_1 event credit-exhausted 1 service-policy type service name DOWN_DEF_TC1_V1 ! class type control MATCH_PRE_2 event credit-exhausted 1 service-policy type service name DOWN_DEF_TC2_V1 !

  Workaround: There is no workaround.

- CSCsm95456

  Symptoms: Duplicate L3 packets may occur on a Cisco Catalyst 6500 switch.

  Conditions: The symptom is observed on a Cisco Catalyst 6500 switch, configured with an L2 Distributed Ether Channel (DEC) and with WS-X6708 blade (s) installed. This issue is due to the mix of 3A/3B and 3C PFC/DFC (and will not occur in a pure 3A+3B or 3C PFC/DFC system). It occurs when: 1. There is a mix of 3C and 3B (or 3A). 2. There is at least one L2 DEC in the system.

  Workaround: Do not use an L2 DEC.

- CSCsm96355

  Symptoms: A Cisco 7600 running a Cisco IOS Release 12.2SR image might experience a small amount of packet loss (about 10-20 ms) during TE-FRR reoptimization. This happens only for EVC (Ethernet Virtual Circuit) or scalable Ethernet Over MPLS (EoMPLS) configurations with large number of traffic engineering (TE) tunnels.

  Conditions: This issue happens only for traffic going over EVC or scalable EoM VCs when the box has scaled configuration, such as a large number of TE tunnels.

  Workaround: There is no workaround.

- CSCsm96785

  Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).

  Conditions: This occurs with the following conditions: - "nsf cisco" is only affected. If "nsf ietf", this problem does not occur. - You may observe this problem if the OSPF interface is "point-to-multipoint non-broadcast" or "point-to-multipoint". If the interface is "broadcast", this problem does not occur. - When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.

  Workaround: Change the OSPF config to "nsf ietf" and change the OSPF interface to "broadcast".

- CSCsm96842

  Symptoms: The command **hold-queue** *length* **in** cannot be configured for port-channel interface.

  Conditions: The symptom is observed with a Cisco 7600 series router after upgrading to Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

  Further Problem Description: Queueing is not supported for port-channel with a Cisco 7600 series router. The hold-queue is a legacy queueing command and is not supported.

- CSCsm97297

  Symptoms: Output direction ACL does not work.

  Conditions: Occurs when **ip cef accounting** is enabled on a MPLS enabled router doing tag disposition. If packets coming in are tagged, and they are going out of the router as untagged, the output IP ACL may not work.

  Workaround: Reconfigure the static route or clear the route.

- CSCsm99079

  Symptoms: The kron process may generate the following syslog and cause the device to reload:

  ```
  Dec 30 23:47:31.920: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (1/0),process = Kron Process.
  -Traceback= 0x42725288 0x42725778 0x42724AC0 0x41E0D72C 0x41E0E0BC 0x41E0E3FC
  ```

  Conditions: The symptom is observed when the command **kron** is configured with the *at* parameter.

Workaround: Try redesigning the **kron** command to use the *in* parameter.

- CSCso00793

  Symptoms: Enhanced-Flexwan crashes with cache error with MEM-CC-WAN-512M=, version "VI4DP647228EBK-MD" installed.

  Example of Symptom: Cache error detected! CP0_CAUSE (reg 13/0): 0x00004000 CPO_ECC (reg 26/0): 0x40000000 Data cache error CPO_BUSERRDPA (reg 26/1): 0xFFDFFFE0 CPO_CACHERI (reg 27/0): 0x200011C0 Tag address parity error Instruct cache index 0x0000008E CPO_CACHERD (reg 27/1): 0x840000A0 Multiple data cache errors External cache error Data cache index 0x00000005 CPO_CCHEDPA (reg 27/3): 0x09271600

  Interrupt exception, CPU signal 20, PC = 0xA0000100

  -Traceback= 40723DA8 406AF1B0 406B5BC8 406BAAF8 406BC200 406B4788 4072AA0C 4011D870 4012D204

  Conditions: This issue is seen under certain conditions, which are not fixed. No specific trigger.

  Workaround: There is no workaround.

- CSCso03047

  Symptoms: The multilink interfaces stop forwarding traffic, and the serial interfaces out of the multilink start to flap.

  Conditions: This symptom is observed when the E3 controller is saturated.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the controller.

- CSCso04897

  Symptoms: The traffic passing in a class may be less than the configured bandwidth.

  Conditions: The symptom is observed when 100 percent bandwidth is assigned to user-classes. It is seen only on SIP-200 with Serial interfaces.

  Workaround: Reserve at least one percent of bandwidth for class-default.

  Further Problem Description: The same policy was applied to a an ATM interface on a SIP-400 using 2xOC3 ATM SPA and the flows were fill as expected.

- CSCso04932

  Symptoms: Traffic is lost for up to 30 seconds on a static route with next hop over ATM interface.

  Conditions: Occurs when next hop goes over an ATM interface.

  Workaround: There is no workaround.

- CSCso06402

  Symptoms: Unconfiguring the router may force the router to crash.

  Conditions: The symptom is observed when unconfiguring the router and where the route-map is configured with DF bit set/unset.

  Workaround: There is no workaround.

- CSCso09607

  Symptoms: All or some of the following symptoms may be experienced: 1. Crash could occur during GTPLB sticky timer expiration. 2. Crash could occur if **show ip slb sticky gtp imsi** command is issued. 3. "%SLB-4-UNEXPECTED: Unexpected error: real num_clients counter already 0"

message might be displayed. 4. Unexpected timer expiration for the same sticky object could occur. This could be realized only with **debug ip slb sticky gtp imsi**. The frequency of expiration might increase periodically.

Conditions: The symptoms are observed under all of the following conditions: - GTPLB sticky and non-zero sticky idle timer should be configured under vserver. - Query should be configured under vserver. - At least one NSAPI's pdp session context should have been deleted in GGSN which is not known to GTPLB when GGSN receives the pdp status query for all NSAPIs from GTPLB. - On sticky timer expiration, the response for GTPLB query should contain status for fewer number of NSAPIs than GTPLB has. Sticky object with the NSAPI should have been deleted after n number of retries and the deletion should have occurred at least twice.

Workaround: There is no workaround.

- CSCso10458

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

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

  Workaround: There is no workaround.

- CSCso10596

  Symptoms: Polling cvpdnSessionAttrDevicePhyId from the CISCO-VPDN-MGMT MIB may show that multiple users are mapped to the same Virtual-Access SNMP ifIndex. This affects statistics collection or billing using IF-MIB counters.

  Conditions: This symptom is observed when PPP renegotiates an existing PPP connection on a Virtual-Access interface.

  Workaround: When possible, use RADIUS accounting for gathering statistics or billing.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route ***.

- CSCso15725

  Symptoms: Module's configuration not synchronized to standby supervisor if module resets while standby is booting up.

  Conditions: This bug may be seen if linecard or SPA were to reset before standby reaches standby hot terminal state.

  Workaround: Use **redundancy reload peer** to reset standby supervisor. On its next boot, configuration is synchronized to standby.

- CSCso24373

  Symptoms: When scaling to a high number of sessions, we sometimes see the following message:

  ```
  "QoS cannot be attached to sessions using full VAI interface"
  ```

  Conditions: This symptom occurs when trying to bring up a large number of PPPoEoVLAN (QinQ) sessions with per session output QoS attached over multiple 1 GE interfaces, or reloading router when PPP sessions tries to reconnect.

  Workaround: For initial session bringup over multiple 1 GE interfaces, bring up sessions on a single port at a time.

For router reload case, shut down 1 GE interfaces initially and bring up sessions on a single port at a time by doing "no shut".

- CSCso26940

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

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient processor memory
  ```

  ```
  %AAA-3-LOW_MEM: Author process is unable to handle the incoming packet due to low
  memory
  ```

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

  Workaround: There is no workaround.

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

- CSCso30669

  Symptoms: The standby RP continuously reloads after showing the following error message: HA-6-INT_SSO_UNAWARE

  Conditions: The symptoms are observed only when a Virtual Router Redundancy Protocol (VRRP) group is configured on one of the RP native GE-interfaces on a Cisco 7304 router (which does not currently support SSO).

  Workaround: VRRP can be configured on the Gigabit Ethernet Shared Port Adapter (SPA) interfaces on this platform, which are fully SSO-aware.

- CSCso30819

  Symptoms: Occasionally upstream traffic may be dropped when a private VLAN is configured, and after an OIR or the **shutdown** followed by the **no shutdown** commands are used.

  Conditions: The symptom is observed after sending untagged upstream traffic using the secondary/isolated VLAN from the promiscuous port. After using the **shutdown** and **no shutdown** command sequence (or an OIR), traffic may get dropped due to CBL logic being in the improper state.

  Workaround: Reload the system.

- CSCso33454

  Symptoms:

  PART 1) In a PE CE setup when 500 BGP VRF sessions are configured on a Cisco 10000 router, the PE PRE goes out of memory. PART 2) In a PE CE setup when 600 BGP VRF sessions are configured on a Cisco 10000 router, the PE PRE goes out of memory and crashes.

  Conditions: The symptoms are seen under the following conditions:

  PART 1) The number of routes is 500*500 /31 routes and 500*220 /24 routes. PART 2) The number of routes is 600*600 /31 routes.

  Workaround: There is no workaround.

- CSCso37750

  Symptoms: In Cisco-data-collection MIB, when SNMP bulk transfer is configured and unconfigured the switch crashes. The following Buffer Overflow message is displayed:

  ```
  Mar 19 22:59:05.272 PST: %SNMP_BULKSTAT-4-BUFFER_OVERFLOW: Buffer size too small to
  accommodate data for one collection interval for myTransfer
  ```

Conditions: Occurs when SNMP bulk transfer is configured and unconfigured.

Workaround: There is no workaround.

- CSCso37882

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

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

  Workaround: There is no workaround.

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

- CSCso40442

  Symptoms: When a router is configured for a redundancy mode other than SSO, BGP sessions may remain in an idle state after an RP switchover.

  Conditions: The symptom is observed after an RP switchover when the redundancy mode configured on the router is not SSO (for example, RPR and RPR+ modes exhibit this problem).

  Workaround: Reload the router.

  Further Problem Description: Until the router is reloaded, all incoming BGP open messages will be ignored and the router experiencing the problem will not initiate any outbound opens.

- CSCso40678

  Symptoms: Multilink PPP interface may cease passing traffic after one of the MLP group's member links receives an AIS from the TDM network.

  Conditions: Problem occurs on a Cisco 7600/SUP-720/OSM/CHOC12/T1-S1 running the c7600s72033-adventerprisek9-mz.122-33.SRB2 image.

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

- CSCso41824

  Symptoms: A router crashes with an unexpected exception to CPUvector 300.

  Conditions: This symptom is observed when you configure MPLS trunks on an 4xT3E3 SPA with FR IETF encapsulation.

  Workaround: There is no workaround.

- CSCso45720

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

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

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

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

- CSCso46427

  Symptoms: A device may crash when the **show clns interface** command is issued on the wrong interface.

Conditions: The symptom is observed when there are a number (around 100 or more) CLNS interfaces on the device.

Workaround: There is no workaround.

- CSCso47048

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

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48 data
  6DF7B48 chunk_freemagic EF430000
  -Process= "Check heaps", ipl= 0, pid= 5,
  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8 chunk_diagnose, code = 2 chunk
  name is PPTP: pptp_swi
  current chunk header = 0x06DF7B38 data check, ptr = 0x06DF7B48
  next chunk header = 0x06DF7B70 data check, ptr = 0x06DF7B80
  previous chunk header = 0x06DF7B00 data check, ptr = 0x06DF7B10
  ```

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

  Workaround: There is no workaround.

- CSCso47301

  Symptoms: Tracebacks may be observed while deleting the Peer-to-Peer (P2P) interface under traffic.

  Conditions: The symptom is observed when deleting the P2P interface under traffic.

  Workaround: There is no workaround.

- CSCso48665

  Symptoms: With COPP configured, L2 traffic coming from VPLS SVI is punted to the RP and is subject to the control plane policy.

  Conditions: The symptom is observed on a Cisco 7600 series router with both VPLS SVI and COPP configured.

  Workaround: There is no workaround.

- CSCso50347

  Symptoms: A router may crash after the command **show ip bgp** *l2vpn vpls* **all prefix- list** is issued.

  Conditions: The symptom is observed when the **show ip bgp** *l2vpn vpls* **all prefix-list** command is used with a configured prefix-list.

  Workaround: Use the **show ip bgp** *l2vpn vpls* **all** command.

- CSCso50484

  Symptoms: An RSVP GR instance may not be created on a sub-interface. Additionally, the interval of GR instance may change to 200 when the backup tunnel on the interface is flapped.

  Conditions: The symptoms are observed after the **shutdown** and **no shutdown** commands are executed on the main interface where the sub-interfaces are created. The other trigger is when the backup tunnel on the interface is flapped.

  Workaround: Unconfigure and reconfigure global RSVP GR.

- CSCso50587

  Symptoms: FRR Protection is failing after using the **no shutdown backup tunnel** command.

Conditions: The symptom is observed after adding for the first time an FRR flag over a TE tunnel using the command **tunnel mpls traffic-eng fast re-route**.

Workaround: Use the **shutdown** command followed by the **no shutdown** command on the Primary Tunnel.

- CSCso50602

  Symptoms: Router reloads after the **show ip bgp ipv4 mdt vrf** command is entered.

  Conditions: Occurred on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB2. Occurs when the **show ip bgp ipv4 mdt vrf** command entered with the *ip address* option, such as **show ip bgp ipv4 mdt vrf abc123** *x.x.x.x*.

  Workaround: The reload can be avoided by not using the IP address option with the 'show ip bgp ipv4 mdt vrf' command. None of the other options available for this command will trigger a reload

- CSCso51519

  Symptoms: Paths with same next-hop may be marked as being multipath.

  Conditions: The symptom is observed when multipath is configured and when using RRs in the environment.

  Workaround: There is no workaround.

- CSCso51661

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

  router ospf 1 shutdown

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

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

- CSCso52598

  Symptoms: The router may crash after the **no interface ethernet** *0/0.1* command is entered.

  Conditions: It could happen on a router with more than 4000 dynamic ARP entries.

  Workaround: Do not execute **no interface ethernet** *0/0.1*.

- CSCso53306

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso53332

  Symptoms: A Cisco 7600 series router acting as an ISG may run into memory issues.

  Conditions: The symptom is observed when a DHCP-initiated session is brought up on a default (null) VRF causing the standby router to run into memory corruption issues. This can lead to malloc failure tracebacks or, in some instances, crash the standby router.

  Workaround: There is no workaround.

- CSCso53377

  Symptoms: With large number of label switched paths (LSP), the SSO recovery process may take longer than expected. Therefore sometimes not all traffic engineering (TE) LSPs can recover after SSO switchover.

Conditions: Occurs on when there is a large number of LSPs.

Workaround: There is no workaround.

- CSCso53557

  Symptoms: A Flexwan 2 linecard may crash after removing and re-applying the WRED.

  Conditions: The symptom is observed when a policy-map is applied under a PVC FR in main interface then a subinterface is configured, and the PVC FR and the map- class is moved to the sub-interface. Then the sub-interface is deleted and the policy-map is applied to the main interface directly. Following this, the WRED is unconfigured and re-configured in class-default.

  Workaround: There is no workaround.

- CSCso54167

  Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

  Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

  Workaround: Delete and reconfigure the neighbor.

- CSCso55047

  Symptoms: Router crashes while unconfiguring **debug condition all** on L2TP network server (LNS).

  Conditions: This symptom occurs when **no debug condition all** is configured to remove the condition that was initially set.

  Workaround: There is no workaround.

- CSCso55081

  Symptoms: Synchronization from the Active RP to the Standby RP may not occur. It may halt during PPP negotiation and stop at AAA sync.

  Conditions: The symptoms are observed during synchronization and where the CoA feature is available for the image and platform.

  Workaround: There is no workaround.

- CSCso55933

  Symptoms: A SIP-400 may crash during RP switchover with scale configuration and heavy load.

  Conditions: The symptom is observed with a Cisco 7600 series router with HA scale configuration and with 28K VC and 500 VPLS.

  Workaround: There is no workaround. The LC will recover after a reload.

  Further Problem Description: This crash shows up rarely during RP switchover. LC will self-recover after a reload.

- CSCso56038

  Symptoms: The following error message may be seen:

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

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

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

Workaround: There is no workaround.

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

- CSCso56111

  Symptoms: The LC may crash if the **mpls traffic-eng tunnels** configuration is removed from the SIP600 interface.

  Conditions: The symptom is observed with a VPLS configuration and TE-FRR protection is configured for the primary ES-20 interface/tunnel which points to the SIP600 interface TE tunnel as a back-up path. If the **mpls traffic-eng tunnels** configuration is removed from the SIP600 interface, the LC crashes immediately.

  Workaround: There is no workaround.

- CSCso56185

  Symptoms: L2TP Start-Control-Connection-Reply (SCCRQ) and Start-Control-Connection-Reply (SCCRP) messages have incorrect setting of mandatory-bit for the receive window Size attribute-value pair (AVP). This may cause L2TP/VPDN sessions to fail to connect.

  Conditions: Occurs in VPDN environments where the peer requires tight protocol adherence.

  Workaround: There is no workaround.

- CSCso56196

  Symptoms: Updates are not being sent or withdrawn.

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

  PE1------UUT----PE2

  On UUT there are neighbors PE1 and PE2. If PE1 and PE2 are in same update group, the **show ip bgp all update-group** command will show that.

  Now there are a lot of updates being formatted and sent in the process. The **show ip bgp all replication** command would show the messages which are enqueued for sending out for particular update groups. At this moment, one neighbor goes to idle and is not coming up, then the new updates will not be formatted unbtil the neighbor comes up.

  Workaround: 1) Remove the idle neighbors of the update-group and add again. 2) Clear the IP BGP neighbor that went idle.

- CSCso56413

  Symptoms: A Catalyst 6000 line card may crash while attempting to free non-chunk memory.

  Conditions: Occurs when MAC out-of-band synchronization is enabled in a distributed forwarding system

  Workaround: There is no workaround

- CSCso57886

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

Workaround: There is no workaround.

- CSCso61282

  Symptoms: Multicast traffic from a VRF may be dropped after encapsulation.

  Conditions: The symptom is observed when a Bidirectional PIM (bidir-PIM) is used in the core network and VRF traffic is forwarded through a data MDT. In this condition, SSO switchover may trigger a packet drop issue.

  Workaround: Use the **clear ip mroute** *group* command.

- CSCso62193

  Symptoms: The standby router may reset unexepectedly.

  Conditions: The symptom is observed when removing the frame relay map on the active using the **no frame-relay vc-bundle** command. The issue occurs because the frame relay map is removed in active but not in standby due to a synchronization problem.

  Workaround: There is no workaround.

- CSCso62526

  Symptoms: Standby supervisor reloads after the interface configuration command **no flow-sampler <name>** is used to remove flow sampler map.

  Conditions: Occurs on a Cisco 7606s with two RSP720-3C-GE configured for normal use with sampled NetFlow configured. To cause the issue, a sampler must be explicitly detached.

  Workaround: There is no obvious workaround to the issue. To avoid the issue, avoid detaching the sampled NetFlow.

- CSCso63263

  Symptoms: The RP will start showing IPC-5-WATERMARK: 988 messages pending in xmt for the port messages on the screen. The number of messages will change.

  Conditions: The router has 275,000 i-BGP routes injected into the router. Among these routes, 100,000 are flapped continuously for one to one and half days. They are flapped every 10 sec. The problem needs at least a days worth of time of continuous flapping.

  Workaround: Stop the route flap. Although the messages will keep coming, there is no impact on functionality. And they are bogus since they are originated from wrong count.

- CSCso63807

  Symptoms: Packet loss when pinging an IP Address in a VPN routing/forwarding (VRF).

  Conditions: This problem is seen on a Cisco 7600 after the VRF configuration on a port is rapidly changed, such as the following example:

  interface gi3.1.88 ip vrf forwarding aaaa ip vrf forwarding bbbb

  Workaround: Delete the VRF with **no ip vrf forwarding aaaa** before changing the VRF under the interface.

  Further Problem Description: The VLAN RAM, which stores the VRF ID, is programmed wrong when this issue is seen. This causes packet loss or packets to be punted to the RP to resolve the conflict

- CSCso64104

  Symptoms: A router may crash after applying the configurations related to PA- MC-2T3-EC immediately after the router reloads.

Conditions: The symptom is observed on Cisco 7200 series and a 7301 router.

Workaround: Do not configure PA-MC-2T3-EC immediately after the router reloads.

- CSCso65193

  Symptoms: The memory occupied by the IP SLA Event Processor may gradually increase.

  Conditions: The issue occurs when IP SLA jitter operation is configured on the router without source port specification.

  Workaround: There is no workaround.

  Further Problem Description: With 1000 IP SLAs configured (200 each of following types: path-echo, path-jitter, icmp-echo, udp-jitter and udp-echo, each with a unique destination), the memory allocated for "IP SLAs Event Pr" increases and the level of available processor memory goes down. This issue will have a performance impact.

- CSCso67141

  Symptoms: When a Border Gateway Protocol (BGP) peer is brought down, some of the routes that were learned may not be removed. If around 200,000 routes are advertised from a neighbor and the BGP process on the neighbor is then stopped, all routes will be removed the first time. On the second time, however, around 20,000-80,000 routes may remain.

  Conditions: The symptom occurs when the BGP process on the neighbor (that has advertised 200,000 routes or more) is brought down.

  Workaround: There is no workaround.

- CSCso67500

  Symptoms: Multicast traffic from the VRF network may be dropped after encapsulation.

  Conditions: The symptom is observed when a Bidirectional PIM (Bidir PIM) is used in the VRF network and when Gigabit port(s) on the active supervisor are in use. An SSO switchover can trigger a packet drop issue.

  Workaround: Reconfigure MDT using the **no mdt default** command followed by the **mdt default** *group- address* command.

- CSCso68344

  Symptoms: The command **no service dhcp** to stop DHCP server/relay from the router may cause a crash.

  Conditions: The symptom is observed when router is receiving requests from DHCP clients at high rate and duplicate-address detection ping is active.

  Workaround: There is no workaround.

- CSCso70986

  Symptoms: When traffic engineering (TE) preferred path is removed, then all the XCs using that pw-class are unprovisioned.

  Conditions: Occurs when xconnect anything over MPLS (AToM) configured with TE tunnel preferred path.

  Workaround: There is no workaround.

- CSCso71350

  Symptoms: The standby may reload when upgrading the software from Cisco IOS Release 12.2(31)SB to Release 12.2(33)SB. After issuing the **issu loadversion** command, when the standby tries to boot up with Cisco IOS Release 12.2(33)SB, it fails and may crash at **config sync** and may continually reboot.

Conditions: The symptoms occur when synchronizing a virtual template/virtual access interface configuration from the active to the standby.

Workaround: There is no workaround if virtual access interfaces are required.

- CSCso72167

  Symptoms: The ISSU AAA client negotiation says the session is COMPATIBLE with the images, even though the standby is loaded with an image that does not support that client.

  Conditions: The symptoms are observed when there is a stale ISSU AAA client on the ACTIVE, which does not clear the session once the standby goes down.

  Workaround: There is no workaround

- CSCso73266

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

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

  Workaround: Reload the router running ISG.

- CSCso74156

  Symptoms: Feature push for VRF-tx does not work.

  Conditions: On the service profile, a "vrf-id=..." is configured. This is pushed onto a session. IPCP renegotiation fails on Client Router.

  Workaround: Within Cisco IOS Release 12.2(31)SB images, the cloning Virtual- Template interface did not require the **ip unnumbered X** command when running Cisco IOS Release 12.2(33)SB. The cloning Virtual- Template interface requires the **ip unnumbered X** command statement similar to the notation below:

  interface Virtual-Template201 ip unnumbered loopback201

- CSCso74257

  Symptoms: Memory leaks may be seen.

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

  Workaround: There is no workaround.

- CSCso75736

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

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

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

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

- CSCso75863

  Symptoms: A service policy is not attached at SIP400 when attached under a virtual template in distributed link fragmentation and interleaving (dLFI) over ATM (dLFIoATM).

Conditions: The symptom is observed with any type of QoS on a SIP400 with dLFIoATM.

Workaround: There is no workaround.

- CSCso76863

  Symptoms: With a Cisco 7600 series router, occasionally the RP may crash when a SIP or SPA is reset.

  Conditions: The symptom is observed when an RP is very busy when a SIP or SPA is reset. For example, the crash has been seen intermittently when an ESM or SPA card was reset while a large number of BGP routes are toggling.

  Workaround: There is no workaround.

- CSCso77762

  Symptoms: On a Cisco 7600 series router, egress iEdge traffic may not be forwarded using the IP session. This is seen only when a subnet session is applied on the IP sessions.

  Conditions: This symptom is observed on a Cisco 7600 series router when subnet sessions are formed from IP sessions.

  Workaround: There is no workaround.

- CSCso78716

  Symptoms: SNMP object entPhysicalVendorType returns incorrect value.

  Conditions: Occurs only on a Cisco 7603s.

  Workaround: There is no workaround.

- CSCso79720

  Symptoms: When the **show interface** command is entered, all of the Layer 2 switch port interfaces on ES-20 are shown with the same bridge MAC.

  Conditions: Only seen on ES-20.

  Workaround: As a workaround, the interface when configured to switchport, then the mac-address for the same can be correctly set by following procedure: a.) Execute the command 'show idprom module <module> details'. b.) lookout for the field 'mac base' and 'mac_len' field in the output. c.) Assign 'mac base + port_num' as the mac-address to the port on ES20. (Ensure that 'mac base + port_num' lie within the range of 'mac base + mac_len'

  Further Problem Description: Ideally, when a port is configured as a switchport, it's desired that each port should have a unique mac-address. However, it was not like this rather all the ports were having same mac-address. which is not correct if the port is put in switchport mode. However, if all those ports which are not switchports' and are routed ports, they'll share the same-mac-address. It's as per the design.

- CSCso80545

  Symptoms: If an interface changes from a down to an up state, and a better native path is available for multicast traffic, the RIB may still use the old path for multicast.

  Conditions: The symptom is observed when the **mpls traffic-eng multicast-intact** command is enabled under **router isis** *tag*. In addition, the route to the source has to be learnt over the TE tunnel.

  Workaround: Use the **clear ip route** *ip prefix* command.

  Further Problem Description: The MPLS TE tunnel appears to be the best path for the sources of traffic and PIM will try to use them, but an RPF check will fail because the packets are never received from TE-tunnels since they are unidirectional.

- CSCso81322

  Symptoms: User is not assigned IP Pool address received from AAA Server.

  Conditions: This symptom is seen when a different IP Pool is defined under the Virtual Template Interface than what is received via AAA Per User settings.

  Workaround: There is no workaround.

- CSCso81370

  Symptoms: With AToM debugging enabled and a shutdown of a core interface, a crash may be experienced.

  Conditions: The symptoms are observed on a Cisco 7600 series router with AToM debugging enabled using the **debug mpls l2transport vc status ev** command, followed by a shutdown of a core interface.

  Workaround: There is no workaround.

- CSCso82551

  Symptoms: A router reloads.

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

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

  buffers verybig permanent 7000 buffers verybig max-free 7000

- CSCso82707

  Symptoms: ISG radius proxy may not proxy the accounting responses back to the radius proxy client. If ISG does not receive a response for the first accounting request, it will create the session but the process will not retransmit consecutive accounting requests.

  Conditions: The symptom is observed when the AAA server goes down immediately after authentication, but before the accounting requests are sent.

  Workaround: There is no workaround.

  Further Problem Description: This has a functional impact as radius clients may think that the AAA server is down.

- CSCso85138

  Symptoms: Packets may get process switched instead of route-cache switched.

  Conditions: The symptom is observed when there is non-process switching on the interface(s) configured with Frame-Relay which results in no proper connectivity, even with the static routes, between the adjacent routers.

  Workaround: There is no workaround.

- CSCso86674

  Symptoms: Border Gateway Protocol (BGP) is unable to get route information after **shut/no shut** is performed on BGP neighbor on far-end.

  Conditions: Issue is seen when BGP is used for IPv6 routing.

  Workaround: This problem can be recovered by doing shut and no-shut again. Also, problem will not happen if you set network <prefix> at address-family on far-end router.

- CSCso87049

  Symptoms: MPLS VPN Inter-AS test fails due to ping failure from CE to CE.

Condition: This symptom occurs when Inter-AS VPN routes are not properly propogated.

Workaround: There is no workaround.

Further problem description: MPLS VPN Inter-AS test fails due to ping failure from CE to CE. CE-CE connectivity is broken in interas-ab option with different RD configuration. On further analysis, it was found that on EBGP2PE the label vpn4 label for the CE loopback interface is not installed in MPLS forwarding table. The entry exists in the BGP table.

- CSCso87838

  Symptoms: Switch may report flapping HSRP peers when the **wr mem** command is issued.

  Conditions: The symptom is observed when HSRP is configured with aggressive timers and the **wr mem** command is issued.

  Workaround: Increase the timer values for HSRP or consider not using aggressive timers.

- CSCso88199

  Symptoms: When an MPLSoGRE tunnel is configured, and a packet is sent through the tunnel with the DF bit set in the outer IP header.

  Conditions: The tunnel encapsulation should be removed by the other end of the tunnel. But when DF bit is set in the IP header, this decapsulation did not happen.

  Workaround: There is no workaround.

- CSCso88615

  Symptoms: When clearing all live sessions plus saving the configuration, the Standby resets with the reason: "Active and Standby configuration out of sync".

  Conditions: This symptom occurs when there is a large number of PPPoA, PPPoEoA, and L2TP sessions. Perform session flapping from the client side and/or the **clear vpdn tunnel all** command and/or the **write memory** command.

  Workaround: There is no workaround.

- CSCso88616

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

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

  Workaround: There is no workaround.

- CSCso88898

  Symptoms: The line card displays memory allocation failure messages, and memory statistics indicate a continuous decline in free memory.

  Conditions: When port mode or VC mode cell relay configuration is applied on an ATM interface, it is observed that after traffic switching for a long time (approximately 48 hours, depending on scale), the above problem occurs.

  Workaround: There is no workaround.

- CSCso89550

  Symptoms: The router crashes as the rxError on the active is slowly increasing after every few minutes. There is no user traffic in the system, so the traffic that caused the rxError can only be the heartbeat packet or the diag packet. Supervisor has bad local fabric channel message.

  Conditions: This is happening on a Cisco Catalyst 6000 Sup720 that is running Cisco IOS Release 12.2(18)SXF12a.

Workaround: Disable GOLD diagnostic tool on switches. If the two tests "TestFabricSnakeForward" and "TestFabricSnakeBackward" are disabled from running as HM tests, we should not see this issue.

- CSCso90021

  Symptoms: If there is a port-channel configured with members from both bays and EVCs are configured on that port channel with BD, removing then adding the EVCs may then cause some of them to fail to send traffic.

  Conditions: The symptom is observed when the port-channel has members from both bays and EVCs are removed and then added.

  Workaround: Conduct a line card OIR.

- CSCso91230

  Symptoms: A router may display the following error:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=ATM0
  -Process= "IGMP Snooping Receiving Process"
  ```

  Conditions: The symptom is observed when bridged traffic is passing to an MLPP interface.

  Workaround: Disable IGMP snooping with the **no ip igmp snooping** command.

- CSCso92930

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

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

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

- CSCso93883

  Symptoms: Upon reload of a DFC, traffic coming from the MPLS cloud might be dropped when the traffic is destined for a EoMPLS connection on a MUX-UNI

  Conditions: This is seen on 12.2(33)SRB3 and 12.2(33)SRA3. The incoming module needs to be a DFC, and the egressing port needs to be a MUX-UNI. This does not happen to regular Ethernet Over MPLS (EoMPLS) connections.

  Workaround: Perform a **shut/no shut** on the connection towards the MPLS network, then **shut/no shut** the VC.

- CSCso98964

  Symptoms: EIGRP authentication with a key string longer than 16 characters may fail. EIGRP neighbors will fail to establish.

  Conditions: Occurs in routers running a variety of Cisco IOS Release 12.2 versions.

  Workaround: Use a shorter key string.

- CSCso99860

  Symptoms: Some of the initially shipped PWR-1500-DC power supplies in Cisco 7603S chassis have incorrect SNMP OID programmed in the IDProm. The vendorOID does not match with the CANA-assigned number in CISCO-ENTITY-VENDORTYPE-OID-MIB.my

  Conditions: This is applicable for those power supplies for which the vendorOID is programmed as 193 and not as 194.

  Workaround: There is no workaround.

- CSCsq05540

  Symptoms: The switching of L2TP sessions from one physical interface to another physical interface takes a long time to complete.

  Conditions: The symptom is observed on a Cisco 10000 series router reparenting as few as 800 PPPoEoQinQ L2TP sessions with an L2TP tunnel.

  Workaround: There is no workaround.

- CSCsq05680

  Symptoms: The Route-Processor may sometimes crash on reset of the ES20 linecard.

  Conditions: The symptom is observed when an ES20 card has ports as members of a port-channel.

  Workaround: There is no workaround.

- CSCsq05997

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

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1,
  -Traceback= 0x61013944 0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C
  ```

  Because the message is generated frequently, the log file may fill up too soon.

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

  Workaround: There is no workaround.

- CSCsq07229

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

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

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

- CSCsq09918

  Symptoms: Switches running REP may crash due to memory corruption (debug exception). This bug is common to ME3750, ME3400 and Cisco 7600. Multiple switches may crash.

  Conditions: This can occur when there is any traffic congestion on the REP link which causes REP EPA packets to be dropped. The problem occurs when REP link state layer retransmits the EPA packet.

  Workaround: No workaround other than solving the congestion problems on the link.

- CSCsq09962

  Symptoms: Cisco 7600 router crashes at "pim_proxy_empty_rd."

  Conditions: Customer seeing crash with decode during initial deployment of new Cisco 7600 router.

  Workaround: There is no workaround.

- CSCsq11427

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

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

Workaround: There is no workaround.

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

- CSCsq12380

  Symptoms: The SNMP engine process may experience a memory leak.

  Conditions: The symptom is observed on a Cisco 7600 series router with CEM interfaces and when the router is polled for 1.3.6.1.4.1.9.10.131.1.3.

  Workaround: Configure a SNMP view to disable polls on 1.3.6.1.4.1.9.10.131.1.3.

- CSCsq13576

  Symptoms: The router may crash when the multilink interface goes down.

  Conditions: The symptoms are observed when the multilink interface has interleave configured.

  Workaround: There is no workaround.

- CSCsq13938

  Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

  Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

  This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

  Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing "q" to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq14340

  Symptoms: While reloading a Cisco router with dual RP with default start-up configuration of active RP, there is a stale **snmp mib community-map ILMI engineid** command seen in standby running configuration which is not seen in active RP configuration.

  Conditions: This symptom is observed in latest nightly build for Cisco IOS Release 12.2(33)SB image.

  Workaround: There is no workaround.

- CSCsq15994

  Symptoms: Low CPS may be observed.

  Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

  Workaround: There is no workaround.

- CSCsq16008

  Symptoms: In DDP DFC, MET entries get programmed on both replication instances.

  Conditions: The symptom is observed when issuing the **shutdown** command followed by the **no shutdown** command on the interface that receives the PIM join instruction.

  Workaround: Use the **clear ipv6 pim topology** *group address* command.

- CSCsq16830

  Symptoms: Stale NFS entry left on ESM20G card when diagnostics is enabled.

  Conditions: Occurs on Cisco 7609 ESM20G cards after the router is reloaded.

  Workaround: Disable diagnostics and reset the line card.

- CSCsq18756

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

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

  Workaround: There is no workaround.

- CSCsq19146

  Symptoms: Customer seeing multiple "%SIP200_SPIRX-3-SPA_INTERRUPT: SPA 0 - seq err, SPA Int status = 0x4" errors.

  Conditions: Occurs under normal operating conditions.

  Workaround: There is no workaround.

- CSCsq19159

  Symptoms: System crash or memory corruption occurs.

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

  Workaround: There is no workaround.

- CSCsq21589

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

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

  Workaround: Reload the router that is running ISG.

- CSCsq21862

  Symptoms: Upon the execution of the **test crash** command on the active supervisor in an HFS-capable chassis, the new active fabric channel may go out of synchronization, the traffic stops passing through the line card, and the following error message may be seen:

  %FABRIC_INTF_ASIC-5-FABRICSYNC_REQ: Fabric ASIC 0: Fabric sync requested after 3 sync errors

  Conditions: The symptoms are observed on an HFS-capable chassis and are triggered by the **test crash** command on the active supervisor. It is seen with both SIP200 and SIP400.

  Workaround: There is no workaround. The only way to come out of the problem state is with a line card reset using the **hw-module module** *slot* **reset** command.

- CSCsq22284

  Symptoms: A policy-map configuration may be corrupted after user entry. The "show run" output shows the corrupted policy-map configuration with (the unexpected output) "use method ssg" after "set".

  Conditions: The symptom is seen when running Cisco IOS Release 12.2(33)SRC and when configuring the policy map.

  Workaround: There is no workaround.

- CSCsq22383

  Symptoms: A Cisco 7600 router may sometimes hang while performing configuration/deconfiguration stress tests

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

  Workaround: There is no workaround.

- CSCsq22417

  Symptoms: A Cisco 7600 running configuration/deconfiguration tests repeatedly over time may crash.

  Conditions: Unknown conditions.

  Workaround: There is no workaround.

- CSCsq23727

  Symptoms: There may be a memory leak in the middle buffer.

  Conditions: This symptom is observed with router-generated broadcast or multicast packets alone. Use the following commands to detect the presence of this defect. 1. **show buffers leak** *inc Cc0* 2. **show buffer usage** *inc Cc0* The count will be incremented, if the problem exists.

  Workaround: There is no workaround.

- CSCsq24171

  Symptoms: Traffic may not flow on an encapsulation untagged EVC after an OIR.

  Conditions: The symptom is observed on an EVC on a physical port with encapsulation untagged, when the linecard is OIR. It is specific to EVC on the ES20 linecard.

  Workaround: Reapply the configuration on the specific interface.

- CSCsq24436

  Symptoms: L2TPv3 sessions may not come up in a scaled scenario.

  Conditions: The symptom is observed when attempting to bring up more than five L2TPv3 sessions. Only half of the sessions will come up and rest remain down.

  Workaround: There is no workaround.

- CSCsq24535

  Symptoms: The tunnel stitching VC may go down resulting in traffic loss.

  Conditions: The symptom is observed when the remote peer is changed with a different MTU, causing the tunnel stitching VC to go down. When the matching MTU is reconfigured, however, the tunnel stitching session does not come back up.

  Workaround: Do a soft OIR of the Provider Edge router’s interface where MTU reconfiguration is done.

- CSCsq25028

  Symptoms: Malloc errors seen on enhanced FlexWANs with 256MB memory in RSP720 systems when another line card is inserted or powered up. FlexWAN I/O memory low watermark becomes very low while number of allocated IPC buffers grow in the hundreds.

  Conditions: Seen only on RSP720, not seen on SUP720 systems. Routing table has 30,000 routes or more.

  Workaround: There is no workaround.

  Further Problem Description: Inserting or powering up a line card prompts the RP to send all info to all cards and FlexWAN bays in chassis. RSP720 sends info at higher rate than FlexWAN can immediately process, so hundreds of IPC buffers are allocated until its I/O pool is exhausted and malloc error reported. May not impact operation, but risk of memory fragmentation and other failures increase.

- CSCsq26085

  Symptoms: The "total output drops" counter will no longer increment with 7600- ES20-GE3C. Instead, the increment is seen on the counter of port-channel which is in administratively down status and is not associated with the interface.

  Conditions: The symptom is observed on a 7600-ES20-GE3C that is configured with a service policy. If a port channel is created that is not associated with the interface, the drops will increment on that port-channel, instead of the expected interface.

  Workaround: Use a port-channel interface with an interface number greater than 20. For example, use "int port-channel 21".

- CSCsq28244

  Symptoms: A new OIF VLAN may not get reprogrammed in HW after a quick link flap using the commands **shutdown** and **no shutdown**.

  Conditions: The symptom is observed when the internal VLAN ID for the outgoing interface changes upon the **shutdown** and **no shutdown** command sequence.

  Workaround: Use the **clear ipv6 pim topology** *group* command.

- CSCsq28584

  Symptoms: A router may crash from memory corruption.

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

  Workaround: There is no workaround.

- CSCsq28896

  Symptoms: There may be an 100 percent packet loss between hosts connected through a Cisco 7600 series router via frame-relay on different bridge groups.

  Conditions: We are still investigating the conditions for this issue. However, we estimate the following conditions: 1. Seen on Cisco IOS Release 12.2(33)SRA5-7 and Release 12.2(33)SRB3. 2. When a Cisco 7600 series router is switching traffic between bridge- domains. 3. When both ingress and egress interfaces are on the same line card and share the same LTL.

  Workaround: Use Cisco IOS Release 12.2(33)SRA4.

  Alternate Workaround: Force the traffic to be switched in software, either by disabling MLS switching, or having an ingress access-list specifying the ’log’ statement. Please be cautious doing this as both workarounds may significantly impact CPU.

- CSCsq29893

  Symptoms: Traffic may not flow on a port channel EVC after an OIR.

  Conditions: The symptom is observed when a port channel EVC is created with encapsulation untagged and then an OIR is performed on the linecard.

  Workaround: Reapply the configuration on the specific interface.

- CSCsq30717

  Symptoms: A NPE-G1 resets due to a hardware watchdog timeout. This is indicated in the **show version** output with "Last reset from watchdog reset".

  Conditions: The Cisco 7200 must have an enabled PA-MC-2T3-EC with channelized T1s.

  Workaround: Disable the PA-MC-2T3-EC.

- CSCsq31206

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

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

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

  Workaround: There is no workaround.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  - The error message below is frequently generated.

  ```
  Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode msg type 0 for slot(s) 0B
  -Traceback= 6044E470 60465864 6043BCFC 6043B570
  ```

  - The **debug cef xdr** command yields the following message:

  ```
  Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event xdr for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0 Mar 31 17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker FIB_FIB xdr Mar 31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580 UTC: - short path ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31 17:44:40.580 UTC: => pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
  ```

  - Checking the prefix, it points to drop entry.

  router#**show mpls forward vrf <vrf name> x.x.x.x** Local Outgoing Prefix Bytes Label Outgoing Next Hop Label Label or VC or Tunnel Id Switched interface 937 No Label x.x.x.x/y[V] 0 drop <========= it is drop

  - Checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set.

  router#**show ip cef vrf <vrf name> x.x.x.x int** [snip] path_list contains at least one resolved destination(s). HW not notified path 70BFFC5C, path list 20E87B58, share 1/1, type recursive nexthop, for IPv4, flags resolved MPLS short path extensions: MOI flags = 0x16 <-------MOI flags 0x10 is incorrectly set (for ebgp path, correct flag should be 0x4, 0x5, 0x6 ..) correct now. [snip]

Conditions: The eiBGP multipath is enabled; iBGP path comes up first, then the eBGP path. Both eBGP and iBGP paths could be in MPLS forwarding causing the issue.

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

- CSCsq31923

  Symptoms: Crash may occur after polling MPLS-LSR-MIB mplsInterfaceConfTable.

  Conditions: MPLS-enabled tunnels exist in configuration and some are removed by doing **no int tunnel** *tunnelid*. If mibwalk of any object in mplsInterfaceConfTable is performed after that, this may result in crash.

  Workaround: Remove MPLS configuration on tunnel with the **no tunnel mode mpls traffic-eng** command before entering the **no int tunnel** command.

  Further Problem Description: It has been found this problem occurs when tunnel also contains the following config: **tunnel mpls traffic-eng path-option 1 dynamic**. Crash occurs only if image contains fix for CSCsm97259. Will see this message similar to the following before the crash:

  ```
  Jun 3 11:53:59.955 PDT: %TIB-3-GENERAL: MPLS MIB subblock ifIndex corrupted for
  ifIndex: 46 - was: 1198404176; corrected
  ```

- CSCsq31958

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

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

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

- CSCsq32443

  Symptoms: MCP rejecting Start-Control-Connection-Reply (SCCRP) with receive window size missing.

  Conditions: Occurs with peers that use or expect the default handling of RxWindowSize of (4) and do not include the attribute-value pair (AVP) in the SCCRQ/SCCRP messages.

  Workaround: Force peer to send AVP.

- CSCsq33677

  Symptoms: PPPoE sessions in relay mode got stuck in attempting state.

  Conditions: This symptom is observed on a Cisco router running an internal build of Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsq34195

  Symptoms: The **show ip rsvp interface** command does not provide reserved bandwidth information.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRC in an MPLS TE environment.

  Workaround: There is no workaround.

- CSCsq36191

  Symptoms: When an RP's CPU memory is almost all consumed (by BGP and/or other processes), repeated use of the **show ip bgp summary** command may cause a router to crash.

  Conditions: The symptom is observed when memory is almost all consumed and the command **show ip bgp summary** command is used repeatedly.

Workaround: Upgrade to more memory.

- CSCsq36782

  Symptoms: In Ethernet Over MPLS (EoMPLS) environment after fast reroute (FRR) from interface on SIP600 to interface on SIP400 and re-optimization, traffic is blackholed from CPE device to core.

  Conditions: This happen only after FRR from SIP600 module to SIP400 module. FRR between SIP400 does not experience this problem.

  Workaround: There is no workaround.

- CSCsq37834

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

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

  Workaround: There is no workaround.

- CSCsq39244

  Symptoms: IPv6 traffic going to a 6PE device may be dropped after an interface flap.

  Conditions: The symptom is observed when the IPv6 prefix is known by BGP and the same prefix is assigned to the local interface. After an interface flap, the MPLS forwarded table is populated with drop and all incoming 6PE traffic going to that interface is dropped.

  Workaround: There is no workaround.

- CSCsq39254

  Symptoms: When call-home profiles are removed by the **no profile all** command, the standby system will reload if a new profile is added or a CiscoTAC profile is edited.

  Conditions: The symptom is observed when a non-default call-home profile is configured, and then removed by the **no profile all** command. The problem will occur when customer tries to add new profile or to edit a CiscoTAC profile.

  Workaround: There is no workaround.

- CSCsq41962

  Symptoms: Unable to get ifIndexes for the GE-WAN interfaces by using SNMP.

  Conditions: The symptom occurs when ES20 and OSM exist in same chassis.

  Workaround: Use Cisco IOS Release 12.2(33)SRB3.

- CSCsq42931

  Symptoms: Cisco 7600 series of router may reload twice when the router is booting up.

  Conditions: This is a very rare occurrence. A Cisco 7600 series might reload while it is booting up. Additionally, spurious access might be seen when line cards are booting up. These messages have no impact on functionality or stability of the router.

  Workaround: There is no workaround.

- CSCsq43591

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

  Conditions: This symptom is observed under the following conditions:

  - LAC<->LNS setup.
  - Clearing of session from CPE.

  - In the **show pxf cpu vcci** command output, there is no VCCI present for the VAI.
  - Also seen in lab when the CPE is booted and the first session comes up.

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

- CSCsq43831

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

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

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

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

  ```
  ip route 10.0.0.0 255.255.255.255 192.168.1.1
  ```

  to

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

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

- CSCsq45761

  Symptoms: Traceback may occur when TE tunnels are configured and after HA is done by script.

  Conditions: The symptom is observed on a Cisco 7600 series router and when TE tunnels and dot1q are configured on a CE-facing interface. This issue is only seen when HA uses a script.

  Workaround: There is no workaround.

- CSCsq47355

  Symptoms: On Cisco 7600 routers, the switch processor may crash the router when BGP is configured in rare situations.

  Conditions: This is a rare condition that can most likely happen with L3VPN and BGP recursive routes configured when a network, routing, or link event occurs (e.g., link flap in the remote ends, routing flaps, etc). This issue may also require routes to be load-balanced over multiple links.

  This issue only affects 12.2(33)SRB and 12.2(33)SRC and is fixed in 12.2(33)SRB4 and 12.2(33)SRC2 and later releases.

  Workaround: There is no workaround.

- CSCsq48201

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

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

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

- CSCsq49176

  Symptoms: Router bus error crash on invalid address:

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

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

Workaround: There is no workaround.

- CSCsq50535

  Symptoms: Split-horizon may not work correctly for a Layer 2 Protocol Tunnelling (L2PT) packet received from a VPLS VC.

  Conditions: The symptom is observed on a Cisco 7600 PE router that is running VPLS and L2PT. The issue causes the L2PT packets to be sent back to the MPLS cloud on the other VPLS VC that is part of the same VFi, despite split- horizon being present. When there are multiple Cisco 7600 PE routers in the VPLS with similar configurations, there may be a loop of L2PT packets between the PEs.

  Workaround: Avoid using L2PT with VPLS.

  Alternate Workaround: Use Cisco IOS Release 12.2(33)SRA6.

- CSCsq52048

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

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

  Workaround: There is no workaround.

- CSCsq52847

  Symptoms: Connection establishment failed with the event agent.

  Conditions: Occurs when the Event Gateway is killed and restarted on a Cisco 1812 router while running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq55071

  Symptoms: Some BGP NSR peers go down when an RP switchover occurs.

  Conditions: The symptom is observed when the BGP peers are configured as BGP NSR peers.

  Workaround: There is no workaround.

- CSCsq55273

  Symptoms: Traffic does not get shaped to parent shaper rate once the child policy is removed from the parent class.

  Conditions: Occurs on a ES20 line card. Apply a HQoS (child policy on class-default) on main interface and then remove the child policy from parent class-default. Traffic should get shaped to class-default shaper.

  Workaround: Remove and reapply the service-policy.

- CSCsq55518

  Symptoms: Deletion of one sub-interface with L2TPv3 cross connect configuration may cause the others L2TPv3 sessions in other sub-interfaces to go down.

  Conditions: The symptom is seen with the Cisco IOS Release 12.2(33)SRD only. It is observed when there is sub-interface with L2TPv3 cross connect configuration, such as:

  l2tp-class vlan-class authentication password x xxxxxxxx

pseudowire-class vlan-pw encapsulation l2tpv3 protocol l2tpv3 vlan-class ip local interface Loopback0

interface GigabitEthernet0/1.1 encapsulation dot1Q 2 xconnect 10.200.1.203 2 pw-class vlan-pw ! interface GigabitEthernet0/1.2 encapsulation dot1Q 3 xconnect 10.200.1.203 3 pw-class vlan-pw ! The problem occurs when one sub-interface is deleted, for example: no interface GigabitEthernet0/1.1

Workaround: There is no workaround.

- CSCsq57238

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

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

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

- CSCsq57462

  Symptoms: Ethernet Out of Band Channel (EOBC) hang causes line card reset. EoBC might get stuck resulting in communication loss between RP/SP and line card. This will result in line cards getting reset. This is a very rare condition and is seen only once so far.

  Conditions: Occurs during increased EoBC traffic due to convergence or link flap and is very rarely seen.

  Workaround: This impacts only one CPU. A forced switchover will recover from this condition.

- CSCsq59977

  Symptoms: EOAM monitoring of CRC errors may not work with 6148A-RJ45 and 6148- FE-SFP linecards.

  Conditions: The symptom is observed when packets with errors are received. It is seen with 6148A-RJ45 and 6148-FE-SFP linecards.

  Workaround: There is no workaround.

- CSCsq60073

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

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

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

- CSCsq60553

  Symptoms: An FW2 card may reload with memory version "VI4DP647228EBK-MD" installed.

  Conditions: The symptom is observed with all FW2 linecards having Memory version "VI4DP647228EBK-MD".

  Workaround: There is no workaround.

- CSCsq62653

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

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

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

- CSCsq62703

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) tries to access invalid memory address and may cause router to stop working.

  Conditions: Occurs when a switch over happens and standby router becomes active.

  Workaround: There is no workaround.

- CSCsq63041

  Symptoms: Xconnect may not be able to be configured if "ip address" has already been configured on the interface.

  Conditions: The symptom is observed when attempting to configure IPv6 protocol demux under xconnect, when "ip address" has already been configured.

  Workaround: There is no workaround.

- CSCsq63176

  Symptoms: PA-MC-T3/E3-EC PA does not pass full traffic after a sudden burst near line rate.

  Conditions: Occurs when 256 interfaces are configured on the port adapter with multilinks operating on those serial interfaces.

  Workaround: Configure fewer than 256 serial interfaces.

- CSCsq63621

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets.

  Conditions: This symptom is observed when OSPF is enabled.

  Workaround: There is no workaround.

- CSCsq63731

  Symptoms: If either the command **vlan-id dot1aq** *vlan-id* or the command **vlan-range dot1aq** *start-vlan-id end-vlan-id* is configured on a main interface which is also configured for routing, and an ARP packet is sent to the router on the configured VLAN, then the router may send an ARP reply with a VLAN ID of zero.

  Conditions: The symptoms are seen on a Cisco 2800 series and a Cisco 7200 series router when the command **vlan-dot1q** *vlan-id* is configured on the GigabitEthernet interface of a Cisco 2800 series router and **encapsulation dot1q** *vlan- id* is configured on the FastEthernet 2/1/2.1 interface.

  Workaround: Change the Cisco 2800 series router's (CE) configuration to use a sub-interface for the vlan-id instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the 2800, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq64663

  Symptoms: Router Crashes when EtherChannel is shut down

Conditions: Occurs on a Metro Ethernet device with over 2000 IP SLA operations configured and CFM services defined for a EtherChannel. The **no int ether-channel ...** command causes the device to crash.

Workaround: There is no workaround.

- CSCsq67588

  Symptoms: On stateful switchover (SSO), the following message is seen on the active followed by the standby reset:

  CONST_ISSU-3-TRANSFORM_FAILED: ISSU CWAN APS Client(7003): receive transformation failed (ISSU_RC_NEGO_NOT_FINISHED)

  Conditions: Occurs after an SSO event.

  Workaround: There is no workaround.

- CSCsq67779

  Symptoms: Port numbering is incorrect during SNMPwalk. For example, PORT 3/1/3 is displayed as 3/0/13.

  Conditions: This is seen during SNMP walk of ES20 line cards.

  Workaround: There is no workaround.

- CSCsq67811

  Symptoms: System crashes due to I/O memory with the following error message:

  ```
  "%ETSEC-3-RECOVER_TX: Interface EOBC0/0 TX workaround invoked"
  ```

  Conditions: This condition is caused by a lockup inside the Ethernet Out of Band Channel (EOBC) MAC. This problem is rarely seen.

  Workaround: There is no workaround.

- CSCsq67817

  Symptoms: ETSEC freeze might cause router to crash due to memory depletion.

  Conditions: There is a rare hardware issue, which might lock up ETSEC driver transmit. This condition has been observed only once.

  Workaround: There is no workaround.

- CSCsq69178

  Symptoms: ISSU fails, and the standby continuously reloads.

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

  Workaround: There is no workaround.

- CSCsq70055

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

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

  Workaround: There is no workaround.

- CSCsq70980

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

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

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

- CSCsq71036

  Symptoms: On Cisco 7600 routers, a possibility exists of various error messages being seen due to memory corruption.

  Conditions: No known triggers. The error has never been reported on a Cisco 7600 router, only on Cisco 6000 routers.

  Workaround: There is no workaround.

- CSCsq73498

  Symptoms: Three MultiOS IPC processes: ciscoipc, ipc_test_admin_proc, and ipc_test_driver_proc fail with "IPC Error: send msg[3] failed ; Error - timeout" or "RPC message timed out".

  Conditions: This symptom occurs if an open IPC port is closed before the RPC response arrives.

  Workaround: Reload the router where IPC master is running.

- CSCsq73727

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

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

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

- CSCsq74300

  Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

  Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq75350

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

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

  Workaround: There is no workaround.

- CSCsq75944

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

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

  Conditions: Occurs when NetFlow is configured on one of the following:

  - Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
  - Catalyst 6500 running Cisco IOS Release 12.2SXH.

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

  no ip flow ingress no ip flow egress no ip route-cache flow

  Other Notes:

  Only the 12.2SRC and 12.2SXH code trains are affected. The specific versions affected are 12.2(33)SXH, 12.2(33)SXH1, 12.2(33)SXH2, 12.2(33)SXH2a, 12.2(33)SRC, and 12.2(33)SRC1

  The issue is fixed in the two affected code trains from the 12.2SXH3 and 12.2SRC2 releases onwards. However, for the SXH train, Cisco would recommend the use of SXH4 due to ddts CSCso71955.

  The following release trains do not have this issue; 12.2(18)SXF, 12.2(33)SRA, 12.2(33)SRB, 12.2(33)SXI and all other release trains after those affected.

- CSCsq77282

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

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

  Workaround: There is no workaround.

- CSCsq77638

  Symptoms: When the **mtu** command is issued in VC mode, before the ATM PVC state sync, the MTU CLI is getting executed in the secondary RP. The secondary RP is accessing invalid memory, which causes the RP to crash.

  Conditions: The **mtu** command is expected to be used in subinterface mode. When this command is issued in VC mode, the secondary RP crashes.

  Workaround: Do not execute **mtu** command in VC mode. Execute in subinterface only.

- CSCsq78539

  Symptoms: When running Cisco IOS Release 12.2(33)SRC1, a buffer leak may be seen in the system buffers.

  Conditions: The symptom is observed when an ARP request needs to be sent to resolve a next hop ip address. The exact conditions required for the leak are still being investigated, however.

  Workaround: Disable the optimized CEF neighbor resolution with the following commands: **no ip cef optimize neighbor resolution no ipv6 cef optimize neighbor resolution**

- CSCsq79253

  Symptoms: Once a packet buffer error is detected on a Pinnacle, traffic loss may occur after recovery.

  Conditions: The symptom is observed after the first packet buffer error is detected. During the first error detection, some interrupts are not re- enabled, leading to problems detecting and correcting subsequent errors.

  Workaround: Reload the affected module.

- CSCsq81116

  Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shut/no shut**.

  Conditions: Only occurs when OER master controller goes down and then rarely.

Workaround: There is no workaround.

- CSCsq81235

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

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

  Workaround: There is no workaround.

- CSCsq83501

  Symptoms: Router crashes while configuring more than 256 channel-groups in PA-MC-2T3-EC

  Conditions: The crash is seen after configuring more than 256 channel-groups in PA-MC-2T3-EC.

  Workaround: Do not configure more than 256 channel-groups:

- CSCsq84624

  Symptoms: A Cisco router might crash when **debug condition portbundle ip 10.1.1.1 bundle 0** is configured.

  Conditions: Occurs when this command is executed prior to configuring **ip portbundle**.

  Workaround: There is no workaround.

- CSCsq85971

  Symptoms: On application of unidirectional configuration on an HA setup having a 2x10GE ESM20 card, the standby will get reloaded. If the HA setup is reloaded with the configuration on active, the standby will not come up due to a configuration-synchronization failure.

  Conditions: The symptom is observed mainly when a unidirectional configuration is applied on a port of a 2x10GE ESM20 card.

  Workaround: There is no workaround.

- CSCsq86014

  Symptoms: When removing a subinterface on a Cisco 7600 series router, connectivity issues might occur on other subinterfaces that are part of the logical main interface.

  Conditions: The symptom is observed on an ES20 linecard and with Cisco IOS Release 12.2(33)SRB3 and Release 12.2(33)SRC1. It is seen when the configuration requires double-tagging. With a back-to-back connection, a QinQ sub-interface is created on either side and an IP address is assigned. Then, another sub-interface with the same outer VLAN is created and then removed.

  Workaround: Use the **shutdown no shutdown** command sequence to restore connectivity.

- CSCsq87788

  Symptoms: Diagnostic TestPortLoopback is failing for OC192 SPA in Cisco IOS Release 12.2(33)SRC image.

  Conditions: Occurs with the following control plane policing (CoPP) configuration:

  In the Service-policy

  Class cpp-default police cir 100000 bc 93750 be 187500 conform-action drop exceed-action drop violate-action drop

  router#sh class-map cpp-default

  Class Map match-all cpp-default (id 4) Match access-group name cpp-default

  router#sh access-lists cpp-default Extended IP access list cpp-default 10 permit ip any any (454914 matches)

Workaround: Remove the CoPP config, let the card boot up, and once the card is up, Apply the CoPP configuration again.

Further Problem Description: Further debugging has revealed that CoPP drops the packet. More specifically the "cpp-default" class that matches any IP address is the class which is hit and then the packet is dropped.

- CSCsq91348

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

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

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

- CSCsq91788

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

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

  Workaround: There is no workaround.

- CSCsq91960

  Symptoms: VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

  Conditions: This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

  - There may be a DATA CORRUPTION ERRMSG.
  - While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

  Workaround: There is no workaround.

- CSCsq93004

  Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

  Conditions: The symptoms are rare and will only be observed if a sub- interface is configured for **mpls traffic-eng auto-tunnel primary use**, and the sub-interface is later removed from the configuration.

  Workaround: Do not remove sub-interfaces.

- CSCsq93507

  Symptoms: After a second switchover, forward downstream traffic rate may be limited to 100 packets per second (pps) for all the ISG IP clients put together in that VRF. Upstream traffic is not impacted and continues to be normal.

  Conditions: The symptom is observed when a Cisco 7600 series router has a SIP400 linecard on the access side, with the sub-interfaces configured with the "access" keyword and when the core is facing MPLS. After the first SSO, traffic is not impacted. After the second SSO, the downstream traffic rate may drop to 100 pps.

  Workaround: There is no workaround.

- CSCsq93611

  Symptoms: Traffic does not flow out from the port with the "unidirection send- only" configuration applied to it. At the same time, counters show the number of packets sent out as almost equal to number of packets received on the interface.

  Conditions: This will be observed on a port on ES20 cards with unidirectional configurations applied to it. It is only observed when UDLD is enabled in global configuration and the ports on ES20 are also enabled for UDLD.

  Workaround: Disable UDLD on the ports with UDE (unidirectional) configurations. Use the following command in the "interface-config" mode: **udld port disable**

- CSCsq95123

  Symptoms: A Cisco 10000 series router that is configured for multicast might crash because of unexpectedly punted and replicated multicast packets.

  Conditions: The issue is caused by a PPPoEoE session churning, having no sessions active, just the loopback configured with "ip igmp static-group <group>" on loopback interfaces to improve delay for IGMP joins.

  Workaround: CoPP may be considered a workaround. However, a rate of 10-50 pps led to the PXF-crash and limiting the traffic more than that may impact multicast operation.

  Further Problem Description: The crashinfos all showed: %C10K-2-BADRSRCNUM: Invalid resource number from PXF (86). (PLEASE REPORT THIS!)

- CSCsr00820

  Symptoms: If the unidirectional configuration is removed from the port and a bi-directional fiber is connected to the port, the port may not come up.

  Conditions: The symptom is observed on ES20 cards.

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

- CSCsr06282

  Symptoms: Causes router to reload following a SNMP get operation.

  Conditions: Only occurs when a DHCP operation is configured with option-82 parameters.

  Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82

- CSCsr08994

  Symptoms: Traceback is seen while running FRF12.

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

  Workaround: There is no workaround.

- CSCsr09173

  Symptoms: After an Not-So-Stubby Area (NSSA) ABR reload, the default LSA may fail to generate on some NSSAs.

  Conditions: The symptom is observed following a reload or other circumstances like interface flapping.

  Workaround: Reconfigure the area as NSSA by the following command sequence: **no area** *number* **nssa no- summary** followed by **area** *number* **nssa no-summary**.

- CSCsr10893

  Symptoms: There may be high RP CPU utilization and the following message may be seen:

  ```
  %CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 30 seconds
  ```

Conditions: The symptom is seen with 2,000 bridge-domain EFPs and 2,000 local connect EFPS on ESM20G interfaces (xconnect is configured on each of these EVCs) and when the egress interface is shutdown using the **config t interface GigabitEthernet** *3/0/5* **shutdown** command.

Workaround: To speed up recovery, traffic into the local connect EFPs may be stopped and restarted.

Further Problem Description: Traffic is momentarily and wrongly punted to RP that causes RP to be busy and results in the above message. The condition is a transient one and system recovers from it in 2-3 minutes.

- CSCsr11085

  Symptoms: A single route loop whose gateway is covered by a default route remains in the RIB after a more specific route which resolves the gateway is removed. For example, the following routes may exist in the RIB:

  S* 0.0.0.0/0 is directly connected, Ethernet1/0 S 192.168.0.0/16 [1/0] via 192.168.1.2 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.1.0/24 is directly connected, Ethernet0/0 L 192.168.1.1/32 is directly connected, Ethernet0/0 192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.169.1.0/24 is directly connected, Ethernet1/0 L 192.169.1.1/32 is directly connected, Ethernet1/0

  If interface eth 0/0 goes down, then we have the following:

  S* 0.0.0.0/0 is directly connected, Ethernet1/0 S 192.168.0.0/16 [1/0] via 192.168.1.2 192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.169.1.0/24 is directly connected, Ethernet1/0 L 192.169.1.1/32 is directly connected, Ethernet1/0

  and

  Router#show ip route loop ->default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2 static 00:01:07 N

  In this case the route

  S 192.168.0.0/16 [1/0] via 192.168.1.2

  should be removed from the RIB.

  Conditions: The default route MUST be present in order for the above behavior to be considered wrong. If a default route is NOT present then the route

  S 192.168.0.0/16 [1/0] via 192.168.1.2

  is a misconfiguration and must be corrected by altering the configuration. Until the configuration is corrected, the route will remain in the RIB and traffic covered by that route will be dropped.

  Workaround: The one route loop can be removed from the RIB using the **clear ip route** command:

  clear ip route 192.168.0.0

  Further Problem Description: In the absence of the default route removal of the one route loop can lead to oscillation, which would seriously degrade the performance of the router.

- CSCsr13399

  Symptoms: Topology:

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

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

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

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

  The problem is seen in the following releases:

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

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

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

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

Workaround: There is no workaround.

- CSCsr20566

  Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

  Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

  Workaround: There is no workaround.

- CSCsr22628

  Symptoms: The secondary console of an HA router goes to disabled state

  Conditions: The symptom is observed when trying to access the standby console.

  Workaround: There is no workaround.

- CSCsr25168

  Symptoms: Router crashes while configuring destination interface range other than available interface.

  Conditions: Configure a monitor session with destination interface range other than available interface.

  Workaround: There is no workaround.

- CSCsr28305

  Symptoms: Connectivity issues are observed when using an L2 Port-Channel on a WS-X6708-10G with two links as part of a Port-Channel.

  Conditions: Member ports of the Port-Channel are on the same module and distributed different fabric connections. Traffic stream is ingress and egress this Port-Channel. For example, default gateway configuration for multiple VLANs, so traffic is ingressing and egressing this Port-Channel when switching between VLANs.

  Workaround: For usage of a Port-Channel with two member ports use interfaces which are on the same fabric connection:

  Fabric Channel #1: Ports 2, 3, 6, 8 Fabric Channel #2: Ports 1, 4, 5, 7

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsr40935

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

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

  Workaround: Stop traffic before applying service policy map.

- CSCsr41295

  Symptoms: The POS interface flaps continuously after removing the three-level policy from the POS interface.

  Conditions: The symptom is observed on a Cisco 7300 series router (NSE 100) with three-level policy.

  Workaround: Reload the router.

- CSCsr43800

  Symptoms: Router crashes on executing **vrf upgrade-cli multi-af-mode non-common-policies vrf**.

  Conditions: Occurs when **ip vrf X** is configured on an interface and execute and the **vrf upgrade-cli multi-af-mode non-common-policies vrf X** command is entered. Observed in a Cisco 7200 running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsr43944

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

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

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

- CSCsr45502

  Symptoms: A router intermittently runs into crashes in a large scale network with active PPPoEoA sessions.

  Conditions: This symptom occurs when many active PPPoEoA sessions exist.

  Workaround: There is no workaround.

- CSCsr48422

  Symptoms: Cisco 7600 router crashes with "no ipv6 unicast-routing", during unconfiguration.

  Conditions: Race condition occurs while deleting Cisco Express Forwarding (CEF) entries from a table.

  Workaround: There is no workaround.

- CSCsr50821

  Symptoms: A router may crash when ARP hits through interrupt level.

  Conditions: This symptom is observed when bridging is configured, but it may also be observed when the ARP code hits by interrupt context, which is unpredictable.

  Workaround: There is no workaround.

Further Problem Description: This defect was introduced via CSCsq05997. Cisco IOS Release 12.4 and 12.4T are not affected by this defect, but Cisco IOS Release 12.2S may be affected by this defect.

- CSCsr53264

  Symptoms: A software-forced crash occurs on the RP of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB2.

  Conditions: Occurs when the **clear ip route-map***name* command is entered.

  Workaround: Upgrade to Cisco IOS Release 12.2(33)SRC3 or later.

- CSCsr55278

  Symptoms: Fast switching of multicast packets may not occur on the interface of a PE router. All multicast packets are forwarded in process switching.

  Conditions: The symptom is observed after the interface is changed from a forwarding interface of one VRF to another VRF.

  Workaround: There is no workaround.

- CSCsr59284

  Symptoms: Memory allocation fails. Sometimes neighbor relationship also drops.

  Conditions: Happens after entering **show mem** command. After the system booted up, while the Cisco 7600 system was receiving the BGP routes, the command is entered. Upon hitting the space key to scroll the windows for two to three times. The following errors are displayed:

  ```
  "%COMMON_FIB-3-NOMEM: Memory allocation failure for CEF: terminal fibs list in IPv4
  CEF [0x08812F1C] (fatal) "
  ```

  Workaround: Enter the **show mem sum** command.

- CSCsr65372

  Symptoms: Router crashes after executing **no address-family ipv4 vrf** and then **clear ip route vrf x *** commands.

  Conditions: Occurs if the commands are entered when there are still BGP prefixes in the BGP table for that VPN routing/forwarding (VRF). The router crashes at some random point of time and not necessarily immediately after executing these two commands.

  Workaround: There is no workaround.

- CSCsr67289

  Symptoms: Router hangs when online insertion and removal (OIR) is performed.

  Conditions: Occurs after changing the interface bandwidth followed by an OIR operation.

  Workaround: Stop traffic before making these changes.

- CSCsr70687

  Symptoms: If we flap the SEND_LABEL configuration too quickly, the MPLS labels for those prefixes on a eBGP neighbor may not get allocated.

  Conditions: The symptom is observed if we apply PEERGROUP to a SEND-LABEL enabled eBGP neighbor.

  Workaround: Re-apply the SEND_LABEL configuration.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 Labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

Workaround: There is no workaround.

- CSCsr72810

  Symptoms: Unidirectional traffic is dropped when the PBR is configured with "set vrf" option between global and VPN routing/forwarding (VRF).

  Conditions: Occurs under the following scenario:

  - When PBR is configured with "set vrf" option between global and VRF

  - The router is running Cisco IOS Release 12.2(33)SRC1.

  Workaround: Configure the PBR with "set vrf" option among VRFs.

- CSCsr72959

  Symptoms: Router crashes.

  Conditions: Occurs after entering **no service dhcp**.

  Workaround: There is no workaround.

- CSCsr74002

  Symptoms: In some scenarios, UDLD packets received on a dot1q tunnel port in a VLAN where a Virtual Private LAN Services (VPLS) VFI is attached may be flooded to the VPLS VLAN without being processed locally. This may lead to port being err-disabled.

  Conditions: Occurs when some port configured as dot1qtunnel port in the VPLS VLAN. It will not process the received UDLD packet on those tunnel ports and will instead send them to the VPLS. If the VLAN interface with the VFI is shutdown, UDLD is processed normally.

  Workaround: Disable UDLD or enable spanning-tree in vfi vlan.

- CSCsr74295

  Symptoms: Upon reload, static routes pointing to MLPPP interfaces do not get inserted in the RIB.

  Example: ip route 172.16.2.2 255.255.255.255 multilink22

  Conditions: Occurs in a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: Reconfigure the static routes being affected, or simply configure **copy run start** to initialize the routes.

- CSCsr76733

  Symptoms: When hardware EoMPLS is configured on Port-channel sub interface, traffic is not forwarded.

  Conditions: This is seen only when the member links of the port-channel are ES20 interfaces.

  Workaround: There is no workaround.

- CSCsr86515

  Symptoms: Router crashed due to watchdog timeout in the virtual exec process:-

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (129/17),process = Virtual Exec.

  -Traceback= 40B5D8A8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
  420AA5A0 4054C05C 420570D8 40575510 41257298 41257284

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.

  -Traceback= 40B5D8C8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
  420AA5A0 4054C05C 420570D8 40575510 41257298 41257284
  ```

Conditions: This was observered on a Cisco 7600 with Supervisor 720 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

Workaround: There is no workaround.

- CSCsr93316

  Symptoms: A Cisco 7600 router is configured with **li-slot list <slot>**. When the slot is OIR removed and re-inserted, Lawful Intercept (LI) becomes RP-based instead of being done by the line card.

  Conditions: Occurs after an online insertion and removal (OIR) operation is performed on a line card configured for LI.

  Workaround: Re-apply the li-slot list config after the line card is inserted.

- CSCsu04360

  Symptoms: Acct-Time-Delay and Tunnel-Link-Stop records are missing from L2TP network server (LNS).

  Conditions: Occurs when using radius server for authentication.

  Workaround: There is no workaround.

- CSCsu04473

  Symptoms: Upon the first SSO switchover triggered with the **redundancy force-switchover** command, the traffic stops on the ATM N-to-1 VCC pseudowires configured with cell-packing in the direction from the MWR towards the 7600 SPA-4XOC3-ATM interface. Traffic recovers normally in the other direction.

  Conditions: Occurs on a Cisco 7600 S-series equipped with dual SUP720-3BXL. The problem is seen only when cell-packing is enabled on the N-to-1 VCC pseudowires and when APS (MR-APS) is configured on the ATM OC3 interface of the Cisco 7600 SPA-4XOC3-ATM.

  Workaround: Disable cell-packing on the ATM N-to-1 VCC pseudowires or alternatively disable APS on the SPA-4XOC3-ATM interface.

- CSCsu05525

  Symptoms: After removing the "default-originate" configuration, the default-route is not withdrawn.

  Conditions: Occurred on a router running Cisco IOS Release 12.2SR.

  Workaround: Clear the session to remove the configuration.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4 byte CE is peered to a 2 byte capable PE using AS 23456 and the command **as-override** is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use "allowas-in" on the CE.

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

  Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map): 1) **neighbor x.x.x.x soft-reconfiguration inbound** 2) **neighbor x.x.x.x weight** 3) **neighbor x.x.x.x filter-list in**

  If any one of the commands is not configured, then the router will not crash.

Workaround: Configure route-map instead of filter-list for inbound direction. For example: "neighbor x.x.x.x filter-list 1 in" replace with "neighbor x.x.x.x route-map *name* in"

where, route-map *name* permit 10 match as-path 1

- CSCsu26315

  Symptoms: Traffic may not resume on ATM over MPLS (ATMoMPLS) connections.

  Conditions: The symptom is observed when both ATMoMPLS and ATM over LS (ATMoLS) connections are on same card and a card reset is done.

  Workaround: Reload the PXF.

- CSCsu26526

  Symptoms: Memory leak can be seen on the LNS.

  Conditions: The symptom is observed on the L2TP Network Server (LNS) when the PPP client does a renegotiation.

  Workaround: There is no workaround.

- CSCsu27642

  Symptoms: When a router performs a failover, traffic may be interrupted to a small number of destinations. Interruption is dependant on the setting of the "ipv6 nd reachable-time" value and will occur within a few minutes of failover.

  Conditions: The symptom is observed when the router is forwarding IPv6 packets to a large number of destinations and when the router has a very large number (several thousand) of ND cache entries. It occurs after the router performs an HA failover from primary to secondary.

  Workaround: Set "ipv6 nd reachable-time" to a value of ten minutes or longer.

  Further Problem Description: Traffic interruption is caused by IPv6 ND refreshing cache entries via NUD during HA failover convergence. If ND has a very large cache then the additional load of NUD during the convergence period may cause some cache refreshes to fail. This will result in traffic interruption.

- CSCsu31549

  Symptoms: When a router with a large-scaled configuration is provisioned to perform a PRE failover, a PXF crash occurs (for example "switchover pxf restart 1 0"). This could result in missed IPC keepalives while the large crashinfo file is being written and cause unexpected behavior, including line card reloads.

  Conditions: This symptom occurs when the router has a large configuration and has been configured with something similar to the following:

  redundancy mode sso main-cpu switchover pxf restart 1 0

  In order to perform a PRE Failover whenever a PXF crash occurs.

  Workaround: There is no workaround.

- CSCsu32104

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

  Conditions: Unknown at this time.

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

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

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

Workaround: Do not use EIGRP to redistribute BGP.

- CSCsu39152

  Symptoms: IF-MIB registration fails as there are no free ifIndex available.

  Conditions: Occurs after an upgrade. Seen only in HA systems.

  Workaround: There is no workaround.

- CSCsu39345

  Symptoms: Local switching may not pass traffic following an ATM LC reset.

  Conditions: The symptom is observed with an ATM LC reset followed by SSO.

  Workaround: Use the following commands on the LS connection: **shutdown** then **no shutdown**.

- CSCsu39689

  Symptoms: A router may crash while unconfiguring 6PE IPv6 Routing Information Protocol (RIP) related configurations.

  Conditions: The symptom is observed when unconfiguring the 6PE IPv6 RIP configurations from all CE and PE routers concurrently.

  Workaround: There is no workaround.

- CSCsu39864

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

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

  Workaround: Do not have this option configured.

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

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

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

  Workaround: There is no workaround.

- CSCsu46644

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

  ```
  % Authentication failed
  ```

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

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

- CSCsu47792

  Symptoms: Convergence for BGP prefixes over unequal paths is not prefix independent and instead depends on the number of BGP prefixes.

  Conditions: The symptom is observed only with BGP prefixes over unequal paths.

  Workaround: There is no workaround.

- CSCsu48898

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

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

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

- CSCsu61813

  Symptoms: Line cards may reset during ISSU upgrade even when there is no change in the major number.

  Conditions: This symptom may occur during ISSU upgrade even though there is no change with the major number of line card images.

  Workaround: There is no workaround. However the line card comes up fine after the reset.

- CSCsu70871

  Symptoms: On a PRE4, the default counters of the "show policy-map" interface do not increment with PPPoEoQinQ sessions.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB with PPPoEoQinQ sessions.

  Workaround: There is no workaround.

- CSCsu73404

  Symptoms: After using the **no card** command on the SPA card, the SPA configuration still exists on the secondary PRE. After switchover, due to configuration mismatch, the standby will keep resetting.

  Conditions: The symptom is observed under the following conditions: 1. The standby crash is seen with a SPA card removal, using the **no card** command and an SSO switchover. 2. The configuration for the SPA continues to exist on the standby when the **no card** command is used on the SPA card.

  Workaround: There is no workaround.

- CSCsu76354

  Symptoms: Some ATM subinterfaces stop the output of packets after an SSO.

  Conditions: Though the encapsulation string is displayed and the VCCI value is not 0x0 on the normal sub-interfaces (using the by **show ip cef** *VRF IP* **plat** command) no encapsulation string is displayed and the VCCI value is 0x0 on the defective sub-interface after the SSO by the **show** command: Encap String:

  After **shut/no shut** on the defective subinterface, the encapsulation string comes to be displayed and VCCI value is not 0x0 on it by the **show** command. Encap String:
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  The incidence of this occuring is about one in every five SSO executions.

  Workaround: There is no workaround.

- CSCsu76800

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

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

  Workaround: There is no workaround.

- CSCsu83765

  Symptoms: Basic ping may fail and hw_vector traceback may be seen.

  Conditions: The symptoms are observed with a basic ping from the client to a Cisco 10000 series router.

  Workaround: There is no workaround.

  Further Problem Description: This issue is seen after the fix for CSCsr85671.

- CSCsu87257

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

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

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

- CSCsu94782

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

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

  Workaround: There is no workaround.

- CSCsu96730

  Symptoms: Intelligent Services Gateway (ISG) traffic from one user to another may fail if the packet needs to be processed by the RP in a Cisco 7600.

  Conditions: Occurs when ISG is configured and packets are switched from one subscriber to a second subscriber.

  Other symptoms: - Counters of packet transfer might show difference between user transferring between each other - Access-list might fail to block the packet

  The 2 above symptoms will be seen when user are sending receiving on the same interface via the ISG

  Workaround: There is no workaround.

- CSCsu97934

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

  Conditions: Unknown.

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

- CSCsu98011

  Symptoms: A router may hang.

  Conditions: The symptoms are observed when doing a snmpbulkwalk on the object .1.3.6.1.4.1.9.9. The router will hang at a QOS object.

  Workaround: Apply a snmpview to block the following object (which is the ciscoCBQosMIB): .1.3.6.1.4.1.9.9.166

- CSCsv01559

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

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

  Workaround: There is no workaround.

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

- CSCsv04674

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

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

  Workaround: There is no workaround.

- CSCsv04752

  Symptoms: An LI tap remains "Operational" even after tap removal.

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

  Workaround: Reload of the router removes the stale tap.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsv05057

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

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

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

- CSCsv05899

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

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

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

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

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

  Workaround: There is no workaround.

- CSCsv13738

  Symptoms: There are two ways to define VRFs when supporting the 6VPE feature: 1) ip vrf 2) vrf definition. The "vrf definition" configuration may take a much longer time to allow convergence between the PE and the CE than the "ip vrf" configuration.

  Conditions: The symptoms are observed under the following conditions: - when the router boots up; and - when the issue has been seen using the "vrf definition" configuration; and - when the router has over 100,000 VPNv4 BGP routes; and - when a large number of VRFs are configured.

  Workaround: Use the "ip vrf" configuration, if you have only IPv4 VRFs configured.

- CSCsv14963

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

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

  Workaround: There is no workaround.

- CSCsv16421

  Symptoms: The cbQosCMDropPkt64 object does not work on the PE-CE policy with priority police command. The value stays at 0.

  Conditions: The symptom is observed when Priority is configured with policy. The cbQosCMDropPkt count stays at 0 during snmpwalk.

  Workaround: There is no workaround.

- CSCsv16869

  Symptoms: BGP updates may not be sent out.

  Conditions: The symptom is observed when neighbors are flapped in a large-scale scenario.

  Workaround: There is no workaround.

- CSCsv25836

  Symptoms: LS-related toaster structures are not set up in UUT and are not allowing the line protocol in CEs to come up.

Conditions: The issue is seen in following scenarios: - **hw-module slot <> sh** and **no hw-module slot <> sh** - **hw-module slot <> reset** - IOS reload.

Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv33977

  Symptoms: BGP peer fails to exchange the OPEN Message for negotiating capability when the neighbor router does not support any BGP capabilities.

  Conditions: The symptom is observed when the neighbor router does not support any BGP capabilities and when the capability negotiation fails due to an SSO switchover.

  Workaround: Configure "neighbor x.x.x.x dont-capability-negotiate". Issue the **clear ip bgp *** command when the issue occurs.

- CSCsv40343

  Symptoms: When a class-map has both "match ip dscp" and "match dscp" (with "match ip dscp" as the first match), IPv6 packets are not matched.

  Conditions: This symptom is observed on PRE4 only and only when class-map has both "match ip dscp" and "match dscp" (with "match ip dscp" as the first match).

  Workaround: Only have "match dscp", which should match both IPv4 and IPv6 packets.

- CSCsv44271

  Symptoms: When an OIR is performed followed by the **no card <>** command, the Standby may crash.

  Conditions: The symptom is observed when the **hw-module slot <> shut /removal of card** command is followed by the **no card <>** command.

  Workaround: There is no workaround.

- CSCsv45649

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

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

  Workaround: There is no workaround.

- CSCsv47932

  Symptoms: A build break is observed while building PRE2 image.

  Conditions: The fix for CSCsu33326 is causing a build breakage.

  Workaround: There is no workaround.

- CSCsv80398

  Symptoms: There may be a PXF crash when removing and re-applying the DLCI.

  Conditions: The symptom is observed when multicast traffic is flowing, and if we remove the existing DLCI and re-apply the same DLCI after a few seconds.

  Workaround: There is no workaround.

- CSCsv82676

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

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

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

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

- CSCsv89255

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

  Conditions: The symptom occurs when there are 500 VRF configurations with ACL and QoS configured.

  Workaround: There is no workaround.

- CSCsv91467

  Symptoms: Unable to bring up PPPoEoVLAN sessions.

  Conditions: The symptoms are observed on a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCsv92961

  Symptoms: Bounce the interface between PE and receiver CE, the traffic does not resume.

  Conditions: This symptom occurs on a multicast-enabled frame relay interface on an ESR that is acting as an encap PE. It appears after a **shut** command followed by a **no shut** command on the frame relay interface connected to the CE sending traffic. The multicast traffic stops passing through this interface. The CE is sending traffic continuously while the the **shut** command followed by the **no shut** command operation is performed on the PE.

  Workaround: Stop traffic and then wait for timers to expire and start traffic again. The traffic flows through the interface.

- CSCsv96082

  Symptoms: PRE4 MLFR shape rate is not working in certain scenarios.

  Conditions: The symptom is observed under the following scenario: 1. When a link is down in the bundle, **show policy-map** shows the shape rate is set to be 3M. 2. After a router reload (with one link still down), the **show policy- map** output now shows that the shape rate is 100M. 3. Bounce the service-policy on the subinterface. (This fixes the issue.) 4. Then, bring the link up. Instead of the shape rate changing to 3072k, it remained at 1536k. The traffic passing also reflected this shape rate (1536k) even though at this point, the shape rate should be 3072k. 5. To fix, bounce the service-policy again.

  Workaround: Remove and re-insert service-policy.

- CSCsv99087

  Symptoms: If a policy with a priority police percent class is applied on a POS FR main interface, it may result in a different policing rate than if the policy is applied on the FR sub-interface.

  Conditions: The symptom is observed on a PRE4 engine on a Cisco 10000 series router only.

  Workaround: Configure policing rate in bps instead of percentage points.

- CSCsv99716

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

Conditions: The symptom is observed on a Cisco platform, when enabling the debug command **debug issu all** in the router and doing a loadversion.

Workaround: Do not turn on ISSU debug.

- CSCsw14166

  Symptoms: A router may crash.

  Conditions: The symptom is observed when the command **test pppoe 1 1** *interfacename* is applied and while establishing a PPPoE session.

  Workaround: Configure service name in the **test pppoe** command.

- CSCsw32073

  Symptoms: EIGRP BFD session may not come up after BFD is added to the interface.

  Conditions: The symptom is observed in the following scenario: We want to set up BFD for interface e0 under EIGRP AS 10. interface e0/0 ip address 10.1.1.1 255.255.255.0 router eigrp 10 net 10.0.0.0 If we configure BFD in this order: - first under router eigrp: router eigrp 10 bfd int e0 - then under interface e0: int e0 bfd int 100 m 100 m 3 If interface e0 also participates in other EIGRP AS configured on the router, then EIGRP may not activate the BFD session.

  Workaround: Configure BFD under interface before configuring under router EIGRP.

- CSCsw37620

  Symptoms: A 4HHCT3 card crashes on performing ISSU/MDR.

  Conditions: This symptom is seen only during ISSU/MDR upgrade.

  Workaround: There is no workaround.

  Further Problem Description: MDR should take effect, but is not taking effect currently.