Caveats for Cisco IOS Release 12.2(33)SRE

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

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

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

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

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

This section consists of the following subsections:

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRE15a

Table 1 Resolved Caveats for Cisco IOS Release 12.2(33)SRE 15a

Caveat ID Number	Description
CSCsv05154	Cisco IOS HTTP server vulnerable to CSRF attacks
CSCuw48118	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCuw77959	Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability
CSCuy82078	Cisco IOS and IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability
CSCva61877	IPv6 neighbor discovery packet processing behavior
CSCva74756	OSPF Rogue LSA with maximum sequence number vulnerability
CSCva94139	IPv6 neighbor discovery packet processing behavior with SIP-400
CSCve54313	Crash in ALPS SNMP code
CSCve57697	Crash in Bstun SNMP code
CSCve60276	Crash in ADSL SNMP code
CSCve60376	Crash in ADSL DMT SNMP code
CSCve60402	Crash in Voice DNIS SNMP code
CSCve66601	Crash in CISCO-SLB-EXT-MIB code
CSCve66658	Crash in TN3270E-RT-MIB code

Resolved Caveats—Cisco IOS Release 12.2(33)SRE15

Table 2 Resolved Caveats for Cisco IOS Release 12.2(33)SRE 15

Caveat ID Number	Description
CSCub04965	TCP Session hung causing Packet loss
CSCuh43252	unable to login and high cpu when authenticating with TACACS
CSCup90532	Cisco IOS and IOS XE Software DNS Forwarder Denial of Service Vulnerability
CSCud36767	Cisco IOS and IOS XE MSDP SA Message Denial of Service Vulnerability
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory contents

Resolved Caveats—Cisco IOS Release 12.2(33)SRE14

Table 3 Resolved Caveats for Cisco IOS Release 12.2(33)SRE 14

Identifier	Description
CSCuv13695	Software crash due to coping local file to unavailable remote FTP server
CSCtx38443	After bulk-sync with churn, multiple issues with scale IP/DHCP sessions
CSCuu66959	Virtual-Access input counters not working as expected
CSCtn19883	IOSD crash seen while negotiating an ISAKMP SA in Codenomicon testing

Resolved Caveats—Cisco IOS Release 12.2(33)SRE13

Table 4 Resolved Caveats for Cisco IOS Release 12.2(33)SRE 13

Identifier	Description
CSCuu18788	DATACORRUPTION-1-DATAINCONSISTENCY when polling ceExtSysBootImageList
CSCtg57619	ASR RP crash due to BGP Router process
CSCum65703	Inconsistency on config "privilege" commands as seen in running-config
CSCue29568	SAMI being power cycled due to SUP keep alive failure
CSCum94811	TCP Packet Memory Leak Vulnerability
CSCts66733	Crash @ tftp_server

Resolved Caveats—Cisco IOS Release 12.2(33)SRE12

Table 5 Resolved Caveats for Cisco IOS Release 12.2(33)SRE12

Identifier	Description
CSCuo18705	SIP400: Traffic through TE backup tunnel is dropped
CSCun86087	Packets for some VPLS VCs dropped in imposition with core Port-Channel
CSCtx04709	Active routes remain in topology but does not go SIA after route lost
CSCup13194	EIGRP Authentication Bypassed if Auth Type is unknown
CSCuo84660	copy command yields DATACORRPUTION error
CSCuo29652	DDTS to fix nightly build errors
CSCur77750	CSCtc51539 happening again on SRE6 onwards

Resolved Caveats—Cisco IOS Release 12.2(33)SRE11

Table 6 Resolved Caveats for Cisco IOS Release 12.2(33)SRE11

Identifier	Description
CSCtt28573	ES20 LC crash observed on router reload / LC OIR
CSCun91678	7600 VPLS PW increase STP cost to 2M for MST0 - moving Vlanfrom MST0to1
CSCuo13314	ES+ crash after Mlacp switchover
CSCun35055	RPF not reset for vlan freed by shut down
CSCun58072	ifOutOctets go backwards when output drop happens on FR subintf
CSCuo62753	LC goes in minor error after microcode reload generating traceback
CSCuo60001	MFR links does not come up after patriot spa reload
CSCui51363	Multilink interface stays down when T-1s flap
CSCuj60533	7600 - CPUHOG on reload when modules fail to come online
CSCue27665	CST: CPUHOG and PRE crash when shut/no shut bundle
CSCth64507	“event manager policy multiple_ed_8.tcl type user” causes bulk sync fa
CSCti08811	event manager cli command cause parser crash
CSCtl70569	Traceback seen under event manager applet mode

Resolved Caveats—Cisco IOS Release 12.2(33)SRE10

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while performing “write memory” or “show running configuration” on the router after configuring “privilege exec level 15 show adjacency”.

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCts39290

  Symptom: Under runs counter increments report for native Gigabit interfaces of NPE-G1.

  Conditions: This symptom is not observed any specific conditions.

  Workaround: This issue can be resolved by clearing the interface.

- CSCue00996

  Symptom: The Cisco IOS Software implementation of the Network Address Translation (NAT) feature contains two vulnerabilities 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 these vulnerabilities.

  There are no workarounds to mitigate these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat

Note The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six 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 2014 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_mar14.html

Conditions: See published Cisco Security Advisory

Workaround: See published Cisco Security Advisory

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

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

CVE ID CVE-2014-2111 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

- CSCug84789

  Symptom: A vulnerability in the Cisco 7600 Series Route Switch Processor 720 with 10 Gigabit Ethernet Uplinks models RSP720-3C-10GE and RSP720-3CXL-10GE could allow an unauthenticated, remote attacker to cause the route processor to reboot or stop forwarding traffic. The vulnerability is due to an issue in the Kailash field-programmable gate array (FPGA) versions prior to 2.6.

  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-20140326-RSP720 10GE

Note The March 26, 2014, Cisco IOS Software Security Advisory bundled publication includes six 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 2014 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_mar14.html

Conditions: See published Cisco Security Advisory

Workaround: See published Cisco Security Advisory

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

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

CVE ID CVE-2014-2107 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

- CSCuh45042

  Symptom: Traffic on some GIG subinterfaces are seen to be dropped at the SPA. The SPA TCAM is seen to have two entries sharing the same logical address as a result of which one entry is seen to overwrite the other.

  Conditions: This symptom was observed after a router/LC/SPA reload. The exact condition that triggers this symptom is not known.

  Workaround: There is no workaround.

- CSCuh91645

  Symptom: WS-SUP720-3B crashes while receiving DHCP packets.

  Conditions: This symptom occurs with the **ip dhcp relay information policy-action encapsulate** command.

  Workaround 1. Use the **ip dhcp relay information policy-action replace** command.

  Workaround 2. Use the **no ip dhcp relay information trusted** command.

- CSCui29745

  Symptom: Member links under MLPPP go down as the LCP negotiation of those PPP links fails.

  Conditions: This symptom occurs after the router reloads and the traffic is flowing through the multilink.

  Workaround: Reload SPA/LC on the other end of the link.

- CSCui65914

  Symptom: Minor or major temperature alarms are reported in the syslog along with the following DATACORRUPTION logs:

  ```
  Aug 5 15:54:30.972 Buc: DATACORRUPTION-SP-1-DATAINCONSISTENCY copy error, -PC=
  0x414DEED4z -Traceback= 4027C4F4 419551C0 414DEED4 414E5BC4 414E0CA0 414E0F00 Aug 5
  15:54:30.972 Buc: C6KENV-SP-4-MINORTEMPALARM interface 10/0 outlet temperature crossed
  threshold #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: There is no workaround.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

- CSCuj82897

  Symptom: The “control-word” length is not set properly for small HDLC packets running over HDLC AToM VC with SIP-200. For example: SPA-8XCHT1/E1.

  Conditions: This symptom occurs when HDLC AToM VC with SIP-200 is deployed, for example, SPA-8XCHT1/E1, will result in a packet length mismatch issue or dropping by the remote PE router when HDLCoverMPLS runs over the Ethernet link adding an additional padding which cannot be classified at all.

  Workaround: Use SIP-400.

- CSCul27327

  Symptom: On the Cisco c7600 router, if PIM is configured on the port-channel and on the port members, any failure on one of the port members will disable the FE CAM.

  Conditions: This symptom occurs when PIM is configured on the port members.

  Workaround: Perform the following workaround:

  1. Do not configure PIM sparse-mode on the port members even though the CLI is accepted.
  2. In case the PIM sparse-mode is configured on the port members, remove it from the port members and the port-channel and then reapply the PIM configuration on the port-channel only.

  Further Problem Description: A similar issue (CSCtf75608) is seen on the Cisco Catalyst 6500 Series Switches, but the workaround is to configure PIM on the port-channel and the port members to avert the FE CAM to be disabled in the event of one of the port members failing.

- CSCul52239

  Symptom: Multicast traffic might get affected after an interface delete and reconfiguration. This is more likely to happen in dot1q sub-interfaces in ES+ and specifically only if the delete and reconfiguration of the interface is done within 30 seconds.

  Conditions: This symptom occurs in Cisco IOS Release 12.2SREx and Cisco IOS 15S based releases.

  Workaround: Perform interface delete and reconfiguration with a time gap of one minute.

  Further Problem Description: To check whether the issue is hit:

  Note down the interface’s internal vlan: PE2#sh vlan int usage | i GigabitEthernet2/24.904 2000 GigabitEthernet2/24.904

  Get to SP console and do “sh fid start <internal vlan> end <internal vlan>”

  PE2-sp#sh fid start 2000 end 2000 FID Id Protocol Bkt Enabled FE CAM Enabled Vlan Don’t Learn Age group ------ -------------------- -------------- ---- ----------- --------- 2000 no no 2000 yes 0x00

  The issue is hit if “FE CAM Enabled” bit is set to “no”.

- CSCul65614

  Symptom: The FAN-MOD-6SHS module consumes more power than expected (should be around 180W).

  ```
  #sh power <SNIP> Fan Type Watts A @42V State ---- ------------------ ------- ------
  ----- 1 FAN-MOD-6SHS 427.14 10.17 OK
  ```

  Conditions: This symptom occurs when the ES+ Combo card is placed in slot-1 of 7600 chassis.

  Workaround: Place ES+ Combo cards in any other slot other than slot-1 of 7600 chassis.

- CSCum16315

  Symptom: Upon reload of a Cisco 7600 router configured with a CoPP policy containing IPv6 ACLs and DSCP matching, the CoPP is only applied to the active RSP as shown below.

After reload:

```
lab-7609-rsp-02#sh mod power Mod Card Type Admin Status Oper Status ---
------------------------------------ ------------ ------------ 1 CEF720 48 port
10/100/1000mb Ethernet on on 5 Route Switch Processor 720 (Active) on on 6 Route
Switch Processor 720 (Hot) on on 7 CEF720 8 port 10GE with DFC on on 8 CEF720 8 port
10GE with DFC on on
```

CoPP is applied to only the active RSP/SUP after reload:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl class-map:
COPPCLASS_MCAST (match-any) Earl in slot 5 : class-map: COPPCLASS_MGMT (match-any)
Earl in slot 5 : class-map: COPPCLASS_ALLOW_ICMP (match-any) Earl in slot 5 :
class-map: COPPCLASS_MONITORING (match-any) Earl in slot 5 : class-map:
COPPCLASS_FILEXFER (match-any) Earl in slot 5 : class-map: COPPCLASS_REMOTEACCESS
(match-any) Earl in slot 5 : class-map: COPPCLASS_OSPF (match-any) class-map:
COPPCLASS_LDP (match-any) Earl in slot 5 : class-map: COPPCLASS_BGP (match-any)
class-map: COPPCLASS_MISC (match-any) class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 5 : class-map: COPPCLASS_IPV4_CATCHALL (match-any) Earl in slot 5 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any) class-map: class-default (match-any)
Earl in slot 5 :
```

When this issue is triggered, the following error will be seen in the logs:

```
*Dec 14 02:33:14.579: %QM-2-TCAM_BAD_LOU: Bad TCAM LOU operation in ACL
```

This issue potentially exposes the device to a DoS vulnerability.

Conditions: This symptom occurs under the following conditions:

1. 7600 HA Environment.
2. CoPP IPV6 ACL with DSCP match.
3. Reload or Switchover.

Workaround: There are two workarounds for this issue.

1. Modify the CoPP Policy to remove IPV6 ACL/DSCP matching.
2. Remove and reapply the CoPP configuration as shown below:

```
lab-7609-rsp-02(config)#control-plane lab-7609-rsp-02(config-cp)#no service-policy in
COPP lab-7609-rsp-02(config-cp)#service-policy in COPP lab-7609-rsp-02(config-cp)#end
```

CoPP is applied to all modulues as required:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl class-map:
COPPCLASS_MCAST (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in
slot 8 : class-map: COPPCLASS_MGMT (match-any) Earl in slot 1 : Earl in slot 5 : Earl
in slot 7 : Earl in slot 8 : class-map: COPPCLASS_ALLOW_ICMP (match-any) Earl in slot
1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_MONITORING
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: COPPCLASS_FILEXFER (match-any) Earl in slot 1 : Earl in slot 5 : Earl in
slot 7 : Earl in slot 8 : class-map: COPPCLASS_REMOTEACCESS (match-any) Earl in slot 1
: Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_OSPF
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: COPPCLASS_LDP (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7
: Earl in slot 8 : class-map: COPPCLASS_BGP (match-any) Earl in slot 1 : Earl in slot
5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_MISC (match-any) Earl in
slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map:
COPPCLASS_UNDESIRABLE (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 :
Earl in slot 8 : class-map: COPPCLASS_IPV4_CATCHALL (match-any) Earl in slot 1 : Earl
in slot 5 : Earl in slot 7 : Earl in slot 8 : class-map: COPPCLASS_IPV6_CATCHALL
(match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7 : Earl in slot 8 :
class-map: class-default (match-any) Earl in slot 1 : Earl in slot 5 : Earl in slot 7
: Earl in slot 8 :
```

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

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

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

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRE9a

Cisco IOS Release 12.2(33)SRE9a is a rebuild release that addresses a critical issue for Cisco IOS Release 12.2(33)SRE.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int and other card types, such as ES20/ LAN cards, are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fails. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

Open Caveats—Cisco IOS Release 12.2(33)SRE9

Cisco IOS Release 12.2(33)SRE9 is a rebuild release for Cisco IOS Release 12.2(33)SRE.

- CSCtn00145

  Symptom: Standby sup reloads on issuing the **no ip route** command.

  Conditions: This symptom is observed when static route statements present on the active and is missing on the stand-by. Perform these steps to recreate the issue:

  1. Configure a static route with an interface dependency (eg: ip static route 1.1.1.0 255.255.255.0 eth 0/0).
  2. Shutdown the Hardware Module/SPA corresponding to that interface. When the hardware module/SPA corresponding to that interface is shutdown, the static route entry is hidden from the configuration.
  3. Reload the stand-by. When stand-by comes up, it performs a bulk sync to the running configuration of master. However the static routes which are HIDDEN, won't be present in the running configuration of master and hence will not be created in stand-by.
  4. Bring up the hardware module/SPA. As this is still treated as OIR, the HIDDEN flag will be removed from the static routes and other related configurations will now be part of running configurations in the master. However these static routes are not present in stand-by as these information is lost due to reload and there will not be a disclosure of routes in standby and standby will be missing these static routes.
  5. User executes no ip route. The route will be removed from master but as standby doesn't have these routes, it will result in a PRC failure leading to a standby reload.
  6. Stand-by comes up after the reload. Now, it will have the entire configuration along with static routes in sync as the unhidden static routes are now part of the running configurations that are synced to standby

Workaround: Reloading the standby (most likely in a maintenance window) is the only way to sync missing ip route statements.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE9

Cisco IOS Release 12.2(33)SRE9 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE9 but may be open in previous Cisco IOS releases.

- CSCsl38246

  Symptom: When console logging is turned on, a flood of the messages shown below can potentially lead to watchdog invocation and a subsequent crash:

  ```
  %MWAM-DFC3-0-CORRECTABLE_ECC_ERR: A correctable ECC error has occurred,
  A_BUS_L2_ERRORS: 0x0, A_BUS_MEMIO_ERRORS: 0xFF, A_SCD_BUS_ERR_STATUS: 0x80DC0000
  ```

  Conditions: A single-bit correctable error is detected on a CPU read from DRAM. As long as the errors remain correctable, and the performance of the processor does not deteriorate, the module is usable.

  Workaround: Since this is a parity error you can prevent the issue from happening in the future by reseating the module. If the issue still persists after reseating the module then we may be facing a hardware issue.

- CSCsv74508

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset(either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

- CSCtb34814

  Symptom: The following error message is reported just before a crash:

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

  There may not be any tracebacks given for the crash.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCtd72271

  Symptom: On an L3 port-channel with member interfaces of a 7600-ES+4TG3CXL module, after a member interface has recovered from a failure or when a shut/no shut is performed, this member interface starts flapping and the output traffic is dropped.

  Conditions: This symptom occurs when a service policy is attached or VRF is configured on a port-channel interface and there are two members on it.

  Workaround: Remove the service policy from the port-channel interface

- CSCtf31377

  Symptom: IOS crashes due to processor pool memory corruption.

Conditions: This symptom occurs due to processor pool memory corruption. IOS generates one or more CLUE memory error messages similar to the following messages:

```
%CLUE-DFC3-3-SOR_CORRUPT: CLUE record corruption in start of record field, record id
3341, record
starting address 0x5FFFFF90
```

This issue could also be seen on LAN cards of a Cisco 7600 router.

Workaround: There is no workaround.

- CSCtj29261

  Symptom: Customer received the following error messages on a Cisco ASR router:

  ```
  %SYS-2-SHARED: Attempt to return buffer with sharecount 0
  ```

  Conditions: This issue can occur when the Cisco ASR 1000 router receives STP packet because it is not yet supported on Cisco ASR 1000.

  Workaround: Stop sending STP packet.

- CSCtj61284

  Symptom: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

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

  Workaround: There is no workaround.

- CSCtk32299

  Symptom: SVI state remains down.

  Conditions: This symptom occurs when scaled MTP and SVI configurations are copied to the router.

  Workaround: Unconfigure and configure MTP and SVI configurations.

- CSCty12641

  Symptom: CFM ethernet ping fails with 7600 as the remote MEP end.

  Conditions: This symptom is observed after remote CFM over Xconnect MEPs with MEPs terminating on 7600 and having ESM20 LC.

  Workaround: There is no workaround. Consider using ES+LC.

- CSCue01146

  Symptom: SNMP GET fails for VPDN-related MIB.

  Conditions: This symptom occurs while receiving an SNMP GET for the MIB before all VPDN configurations are applied.

  Workaround: Reload the router.

- CSCue05492

  Symptom: The DHCP snooping client ignores the IPC flow control events from CF.

  Conditions: This symptom is observed when CF gives flow control off event and the DHCP snooping client does not handle it.

  Workaround: There is no workaround.

- CSCue44554

  Symptom: Traffic stops forwarding over port-channels configured with FAST LACP after an RP switch over.

  Conditions: This symptom occurs after an RP fail over.

  Workaround: A shut/no shut interface will help recover.

- CSCue59592

  Symptom: Multiple crashes observed with the following tracebacks after upgrading the Cisco IOS Release from 12.2(33)SRC1 to 12.2(33)SRE6:

  ```
  *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to lock a
  semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
  lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
  lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC
  ```

  Conditions: This symptom is observed with a combination of BGP VPNv4 prefixes + PBR enabled on the interface for the VRF and during upgrade of image or reload of the device. If “mls mpls recirc agg” is enabled in global mode, then this crash will not be observed.

  Workaround: Enable “mls mpls recirc agg” in global mode.

- CSCue86845

  Symptom: An unexpected behavior caused with Ingress QoS, caused by commit CSCuc01040.

  Conditions: This symptom is observed with Ingress QoS, caused by commit CSCuc01040.

  Workaround: There is no workaround.

- CSCue94653

  Symptom: When the port-security configured interface goes to blocking state (MST), the VLANs configured on the port go to not-forwarding state temporarily. The secure mac-addresses are not added back resulting in loss of traffic.

  Conditions: The symptom is observed when the port-security configured interface goes to blocking state.

  Workaround: Shut and no shut the port-security interface to re-add the mac-addresses.

- CSCuf17009

  Symptom: With PIM enabled on a P2P GRE tunnel or IPSec tunnel, the SP of the Cisco 7600 series router might crash.

  Conditions: This symptom occurs when there are more number of tunnels going via the same physical interface. This issue is seen in Cisco IOS SREx and Cisco IOS 15.S based releases only.

  Workaround: There is no workaround.

- CSCuf64313

  Symptom: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

- CSCuf73798

  Symptom: Tracebacks are seen when Lc/Sp is comes up.

  ```
  May 15 10:14:22.145 IST: %MFIB_PLTF-SP-3-ENTRY_HANDLE_BAD: Space. 0x291E5D04 -Process=
  "mfib-const-lc Process", ipl= 0, pid= 303 -Traceback= 81D35D8z 8B13630z 8B0C434z
  8A86784z 8A3F588z 8A434A8z 8A65C64z 8A68ED0z 8A86EA8z 83ECFF0z 83E82D0
  ```

  Conditions: This symptom occurs in Cisco IOS Release 15.3(3)S.

  Workaround: There is no workaround.

  More Info: This issue was not reproducible. So a code walk-through and some safe checks and code strengthening was done to avoid such an error.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCug23348

  Symptom: The “mod” value in the SSRAM may be inconsistent to the number of ECMP paths.

  Conditions: This occurs with ECMP TE tunnels with **tunnel mpls traffic-eng load-share** *value* commands configured.

  Workaround: Remove the **tunnel mpls traffic-eng load-share** *value* commands from the TE tunnels.

- 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.

  Conditions: 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.

  Workaround: 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-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

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh40617

  Symptom: Ping fails when “encap dot1q” is configured on an FE SPA inserted in bay 1 of flexwan.

  Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

  Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh48840

  Symptom: A Cisco Router crashes.

  Conditions: This symptom is observed under the following conditions:

  a. sup-bootdisk formatted and copied with big size file, like copy 7600 image file around 180M size

  b. reload box, and during bootup try to write file to sup-bootdisk (SEA write sea_log.dat 32M bytes)

  c. then the issue appear

  – When the issue seen, check the sea_log.dat always with 0 byte

  – No matter where (disk0 or bootdisk) to load image.

– No matter sea log disk to sup-bootdisk or disk0:. I reproduced the issue with “logg sys disk disk0:” config.

SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.

```
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE8

Cisco IOS Release 12.2(33)SRE8 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE8 but may be open in previous Cisco IOS releases.

- CSCsx46323

  Symptoms: When a span monitor source or destination is a port-channel that is automatically created by a service module, the monitor configuration will be discarded on reloads. Also, for a redundant system, restarting the standby will cause the standby to continually reset, until the monitor session source/destination using the PO is removed.

  Conditions: This symptom occurs when the configuration is “monitor session x source interface port-channel yyy”, where yyy is the port-channel that is automatically created by the service module.

  Workaround: Remove the monitor session created on internal port-channels of service modules before any redundant SUP reset or reload. A full system reload will also cause the monitor session to be discarded and will therefore prevent a continual reload cycle of the standby.

- CSCtd87110

  Symptoms: IP session fails to sync as DHCP static bindings do not exist on Standby router.

  Conditions: This symptom is seen in HA setup.

  Workaround: There is no workaround.

- CSCtg39957

  Symptoms: Spurious memory access with MPLS-TE is enabled.

  Conditions: This symptom is seen when PATH message without any Session Attribute object is being received from TE head end. Note that Cisco IOS and XR routers always send the Session Attribute object, so this is only a potential issue with other vendors which do not do this (most do).

  Workaround: There is no workaround.

- 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

- CSCtg39957

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.

  This advisory is available at the following link:

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

  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

- CSCtk15775

  Symptoms: One or more prefixes are missing on line cards, switch processors and standby supervisor, compared to the active supervisor.

  Conditions: This symptom occurs after one of the following occurs:

  - switchover
  - standby supervisor reload
  - multiple line cards reloading

  Then a race may be hit such that one or more prefixes are not distributed to line cards, switch processors and the standby supervisor causing traffic to be misforwarded or not at all. The issue only affects prefixes downloaded at first priority, as listed in the "show cef table download priority" output.

  Workaround: The default behavior is for routes with recursive dependents and the default route are downloaded as first priority, so configuring "cef table download recursive-dependents priority 2" and "cef table download default- route priority 2" will cause such prefixes to be downloaded as second priority and the defect will not be hit. Configuring these commands may have a slight adverse effect on convergence performance.

  Alternatively, the CEF consistency checker can be used to detect prefixes missing on the line cards and switch processors and automatically repair the inconsistencies. This can be configured by the following:

cef table consistency-check IPv4 type scan-lc-rp
cef table consistency-check IPv4 type scan-rp-lc
cef table consistency-check IPv4 data-checking
cef table consistency-check IPv4 error-message

If the issue is hit, then the system state can be fixed by doing: **clear ip route ***

- CSCtk31340

  Symptoms: Cisco route processor (RP) crashes when a port-channel is removed and the member link is defaulted.

  Conditions: When a port-channel is removed (no int port-channel 200) and the member link is defaulted, the port-channel does not automatically remove the configurations on the member link. This crashes the route processor.

  Workaround: There is no workaround.

- CSCtk67455

  Symptoms: The fragmented traffic is dropped when the LOG option is set for IPv6 ACLs on 3CXL PFC-based supervisors.

  Conditions: This symptom is observed when the LOG keyword is specified for IPv6 ACLs on 3CXL PFC mode.

  Workaround: There is no workaround.

- CSCtl70143

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

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

  Workaround: There is no workaround.

- CSCtn41225

  Symptoms: The IPC port disappears and error messages are displayed on the Cisco CMTS. On the Cisco 7600 platform, it causes a crash.

  Conditions: This symptom is observed while doing a quit operation using the **show ipc util** command.

  Workaround: Do not use the **show ipc util** command.

- CSCtq09206

  Symptoms: Traffic flowing via MPLS TE tunnels gets blackholed after FRR-protected primary link flaps initiate an FRR cutover. CEF Backwalk failure messages may be observed on the SP/DFC console.

  Conditions: This symptom is observed with TE/FRR configuration with node protection.

  Workaround: There is no workaround.

- CSCtu42387

  Symptoms: Gigabit and 10 Gigabit Fiber link reporting threshold violation alarm in Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The "%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm" error message is seen on ports.

  Conditions: This symptom is observed on Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The messages are seen with the interface shut or no shut.

  ```
  SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value:
  -28.5 dBm, Threshold value: -24.0 dBm
  ```

Workaround: Fixing the fiber signal issue or disconnecting the fiber from the transceiver has been known to stop the messages.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCty07558

  Symptoms: DHCPv6 packets are dropped on a Cisco 7600 switch. For example, they are not flooded.

  Conditions: This symptom is observed when there is no IPv6 address on an SVI or if l2 VLAN has SVI in shut state (default existence after a new ACL feature).

  Workaround: Two possible workarounds which essentially serve as the fix due to the limitations they impose:

  1. When working with a pure L2 VLAN, remove ttl rate limiter (selected as default rate limiter on Cisco7600, but not on other boxes) using “no mls rate-limit all ttl-failure”.
  2. If the design permits and TTL rate limiter is necessary, put a dummy IPv6 address on the SVI or simply configure IPv6 enable on the SVI.

- CSCtz33778

  Symptoms: MDT remains in deleted state after several successive mdt removes/adds under the VRF.

  Conditions: The issue is seen when remove and add mdt is done quickly for multiple VRFs through a script.

  Workaround: Remove and re-add the VRF.

- CSCtz34869

  Symptoms: Aps-channel stops working.

  Conditions: This symptom occurs with an open ring and is seen in the following scenario:

  A1(po2)(RPL)<======>(po2)A3 (gig3/2)<=======>(gig3/3)A4

  Shut down gig3/2 on A3. Does not make A1 into protection.
  => Debugs show no SF packets are being transmitted to A1 which is connected to A3 via “Port-channel”
  => A1 (po2) is RPL of the ring. It is not going to unblocked even after A3-A4 link goes down.

  Workaround: Reload the line card.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

  ```
  %C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  %C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, the reported temperature will be far off from reading of other sensors on the line card.

  Workaround: There is no workaround.

- CSCtz68466

  Symptoms: Router crashes when the QoS policies are applied through radius server under multiple virtual-access interfaces, which are cloned from virtual-template configurations.

  Conditions: This symptom occurs when the router is using the following configurations:

  - Virtual-template settings
  - L2TP sessions
  - Radius server for the QoS policies

  Workaround: There is no workaround.

- CSCua25671

  Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

  Conditions: This symptom is observed under the following conditions:

  1. The router has a RSPAN source session.
  2. The source interface being added to the RSPAN source session is on ES+.
  3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
  4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

  Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

  Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25748

  Symptoms: The PW receive counter does not work.

  Conditions: This symptom is observed only with the ES+ card. This issue is not seen always due to timing events.

  Workaround: Flap VC again, and check if the counter works. If it does not work, reconfigure the VC.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, the mac-address table for IGMP snooping entries is not populated.

  Conditions: This can be seen on a Cisco 7600 series router that is running IOS where IGMP and PIM control packets come in on an SVI only after the condition where the SVI link state goes down and comes up again. This does not affect routed ports.

  Workaround: In the SVI configuration mode:

  1. Unconfigure PIM by using **no ip pim**.
  2. Unconfigure IGMP snooping by using **no ip igmp snooping**.
  3. Re-enable both PIM and IGMP snooping.

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller “mtu” or “ip mtu” configured.

```
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP
Notification sent
%BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0
(hold time expired) 0 bytes
%BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4
Unicast topology base removed from session  BGP Notification sent
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
%TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
```

  Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

  - If the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
  - Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCub23231

  Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known currently.

  Conditions: This symptom occurs when the ES20 interface has an EVC or MPLS configuration.

  Workaround: Reload LC.

- CSCub36356

  Symptoms: Scaling up routes result in huge memory allocations, eventually depleting the SP memory, leading to MALLOC FAIL and subsequent system crash.

  Conditions: This symptom occurs in normal conditions.

  Workaround: There is no workaround.

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

Conditions: The symptom is observed on the ES+ series line cards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

Workaround: There is no workaround.

- CSCub47520

  Symptoms: “Match dscp default” matches router initiated ARP packets.

  Conditions: This issue seen on Cisco 7600 ES+ line cards.

  Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub58312

  Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is seen when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: There is no workaround.

- CSCub60678

  Symptoms: Standby RSP is periodically reset after memory exhaustion. This can be checked by checking free memory on standby SP by the **show memory statistic** command.

  Conditions: This symptom is triggered by standby RSP restart or router reload.

  Workaround: There is no workaround.

- CSCub87579

  Symptoms: Multicast traffic gets forwarded to the wrong tunnel protected with IPsec.

  Conditions: This symptom is observed when Multicast (PIM) is enabled on the GRE tunnel protected with IPsec on the Cisco 7600.

  Workaround: Shut/no shut on the tunnel protected with IPsec resolves the issue.

- CSCub90038

  Symptoms: A 7600 series router may log IPC and ICC error messages.

  Conditions: The symptom is observed when multipoint GRE tunnels are configured in combination with a large number of VLANs. The continual buildup of IPC/ICC messages on the supervisor engine may cause TestMacNotification diagnostic failures for modules in the router.

  Workaround: Remove the GRE tunnel configuration or increase the GRE keepalive timers using the command **keepalive** *period retry* on the tunnel interface.

- CSCub91428

  Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

Workaround: There is no workaround.

- CSCub91546

  Symptoms: Traffic is dropped silently on the VLAN.

  Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

  Workaround: There is no workaround.

- CSCuc28757

  Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.

  Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.

  Workaround: There is no workaround.

- CSCuc41369

  Symptoms: Complete traffic loss occurs for V6 mroutes.

  Conditions: This symptom occurs during deletion and addition of VRFs for the MVPNv6 inband signaling configuration.

  Workaround: There is no workaround.

- CSCuc44306

  Symptoms: The IPv6 HbH packets get punted to RP as a result of HbH rate-limiter not working.

  Conditions: This symptom is observed when IPv6 HbH packets hit the bridged interface on SIP400/SIP200 with IPv6 HbH rate-limiter configured.

  Workaround: There is no workaround.

- CSCuc46356

  Symptoms: Router hangs and crashes by WDOG.

  Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.

  Workaround: Delete the ACL before deleting the port-ch sub-if.

- CSCuc48162

  Symptoms: EVC Xconnect UP MEP is sending CCMs when the remote EFP is shut.

  Conditions: This symptom occurs when EFP is admin down.

  Workaround: There is no workaround.

- CSCuc50482

  Symptoms: With P2P GRE PIM enabled tunnels in Cisco 7600, high CPU might occur in standby SP. It could happen mostly when the tunnel is configured under a MVPN.

  Conditions: This symptom may happen when running Cisco IOS Release 12.2(33) SRE7 and later releases.

  Workaround: Boot up the standby with tunnel shut and then enable it once the standby is up.

- CSCuc60245

  Symptoms: Pseudowires stop passing traffic until the LSP is reoptimized.

  Conditions: This symptom is observed when pseudowires stop passing traffic until the LSP is reoptimized.

  Workaround: The common fix is reoptimizing the LSP onto a new path in one or both directions.

- CSCuc72244

  Symptoms: On the Cisco 7600, both sides running Cisco IOS Release SRE4, Ethernet SPA configured with “negotiation Auto” and changed to “no negotiation auto”. The interface is operating in half-duplex instead of full-duplex mode.

  Conditions: This is a timing issue seen when configuring/un-configuring auto-negotiation or when doing continuous router reload.

  Recovery action: Configuring “shut” and “no shut” on the interface changes the duplex state to full-duplex.

  Workaround: There is no workaround.

- CSCuc85297

  Symptoms: If a Cisco 7600 router’s IOS image is upgraded using the ISSU procedure, the P2P tunnel interface multicast traffic might be affected.

  Conditions: This occurs with a SRE7-based release.

  Workaround: Perform a shut/no shut of the P2P tunnel interface.

- CSCuc96345

  Symptoms: ARP exchange between the Cisco 7600 and the client device fails. The Cisco 7600 has an incomplete ARP entry in its ARP table for the client. This issue is likely to be seen between the Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. The incoming ARP reply is parsed by the platform CEF as an IP packet and dropped.

  The following OUIs (as of October 30, 2012) are affected: (first 3 bytes from MAC address/MAC starts with)

  ```
  14-73-73
  20-73-55
  4C-73-67
  4C-73-A5
  54-73-98
  60-73-5C (One of Cisco's OUI ranges)
  64-73-E2
  70-73-CB
  8C-73-6E
  98-73-C4
  A0-73-32
  C4-73-1E
  D0-73-8E
  F0-73-AE
  F4-73-CA
  ```

  Conditions: This symptom is observed with the EVC pseudowire and 802.1q subinterface on the same physical interface, and connectivity via the subinterface is affected.

Sample configuration:

```
interface TenGigabitEthernet3/1
  service instance 2013 ethernet
    encapsulation dot1q 411 second-dot1q 200
    rewrite ingress tag pop 2 symmetric
    xconnect 10.254.10.10 3350075 encapsulation mpls
interface TenGigabitEthernet3/1.906
  encapsulation dot1Q 906
  ip address 10.10.10.1 255.255.255.0
```

Workaround:

- There should be a static ARP entry on the Cisco 7600 for the client's MAC and IP.
- Change the MAC address of client to a nonaffected OUI.

Note: This ddts is caused/exposed due to fix of CSCtc22745.

- CSCuc97711

  Symptoms: After SSO, traffic on the P2P-GRE tunnel within an MVPN may be affected.

  Conditions: This symptom is observed with Cisco IOS Release SREx- and RLSx-based releases.

  Workaround: Shut/no shut the P2P tunnel interface.

- CSCud13862

  Symptoms: The Cisco WS-SUP720 running Cisco IOS Release 12.2(33)SRE3 crashes.

  Conditions: This symptom occurs during a CPU process history update.

  Workaround: The issue can be avoided by removing the configuration statement for "CPU Utilization Statistics".

  conf t no process cpu statistics limit

- CSCud19230

  Symptoms: ES+ line card reload occurs with the following error messages:

```
%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus
Error Add:332 Bus Err
data: 0

%OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset
due to exception or
user request)

%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due
to exception or user
request)
```

  Conditions: This symptom is observed with the ES+ line card.

  Workaround: There is no workaround.

- CSCud27379

  Symptoms: WS-SUP720-3B running Cisco IOS Release 12.2(33)SRE4 crashes at get_alt_mod after issuing “sh run int g4/13” with several trailing white spaces until the cursor stops moving.

  Conditions: This symptom occurs when you issue the **show run interface** command with trailing spaces until the cursor stops moving.

  Workaround: Do not specify trailing spaces at the end of the **show run interface** command.

- CSCud28759

  Symptoms: SPA crash is seen when invoking spa_choc_dsx_cleanup_atlas_ci_config with no data packed.

  Conditions: This symptom is observed when the packed data size should be 1 and the status should be success.

  Workaround: There is no workaround.

- CSCud71211

  Symptoms: The **mpls traffic-eng reoptimize timers delay cleanup** command does not take effect in the path protection. When path protection kicks in and “mpls traffic-eng reoptimize timers delay installation” expires, the new best LSP is installed, but the protection path is torn down at the same time. This can cause a few seconds of packet drops, which are being carried over the protection LSP.

  Conditions: This symptom occurs when the path protection switchover is triggered on the protected tunnel.

  Workaround: There is no workaround.

- CSCud90950

  Symptoms: Multicast traffic might not flow through when the P2P tunnel is the incoming interface in the Cisco 7600 router.

  Conditions: This symptom occurs in the Cisco IOS Release 12.2SREx and Cisco IOS Release 15.0x.

  Workaround: Shut and no shut of the P2P tunnel interface.

- CSCue01579

  Symptoms: Receivers on slot10 - 13 of the Cisco 7613 chassis cannot receive multicast traffic when the egress replication mode is used.

  Conditions: This symptom occurs on RSP720-10G + CISCO7613 chassis and when using the egress replication mode.

  Workaround: Change the replication mode to ingress by using the below given CLI:

  mls ip multicast replication-mode ingress

- CSCue03598

  Symptoms: Carrier-delay does not work on an ES+ card under the following specific condition:

  Carrier-delay configured on gig 4/13 does not work on an ES+ card when we sh down gig0/1 on peer Cisco 3560 in the below given situation:

  gig4/3[no sh] gig0/1[no sh]

  7600 ========== 3560

  gig4/13[sh] gig0/2[no sh]

  1. do [no sh] on gig 4/13

2. do [sh] on gig0/1 right after 1

gig4/1 will go up as soon as gig 4/3 gets down instead of waiting till the configured carrier-delay timer expires.

Conditions: This symptom occurs when we enter show on the peer device.

Workaround: There is no workaround.

- CSCue32450

  Symptoms: Filtering based on L4 ports does not happen for redirection to CE.

  Conditions: This symptom occurs when the WCCP service uses a redirect-list and this ACL has its first entry as a “deny”.

  Workaround: Make the first entry in the redirect-list ACL as a “permit”.

- CSCue61286

  Symptoms: RSA keys fail to replicate.

  Conditions: This issue is specific to adventerprisek9 image and is seen in the following condition:

  1. In HA setup, if router has RSA configuration and Active supervisor goes down, then RSA keys are not getting replicated on Standby Supervisor.
  2. During ISSU upgrade, upgrade will fail because of failure of RSA key replication.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SRE7a

Cisco IOS Release 12.2(33)SRE7a is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are open in Cisco IOS Release 12.2(33)SRE7a. This section describes only select open caveats.

- CSCuc85297

  Symptoms: If a Cisco 7600 router’s IOS image is upgraded using the ISSU procedure, the P2P tunnel interface multicast traffic might be affected.

  Conditions: This occurs with a SRE7-based release.

  Workaround: Perform a shut/no shut of the P2P tunnel interface.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE7a

Cisco IOS Release 12.2(33)SRE7a is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE7a but may be open in previous Cisco IOS releases.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

  ```
  %C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold #1(=60C).
  It has exceeded normal operating temperature range.
  %C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
  #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: The symptom is observed on ES+ series linecards of Cisco 7600 series routers. Specifically, the reported temperature will be far off from reading of other sensors on the linecard.

Workaround: There is no workaround.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, the mac-address table for IGMP snooping entries is not populated.

  Conditions: This can be seen on a Cisco 7600 series router that is running IOS where IGMP and PIM control packets come in on an SVI only after the condition where the SVI link state goes down and comes up again. This does not affect routed ports.

  Workaround: In the SVI configuration mode:

  1. Unconfigure PIM by using **no ip pim**.
  2. Unconfigure IGMP snooping by using **no ip igmp snooping**.
  3. Re-enable both PIM and IGMP snooping.

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCub74451

  Symptoms: EARL inlet/outlet displays incorrect temperature values. If the temperature crosses the minor/major threshold false alarms will be generated. In case of a major alarm the linecard will shut down as a preventive measure.

  Conditions: There is no trigger for the issue.

  Workaround: Reload the linecard.

- CSCub90038

  Symptoms: A 7600 series router may log IPC and ICC error messages.

  Conditions: The symptom is observed when multipoint GRE tunnels are configured in combination with a large number of VLANs. The continual buildup of IPC/ICC messages on the supervisor engine may cause TestMacNotification diagnostic failures for modules in the router.

  Workaround: Remove the GRE tunnel configuration or increase the GRE keepalive timers using the command **keepalive** *period retry* on the tunnel interface.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE7

Cisco IOS Release 12.2(33)SRE7 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE7 but may be open in previous Cisco IOS releases.

- CSCtb30811

  Symptoms: The aggregate route is not removed in certain scenarios.

  Conditions: This symptom is observed when all aggregated child routes are marked for deletion and the periodic function (which processes these routes to be deleted) gets to remove the route from routing table before the aggregate processing function gets a chance to process the aggregate route to which they belong. That is, the aggregate routes remain in the routing table although the child routes get deleted.

Workaround: Configuring “bgp aggregate-timer” to 0, which is the lowest value, would reduce the chances of hitting this problem considerably.

In case this issue occurs, then in order to delete the stale aggregate route, you need to configure a temporary local BGP route (say, redistribute a static route or network a loopback) with the 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 the table and also send withdrawals to other routers.

Further Problem Description: The periodic function is by default called at a 60-second interval. 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 1 second from when the tie routes are marked for deletion, and hence the chances of hitting this problem is very minimal. 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 the command. By default, this maximum value is 30 seconds and is configurable with a range of 6-60 seconds. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- CSCtc73759

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

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

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

- CSCtf71636

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

  Conditions: This 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.

- CSCth35873

  Symptoms: The Subject Alternative Name (SAN) is incorrect in persistent self-signed certificates.

  Conditions: This symptom occurs in persistent self-signed certificates. The SAN is displayed as DNS:secp6-11.cisco.com, but it is supposed to be DNS:zzztmp.cisco.com

  Workaround: There is no workaround.

- CSCth96200

  Symptoms: A continuous traceback is seen:

  ```
  *Nov 30 00:10:11.795: %FRR_OCE-STBY-3-GENERAL: un-matched frr_cutover_cnt.
  -Traceback= 7021958 70217D4 7021A34 7034130 4686294 4671348 4A2E548 4682AA4
  4683524 4F69DA4 4F63664
  ```

  Conditions: This symptom occurs when the FRR feature is configured and possibly under scale conditions.

  Workaround: There is no workaround.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCto04463

  Symptoms: A device crashes upon rebooting the routers with BGP PIC configurations for IPv6 networks. The crash is seen in both SRE code and 15.1 code.

  Conditions: This symptom is observed mainly with the code-affected handles. This issue is seen with the following conditions:

  1. Some error conditions by adding defensive code.
  2. Proper extraction of adjacency subblock in BGP PIC cases.

  Workaround: There is no workaround.

- CSCtq24526

  Symptoms: A memory corruption crash is seen on a device running crypto.

  Conditions: This symptom occurs on a device running crypto.

  Workaround: There is no workaround.

- CSCtq77973

  Symptoms: An ATM interface is created on a CEoP SPA, followed by range-pvc configurations on it. Later, when trying to delete and recreate the interface, the configuration fails with the below message.

  ```
  *Jun  7 07:07:11.103 EST: %CEMA-3-INTERFACE_CONFIG_FAIL: ATM2/1/0.2/1/1:
  interface configuration failed (unsupported)
  *Jun  7 07:07:11.111 EST: %CEMA-3-INTERFACE_DELETE_FAIL: ATM2/1/0.2/1/1:
  interface delete failed (unspecified error)
  SLOT 2: *Jun  7 07:07:11.095 EST: %CEMA-3-INTERFACE_CONFIG_FAIL:
  ATM2/1/0.2/1/1: interface configuration failed (unsupported)
  SLOT 2: *Jun  7 07:07:11.099 EST: %SPA_PLIM-3-ERRMSG: SPA-1CHOC3-CE-ATM[2/1]
  (CEOP-3-UNSUPPORTED: modify UNI/NNI (cema_atm_header_mode_t))
  ```

  Conditions: This symptom is not seen easily and seems to be related to the timing of events.

  Workaround: Reload the SPA.

- CSCtr20762

  Symptoms: L3VPN tunnel is not coming up after the router is reloaded.

  Conditions: This symptom is observed with “aaa system accounting” configured and when the TACACS server is not reachable.

  Workaround 1: Disable “aaa system accounting”.

  Workaround 2: Ensure that the TACACS server is reachable.

- CSCtr27674

  Symptoms: A SIP-200 linecard crashes.

  Conditions: This symptom is observed with a POS SPA on SIP-200 line card after performing an ISSU upgrade on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCtr44384

  Symptoms: Spurious memory access will be seen while deleting a subinterface with two VLAN tags.

  Conditions: This symptom is observed only when a subinterface has a policy with two VLAN tags.

  Workaround: There is no workaround.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts20857

  Symptoms: This issue is actually a fix for CSCtj96916, which is the original issue

  Conditions: This symptom occurs when changing the card type from T3 to E3.

  Workaround: There is no workaround.

- CSCts69115

  Symptoms: Remote router (PE2) crash is seen after 500 shut/no shut of UUT primary paths.

  Conditions: This symptom occurs after shut/no shut (500 times) of primary paths on UUT (PE1). The router is in hung state, and after rebooting, the crash file is not generated. From the logs, it is seen that the number of siblings in a chunk has gone above the threshold.

  Workaround: Reload the router.

- CSCts81427

  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.

  Conditions: This symptom is observed after doing SSO.

  Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

- CSCts84700

  Symptoms: The incoming VRF stream over the MDT data tunnel is vanishing.

  Conditions: This symptom occurs when deleting and recreating the VRF.

  Workaround: Introduce a delay of 6 minutes between the deletion and the recreation of the VRF.

- CSCtt99627

  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.

  Conditions: This symptom affects the Cisco 7600 platform.

  Before performing a switchover, one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP then they will disappear if a switchover occurs.

  Workaround: Prior to switchover, if the commands do not show up on the standby RP, as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.

  Otherwise, if the commands disappear after a switchover, then the commands must be reconfigured on the newly active RP.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA-4T/8T) becomes inactive after PA OIR.

  Conditions: This symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtu90140

  Symptoms: A chunk memory leak is observed.

  Conditions: A chunk memory leak is seen after configuring the IP source guard.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: This symptom is observed with PPP negotiations and the session involving PPPoA.

  Workaround: Ensure that all your PPP connections stay stable.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This symptom occurs in the Cisco 7600 router with a 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw55401

  Symptoms: The SPA-1XCHSTM1/OC3 card goes to out of service after SSO followed by OIR.

  Conditions: This symptom is observed with the SPA-1XCHSTM1/OC3 card with Cisco 7600-SIP-200 combination.

  Workaround: There is no workaround.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: “no shut” the interface in the QMOVESTUCK error message, remove QoS policies on the interface and subinterfaces, and remove the interface from T1/T3 controller. Then, rebuild the configuration.

- CSCtw88599

  Symptoms: If “port acl” is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: This symptom is observed when you configure “port acl” on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

  This issue will effect only if there is a switchport configured on the router. The issue will not affect the traffic or the filtering based on the ACL, even if the testAclDeny fails and the card is on MajFail (due to this test only).

  As a workaround, we can remove the switchport configurations for the ports (if they exist), then reload and apply the configurations after the router has come up. Alternatively, do a “no diagn crash” and try to bring up the router.

  In case the router reloads, the ports will not go into shutdown state. Hence, it is a cosmetic issue. It can be ignored. If reloaded in presence of the switchport configurations, it should come up after two reloads into a minor error state.

- CSCtx23014

  Symptoms: HSRP hellos cannot be sourced from certain IPs.

  Conditions: This symptom is observed when HSRP hellos cannot be sourced for an IP address with a standby IP address in the same subnet and both are configured in the global VRF. For example:

```
Router(config)#interface Ethernet0/0
Router(config-if)# ip address 192.168.68.13 255.255.252.0
Router(config-if)# standby 68 ip 192.168.70.1
Router(config-if)# standby 68 priority 120
Router(config-if)# standby 68 preempt
Router(config-if)# arp timeout 300
```

  Workaround: Use an IP from the subnet for the SVI interface in the same VRF.

- CSCtx23593

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwal** command, but not in the router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in the customer network. This issue may also occur in other releases.

  This issue typically occurs over a period of time due to create/delete of subinterfaces. It also occurs if the customer uses the **snmp ifmib ifIndex Persist** command, which retains ifIndicies assigned to the @~@subinterfaces across router reload.

  Workaround: There can be two workarounds where there is no fix present in the Cisco IOS code for this bug.

  Workaround 1:

  - Enter the show atm vc privileged EXEC command on the same device to obtain a complete list of all the VCs. Or,
  - Do the SNMPWALK suffixing the ifIndex of the interface to get the value.

```
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.2.1.2.2.1.2 | grep
"4/0.120"
IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif
```

```
IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer

$  snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3 |
grep 9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete
snmpwalk
$
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
```

Doing the SNMPWALK suffixing the ifindex and getting the value can be one workaround.

```
SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041
```

Workaround 2:

1. Under configuration mode: no snmp ifmib ifIndex Persist.
2. On all the ATM main interfaces: no snmp ifindex persist.
3. Save the configuration: copy running start.
4. Reload the box: reload. Reapply the persist configurations.
5. Configure in configuration mode: snmp ifmib ifIndex Persist.
6. Under the ATM main interface: snmp ifindex persist.

After this workaround, the problem may reappear over a period of time, but chances are very less.

The workaround/fix which needs to be enabled where the code fix is present in the Cisco IOS code for this bug.

Since this will go over all the possible ifIndicies, it will take more CPU cycles, causing some delay. The below global CLI can be used to enable/disable the fix based on the need.

CLI: snmp-server enable traps atm snmp-walk-serial

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)S1, with ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  ```
  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0
  0 0x5fa
  ```

- CSCtx48473

  Symptoms: A router crashes when the following command is executed:

  ```
  sh platform software xconnect circuit-index interface <tunnel-name> | i <VC-number>
  ```

  No crashinfo is generated on the RP and SP. Please see the attached console before the crash.

  Conditions: The above command must be executed.

Workaround: There is no workaround.

- CSCtx57154

  Symptoms: RP crashes and brings down the router.

  Conditions: This symptom is observed upon shut/no shut of an ES+ access interface configured with 5K EVC.

  Workaround: There is no workaround.

- CSCtx62138

  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.

  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.

  Workaround: There is no workaround.

- CSCtx77501

  Symptoms: Traffic is dropped at the decap side of a PE box.

  Conditions: This symptom occurs with SSO at the decap side of an MVPN setup, with DFC core-facing and 6748 access facing.

  Workaround: Do a switchover.

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx85247

  Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.

  Conditions: This symptom is seen with redundancy switchover of RSPs.

  Workaround: There is no workaround.

- CSCty12312

  Symptoms: Multilink member links move to an up/down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty13647

  Symptoms: Symptoms vary from one image to another. The following symptoms have been mostly observed:

  1. Spurious memory access tracebacks from SPAN code even when SPAN is not configured.
  2. RP crash when unconfiguring a SPAN session with a particular session number.

  Conditions: This symptom is always seen on a particular SPAN session number.

Workaround: Use a different a SPAN session number for SPAN configurations to avoid the router crash. Shutdown the SPAN session if not in use. There is no workaround to avoid spurious memory access messages.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, and **ip mfib** output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: This symptom is observed with a Cisco 7600 running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.

  Conditions: This symptom is observed when the interface is configured with a VRF.

  Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router’s GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty37396

  Symptoms: The remote PE sees label 442.

```
====================
DXB-BSH-OR-C6509-1#show mpls for 2001:6E8:1C0::/42
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       442        2001:6E8:1C0::/42   \
                                       0             Te1/1      10.162.111.25
DXB-BSH-OR-C6509-1#
```

  However, this label is punted and passed on to the rate limiter as it is with destination index 0x7FFF, and packet drops are seen.

```
F340.11.12-7600-1A#show mls cef mpls label 442 det

Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
       D - FIB Don't short-cut, m - mod-num, E - ELSP?
Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2 eos2)
V(3187   ): B | 1 0    0 0 0 442     0 1 0 0       0 0 (A:24     ,P:0,D:0,m:0 :E:1)
M(3187   ): F | 1 FFF  0 0 1 FFFFF   0 1 0 0       0 0
F340.11.12-7600-1A#show mls cef ad entry 24 det

Index: 24      smac: 0000.0000.0000, dmac: 0000.0000.0000
               mtu: 9234, vlan: 0, dindex: 0x7FFF, l3rw_vld: 1
               format: MPLS, flags: 0x20000690600 (mpls_drop)
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 0, exp: 0, ovr: 0
               op: PUSH_LABEL2
               packets: 0, bytes: 0
```

  Conditions: This symptom occurs in a 6PE setup and when the IPV6 address is aggregated.

Workaround: Do not use the aggregate address.

- CSCty51172

  Symptoms: The MAC address learned on L2 DEC on 7600-ES+40G3CXL is not installed as the primary entry on all the member interfaces, if the ingress traffic is on the nonhashed interface for that EFP.

  Conditions: This symptom occurs when Layer 2 distributed Etherchannel traffic is learned on a hashed interface first and then moved to a nonhashed interface.

  Workaround: Do not use Layer 2 distributed Etherchannel.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the FlexWAN line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

  Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300 seconds.

  ```
  mpls traffic-eng reoptimize timers delay cleanup 300
  ```

- CSCtz28024

  Symptoms: On a TE tunnel midpoint, the incoming label shown as allocated for the LSP by the TE does not match the label allocated for the LSP in the forwarding. Packets going over the TE tunnel are dropped.

Conditions: This symptom can occur when the midpoint router receives multiple RSVP RESV messages for the same LSP and requests TE to admit the reservation. This could be due to receiving duplicate RSVP RESV messages within a very short duration or if the downstream neighbor should change certain session attributes for the RSVP RESV message. Changes to the RSVP RESV message are not a normal occurrence and this issue is not easily reproducible.

In the case observed, the downstream router was modifying the Record Route Object (RRO) unexpectedly. However, changes in the RESV outgoing label or next-hop would also trigger the problem. In the case where the issue was observed, the downstream next-hop router was a CRS running Cisco IOS XR. The conditions in which this problem was observed were during a reload of the tailend router and multiple manually triggered TE reoptimizations throughout the network. It is not known what caused the CRS to send RSVP RESV change to RRO.

Should the midpoint router process a change to an existing RSVP RESV message, TE will not handle reprogramming the forwarding properly and arrive at the problem. This problem exists in Cisco IOS Release 12.2SRE and later releases.

Workaround: Shut and no shut the tunnel.

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the **show hw-module slot X tech-support** or **show platform hardware version** command. This is similar to CSCti78408 but not to CSCti78408.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the **show hw-module slot X tech-support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

  Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz35040

  Symptoms: The router crashes when “clear up route *” is issued.

  Conditions: This symptom is observed when a router is operating few thousand BGP/IGP routes and “clear ip route *” is issued.

  Workaround: There is no workaround.

- CSCtz46399

  Symptoms: VLAN RAM is not programmed with the correct VPN number for a few VRFs.

```
Eagle2-es20-dfc4#sh mls vlan-ram 1182 1182
TYCHO Vlan RAM
Key: * => Set, - => Clear

vlan   eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro
rpf-pbr-ovr
-------+-----+-------+-----+-----------+------+-----+---+-----------+----------+------
----+-----------
1182    -      -       *         0        0       -     -       0          0
        -         *
```

  Conditions: This symptom is observed with the OIR of the ES-20 line card with scaled MVPNv6 configuration and 50 VRFs configured.

  Workaround: There is no workaround.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear, along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: When service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default-class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCua09073

  Symptoms: If 6708 generates txCRC errors, CSCtq73026 accounts for these errors in TestErrorMonitor diagostic test and takes the necessary recovery action. But, for CSCtq73026 to be invoked, the TestErrorMonitor test should be included in the test suite for 6708. This test is missing and hence, the fix in CSCtq73026 will also not be invoked.

  Conditions: See the description of CSCtq73026. For this fix to be take effect, TestErrorMonitor should be added in the test suite. In this DDTS, this test has been added so that in case of an error, as mentioned in CSCtq73026, recovery action will be triggered.

  Workaround: There is no workaround.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4-hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua18382

  Symptoms: There are locally originated packets larger than 1476 bytes and are going through the IPsec tunnel with GRE.

Conditions: This symptom occurs when the Cisco 7600 router has encryption processing on the c7600-spa-ipsec-2g and is configured with the **crypto engine gre vpnblade** command. However, only locally originated traffic to CPE is prone to not break through traffic via the tunnel.

Workaround: Configure “crypto engine gre supervisor” instead of the VPN blade under the tunnel interface. However, this can be useful only if there is one tunnel. If there is more than one tunnel, the crypto would be offloaded to the VPN blade irrespective of the configuration.

- CSCua25943

  Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

  Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua41398

  Symptoms: The Cisco SUP720 crashes.

  Conditions: This symptom occurs when you issue the **sh clns interface | i ^[A-Z] | Number of active** command multiple times via script with the following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

  Workaround: There is no workaround.

- CSCua42089

  Symptoms: Configuring Ingress redirection for service group 61 (Mask) and applying an extended ACL in the outbound direction on the same interface causes software switching even when there are no punt entries in the TCAM.

  Conditions: This symptom is observed when WCCP service 61 with Mask assignment in the Ingress indirection, along with an outbound ACL, is configured on the same interface.

  Workaround: Do not configure the outbound ACL along with a WCCP service.

- CSCua57728

  Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

Conditions: This symptom is observed with four core-facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

Workaround: There is no workaround.

- CSCua67532

  Symptoms: IPsec sessions fail to come up.

  Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

  Workaround: There is no workaround.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCub21468

  Symptoms: UDP header is corrupted randomly.

  Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

  Workaround: There is no workaround.

- CSCub31902

  Symptoms: Alignment correction tracebacks are seen from within the diag_dump_lc_l2_table() cosmetic issue, which create temporary memory inconsistencies in the function.

  Conditions: This symptom occurs in normal conditions, during bootup time, provided testMacNotification fails.

  Workaround: Disable bootup diagnostics or disable the testMacNotification health monitoring test.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via “neighbor default-originate” to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

  Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

  Workaround: Remove and readd the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCtw76855

  Symptoms: IPC times out, and hence disconnects on line cards, resulting in MFIB table resync.

Conditions: This symptom is observed when IPC times out.

Workaround: This fix is an enhancement to avoid such unnecessary table disconnects due to IPC timeouts.

- CSCub67101

  Symptoms: The POS interface line protocol is down with encapsulation PPP in an MPLS setup.

  Conditions: This symptom occurs when configuring encapsulation PPP on both ends of PE1 and CE1, and then configuring xconnect in the customer-facing interface of PE1.

  Workaround: Reconfigure the xconnect settings. Then, the interface will come up in the proper state.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE6

Cisco IOS Release 12.2(33)SRE6 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE6 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsd98525

  Symptoms: An SSH version 2 (SSHv2) session is terminated prematurely.

  Conditions: This symptom is observed when large chunks of data are transferred in the SSHv2 session, for example, when the **show tech** command is entered and the command output is transferred in the SSHv2 session.

  Workaround: Use SSH version 1.

- CSCsf17406

  Symptoms: A memory leak is seen.

  Conditions: The symptom is observed when a Cisco router performing crypto certificate revocation checks downloads a Certificate Revocation List (CRL). It is seen in the “Crypto PKI-CRL” process when the CRL is larger than roughly 70 kbs in size.

  Workaround: Reduce the CRL size or disable the CRL revocation check.

  Further Problem Description: Cisco IOS Release 12.3(11)T and earlier releases (including Cisco IOS Release 12.3/12.2, etc.) are not affected by this issue.

- CSCta27728

  Symptoms: A Cisco router may crash.

Conditions: This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.

Workaround: There is no workaround.

- CSCte53162

  Symptoms: In radius messaging, nas-port-id is not prepended to “acct-session- id” when the **nas-port format e** *encoding string* command is configured.

  Conditions: This symptom is observed when the **nas-port format e** *encoding string* command is configured.

  Workaround: Use the **nas-port format d** *encoding bits* command.

- 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

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- CSCth10764

  Symptoms: PPP Negotiation not working correctly between Cisco GSR XR and Cisco 7200.

  Conditions: Max-header size different on both ends, PPP not negotiating lower size.

  Workaround: There is no workaround.

- CSCth84995

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

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

  Workaround 1: Reload the router.

  Workaround 2: Upgrade from Cisco IOS Release 12.2(33)SRD4 to 12.2(33)SRD5 first and then from 12.2(33)SRD5 to 12.2(33)SRE6.

- CSCti81539

  Symptoms: Some of the ACLs related to TCP cannot be removed from a router.

  Conditions: This symptom is observed while unconfiguring ACLs.

  Workaround: Remove the entire ACL, and recreate it again.

- CSCtj84234

  Symptoms: With multiple next-hops configured in the set ip next-hop clause of route-map, when the attached interface of the first next-hop is down, packets are not switched by PBR using the second next-hop.

  Conditions: This symptom is seen only for packets switched in software and not in platforms where packets are PBR'd in hardware. This symptom is observed with route-map configuration, as given below:

  ```
  route-map <RM name>
   match ip address <acl>
   set ip next-hop <NH1> <NH2>
  ```

  Workaround: There is no workaround.

- CSCtk03371

  Symptoms: SVI-based EoMPLS/VPLS VC fails to forward traffic even when VC is up.

  Conditions: This happens when the **ip cef accounting non-recursive** command is configured on the router. This command is documented as an unsupported command on the Cisco 7600 platform, but it should also generate an error message when configured on the Cisco 7600. Preferably it should not take any action, for example, it should not affect any other working features.

  Workaround: Unconfigure the command by typing "no ip cef accounting non- recursive".

- CSCtk46363

  Symptom: A device running Cisco IOS and acting as a DHCP server crashes.

  Conditions: This symptom is observed when a client requests a specific IP address.

  Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- 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.

- CSCtl86141

  Symptoms: Data traffic is switched over BPDU PW. This issue can result in MAC-FLAPs over the multiple MST rings configured to be part of MST 0 instances (configured along with RL2GP) as BPDU PW acts as a loop in the network connectivity for those MST rings.

  Conditions: This symptom is observed when data traffic is received on the access VLAN on which BPDU PW is configured.

  Workaround: There is no workaround. This issue is not expected to be seen on the customer VLAN as data traffic is not expected over the native VLAN.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```
  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn22523

  Symptoms: IPSLA udp-jitter probes may crash at saaAddSeqnoDupQ in Cisco IOS Release 12.4T/15.0M. There is no impact to other releases.

  Conditions: This symptom is observed when the network experiences delay, and reordered and duplicate packets can trigger this problem when IPSLA udp-jitter is scheduled.

  Workaround: Disable udp-jitter probes.

- 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.

- CSCto13462

  Symptoms: A Cisco router may reload when it is acting as a DHCP server.

  Conditions: The symptom is observed when there are two DHCP clients using the same client ID. The reload is triggered when the second client releases its DHCP address.

  Workaround: There is no workaround.

- CSCto71004

  Symptoms: Router crashes with high scale and a lot of BGP routes and scaled MPLS L3 VPNs enabled. This crash is seen in the router when core links flap.

  Conditions: The symptom is seen when a scaled router with a lot of BGP routes crashes when some of the core links flap. Setup has scaled MPLS L3 VPNs enabled.

  The following messages are seen:

  ```
  %COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
  10.173.30.125/32 is found to resolve via itself during setting up switching info
  %COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
  10.173.19.16/30 is found to resolve via itself during setting up switching info
  %COMMON_FIB-SP-6-FIB_RECURSION_VIA_SELF:
  10.173.19.17/32 is found to resolve via itself during setting up switching info
  ```

  Workaround: There is no workaround.

- 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.

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. If a particular path is threaded to be sent - in this case it is scheduled for a reply message - the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packtization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- 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.

- CSCtr34960

  Symptoms: A router that is running Cisco IOS may run out of IO memory.

  The **show buffers** command shows that the count reaches 0 in free list.

```
Router#sh buffers
...
Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)
EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

  Conditions: This issue is seen post bootup. The Cisco 7600 in HA is required to hit the issue. The **show buffers old** command shows some buffers hanging on EOBC buffers list for a long time, weeks or more. The issue is a corner case, and buffer leak rate is slow.

  This DDTS fixes leaks for the **mls cef maximum-routes** and **mls cef adjacency-mcast** commands.

  See the output from the **show buffers old pack**:

```
F340.08.04-6500-2-dfc1#show buf old packet

Buffer information for EOBC0/0 buffer at 0x275A0B00
  data_area 0x275A0FB8, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:36.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A100C, datagramsize 50, maximum size 1680
  mac_start 0x275A0FFE, addr_start 0x275A0FFE, info_start 0x0
  network_start 0x275A100C, transport_start 0x0, caller_pc 0x205DF718

275A100C: 00200000 02010000 00010006 01000000  . ..............
275A101C: 00350001 00101608 00000053 000000A6  .5.........S...&
275A102C: 000603E7 01170000 00000000 00000000  ...g............
          --------
275A103C: 000000                               ...

Buffer information for EOBC0/0 buffer at 0x275A5B48
  data_area 0x275A6000, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:41.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A6054, datagramsize 80, maximum size 1680
  mac_start 0x275A6046, addr_start 0x275A6046, info_start 0x0
  network_start 0x275A6054, transport_start 0x0, caller_pc 0x205DF718


275A6054:          00200000 02010000 02150007      . ..........
275A6060: 01000000 000A0001 00301608 00000052  .........0.....R
275A6070: 000000A4 00480002 01047FFF 00000001  ...$.H..........
                   --------
275A6080: 00000000 00000000 00000000 00000000  ................
275A6090: 00000001 00000000 00000000 00000000  ................
275A60A0: 00000000 00

F340.08.04-6500-2-dfc1#
```

  The **show buffers old packet** command output will be either 000603E7 OR 00480002.

Workaround: Reload the supervisor to clear the leaked buffers.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  – An internal service module session for a FWSM or other service modules exists:

```
UUT#show monitor session all Session 1 Type : Service Module Session
```

  – If you attempt to configure a span session with the session number already in use:

```
UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40 % Session 1 used by
service module
```

  – The command seems to be rejected, but it is synchronized to the standby supervisor.

  – A switchover happens.

  Workaround: There is no workaround.

- CSCtr51926

  Symptoms: IPv6 packets are not classified properly in a subinterface when a service-policy is applied on the main interface.

  Conditions: The symptom is observed when a service-policy is applied on the main interface.

  Workaround 1: Enable IPv6 explicitly on the main interface:

```
interface x/y ipv6 enable
```

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

```
interface x/y.z no ipv6 address ipv6 address ...
```

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

  Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: crashes at BGP Task without a BGP configuration change or BGP neighbor up/down event.

```
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
Traceback summary % 0x80e7b6 : __be_bgp_tx_walker_process % 0x80e3bc :
__be_bgp_tx_generate_updates_task % 0x7f8891 : __be_bgp_task_scheduler
```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

  Conditions: The symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

Workaround for symptom 1: Remove “import-route target” and reconfigure route-target.

Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- 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

- CSCtr92285

  Symptoms: The following log is seen, and VCs cannot be configured.

  ```
  SSM CM: SSM switch id 0 [0x0] allocated ACLIB [Gi9/1/0.3830, 3830]: Failed to setup
  switching for VLAN interface ...
  ```

  Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.

  Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

- CSCts06929

  Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

  Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

  Workaround: Configuring graceful restart resolves this issue.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

Workaround: There is no workaround.

- CSCts32920

  Symptoms: Traffic gets punted to the RP.

  Conditions: This symptom occurs when there are multiple P2P-GRE tunnels in a particular VRF. Remove one particular P2P-GRE tunnel from that VRF.

  Workaround: Shut/no shut P2P-GRE tunnels in that particular VRF, for which traffic is getting punted to the RP.

- CSCts38429

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

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

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

- CSCts41217

  Symptoms: Memory leak occurs in const_mfib_lc_* processes.

  Conditions: This symptom is observed during deletion and addition of VRFs. Multicast needs to be enabled in the VRF and the P2P tunnels should be present in the VRF. VRF should be removed before deleting the P2P tunnels for this to happen.

  Workaround: Delete all the P2P tunnels before removing the VRF

- CSCts47566

  Symptoms: During standby RP bootup, an incorrect ICMP punt entry for MPLS interfaces gets programmed. This entry appears even if the interface has no ACL applied in the input/output direction.

```
2037#show tcam inter gi4/0/3 acl in ip

* Global Defaults shared
Entries from Bank 0
punt         icmp any any eq 11 <<<<<<<<<<<<<<<<
    permit       ip any any (1895 matches)
Entries from Bank 1
```

  Conditions: This symptom is observed with the ICMP punt entry, which is required to allow trace route across MPLS cloud. This is a workaround for a hardware problem with Tycho. The feature is called “FM_FEATURE_MPLS_ICMP_BRIDGE”. This workaround is required only if there are aggregate labels programmed in the superman VPN cam, but can get set incorrectly even when there is no VRF configuration on the box.

  Workaround: To clear the entry set unnecessarily, disable/enable MPLS on the interface for which it appears.

- CSCts58394

  Symptoms: The SNMP graph traffic rate (collected from the port-channel subinterface) does not match the 5-minute offered rate from “show policy-map inter port-channel x.x”.

  Conditions: This symptom occurs on the Cisco 7600-S running Cisco IOS Release 15.0(1)S4 with the port-channel subinterface on 76-ES+XC-40G3CXL. This issue is seen only when there is EARL recirculation of packets and affects only the ingress traffic rate.

  Workaround: There is no workaround.

- CSCts59014

  Symptoms: Only one ATM VC shaper token is updated per cycle in a high-scale scenario.

  Conditions: This symptom is observed with HQOS on ATM VC with many ATM VCs per interface.

  Workaround: There is no workaround.

- CSCts88467

  Symptoms: Drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue, then remove and reapply the policy. Configuring queue-limit in parent policy automatically triggers calculation based on the parent queue-limit value on the child queue-limits based on bandwidth allocated to various classes.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code was integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt03485

  Symptoms: ES40: IDBMAN crash is seen with “no ip flow-export destination <> vrf <>”.

  Conditions: This symptom occurs when “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120” is removed.

```
PE2(config)#no ip flow-export destination 10.21.1.1 3000 vrf vrf_1120

PE2#show vlan internal usage | i NDE      both NDE internal VLANs 1013, 1015
are cleared  from 'internal VLAN table'

PE2#show monitor event-trace idbman all | i NDE
clear NDE_1013 vlan 1013
clear NDE_1013 vlan 1013
```

  mapping 1013 is cleared, but 1015 is not cleared from idbman mapping

```
PE2#test platform debugger callfn name idbman_dump_vlans 0
Calling address (0x0AF46AFC) 1: Vl1 : 1
1015: NDE_1015 : 1015
```

  mapping 1015 is still present in IDBMAN, eventhough 1015 is a free VLAN, so, it can be allocated to any new interface

  Now, 1015 can be allocated for any other new interface, as it is cleared from “internal VLAN table”, whereas it is not cleared from IDBMAN mapping. Thus, you can reproduce the IDBMAN inconsistency with NDE interfaces.

  When a new interface comes UP, the IDBMAN set will fail, as there is already an old mapping existing (NDE_1015). When you try to delete this new interface, it will try to clear the mapping in IDBMAN. But, it finds the old mapping (NDE_1015); hence, you must perform forced crash in idbman_if_clear_vlan_id and configure “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120”.

```
PE2#show vlan internal usage | i NDE
1013 NDE
1015 NDE_vrf_0
```

```
PE2#show monitor event-trace idbman all | i NDE
set NDE_1013 vlan 1013
set NDE_1015 vlan 1015

                              PE2#test platform debugger callfn name
idbman_dump_vlans 0
                             Calling address (0x0AF46AFC) 1: Vl1 : 1
                              1013: NDE_1013 : 1013
                              1015: NDE_1015 : 1015
```

Workaround: Reload.

- CSCtt06191

  Symptoms: You cannot FTP copy file from the router to the FTP server.

  Conditions: The symptom is observed when using Cisco IOS Release 12.2(33)SRE3 and an FTP server configuration with overwrite off.

  Workaround: Change the FTP server configuration to allow overwrite.

- CSCtt19442

  Symptoms: Cisco 7600 subinterface that is configured for bridging after router reload sends traffic even when being shutdown. This traffic is sent from physical interface to which subinterface correspond and further received on the other side of the link.

  Conditions: This symptom is seen when bridging is configured on subinterface.

  Workaround:

  - Doing a **no shutdown**, then **shutdown** on the subinterface clears the issue.
  - Remove bridging configuration from subinterface.

  Deleting subinterface, and then recreating it does not fix the issue.

- CSCtt23367

  Symptoms: The status on active PoA is A/U. The status on standby PoA is S/A.

  Conditions: This symptom is seen after HA switchover. When configuring a new mLACP port-channel on new ACTIVE RP, it may get stuck in A/U state.

  Workaround: Remove the port-channel and RG configuration and add back again.

- CSCtt25612

  Symptoms: The router crashes with traceback error messages and the standby takes over. After this, the router is stable.

  Conditions: There is no known trigger or changes that were made as per the user update.

  Workaround: There is no workaround.

- CSCtt36757

  Symptoms: The following error message is noticed when configuring QoS on the interface of an ES+ card:

  ```
  %X40G_QOS-DFC9-3-CFN: qos tcam programming failed for policymap
  AGGR-CHA-INTERFACE-OUTPUT-POLICY
  ```

  Conditions: The symptom is observed after a misconfiguration in the interface. The interface was misconfigured as switchport which removed the QoS configuration from the interface configuration but not from the linecard. After the interface was configured back to an L3 port, the issue started occurring when the same policy was reapplied.

  Workaround: A new policy can be applied but the required policy cannot be applied again.

- CSCtt43834

  Symptoms: Netflow counter gets incremented when sending SSM group range as v2.

  Conditions: The symptom is observed when doing an SSO.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtt46873

  Symptoms: In an MVPN setup, when the **mdt default** command is removed from under the VRF, unicast packets coming from the core, such as LDP and BGP, get dropped, leading to router isolation.

  Conditions: This issue is primarily seen when mls mpls tunnel-recir is not configured on the box (or does not get enabled due to the absence of a sip10g device). In such a case, MDT tunnel VLAN gets allocated, but is never released, until the **mdt default** command is removed. Since the decap adjacency handling the unicast packets is a GRE decap, with an MDT tunnel VLAN allocated, removal/re-add of **mdt default** command will program the adjacency with the MDT tunnel VLAN. Another removal along with a race condition might leave the adjacency with the tunnel VLAN (now deallocated), thereby causing the unicast packets to be dropped.

  Workaround: Configure mls mpls tunnel-recir on the box and remove/re-add the **mdt default** command or reload with mls mpls tunnel-recir configured to be safe.

- CSCtt90672

  Symptoms: CFM MEP enters the INACTIVE state on deleting the subinterface.

  Conditions: This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check “CC-Status” = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check “CC-Status” = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT’s provisioning system does it, for example, for a new policy change). The “CC-Status” goes to inactive.

  Workaround: Unconfigure and reconfigure the **continuity check** command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

```
Router#sh buffers
Buffer elements:
     779 in free list (500 max allowed)
     1582067902 hits, 0 misses, 619 created

Interface buffer pools:
....
```

```
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ............... --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu30649

  Symptoms: Standby is reset.

  Conditions: This issue is seen when the ISSU standby is reset because of MCL failure.

  Workaround: There is no workaround.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

  Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

  Workaround: There is no workaround.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu42550

  Symptoms: ARP failure.

  Conditions: Occurs when IPv6 address or IPv6 multicast is configured.

  Workaround: There is no workaround.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

  Workaround: Remove “switchport port-security” from ports associated with the VLAN on which the IGMP reports are received.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if “DHCP Client” process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces.
  3. if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: The symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtx08147

  Symptoms: Mismatch in next-hop interface is observed in the outputs of the CEF table in **show ipv6 cef** as compared to **show mls cef ipv6**. For example:

```
Router#show ipv6 cef 2001:901:10::3/128
2001:901:10::3/128
  nexthop FE80::223:33FF:FE69:3DC0 TenGigabitEthernet2/1
  nexthop FE80::223:33FF:FE69:3DC0 TenGigabitEthernet2/2
  nexthop FE80::223:33FF:FE69:3DC0 TenGigabitEthernet2/3
  nexthop FE80::223:33FF:FE69:3DC0 TenGigabitEthernet2/4

Router#show mls cef ipv6 2001:901:10::3/128
Codes: + - Push label
Index  Prefix                              Adjacency
196610 2001:901:10::3/128                  Te1/4
```

```
001d.7083.3e00 (Hash: 000F)
                                                Te1/3
001d.7083.3e00 (Hash: 00F0)
                                                Te1/2
001d.7083.3e00 (Hash: 0F00)
                                                Te1/1
001d.7083.3e00 (Hash: 7000)
```

Conditions: The issue is triggered with link flaps and the traffic shifting completely to use an alternate path. Issue is observed with recursive routes enabled over BGP and ISIS. It is associated with ECMP paths. It occurs for IPv6 prefixes for which the CEF OCE chain (output chain: field in the output given by **show ipv6 cef** *prefix/mask* **internal**) starts with a load balance object.

Workaround: You can recover by these methods:

1. Clear IPv6 routes.
2. Add/remove static IPv6 routes for the bad prefixes.
3. Shut/no shut the interfaces.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE5

Cisco IOS Release 12.2(33)SRE5 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE5 but may be open in previous Cisco IOS releases.

- CSCso88042

  Symptoms: The VLANs allowed on the trunk to WiSM are lost on every reload.

  Conditions: This symptom occurs when the number of entries in the allowed-VLAN statement exceeds five.

  Workaround: Limit the number of entries to five or less, using ranges instead of single VLANs.

  Further Problem Description: When the entries in the VLAN-allowed statement are more than five, two WiSM module allowed-VLAN statements are seen, even though one line was allowed during configuration. When reloaded, only one WiSM module allowed-statement is taken, and the first statement is lost.

- CSCsq45560

  Symptoms: The port-channel member link stays as a standalone port with LACP.

Conditions: This symptom is observed only with the “vlan dot1q tag native” feature enabled.

Workaround: There is no workaround.

- CSCsy82121

  Symptoms: Flooding of multicast traffic can be seen on source-only multicast networks.

  Conditions: The symptom is observed on a Cisco Catalyst 6500 series switch that is running a SUP720 and with Cisco IOS SXF and SXH Releases.

  When the issue occurs, the **show mac-address multicast** command does not show the group to be installed. It is expected that the mrouter ports installed would be seen so that traffic is directed upstream. Once an IGMP join is received from a receiver, the group will not be source-only and will be installed in the MAC table.

  Workaround: There is no workaround.

- CSCtb24959

  Symptoms: The router may crash while clearing a large number of RP mappings.

  Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

  Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- CSCtd15853

  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

  Conditions: This symptom occurs under the following conditions:

  – mVPN is configured on the PE router.

  – Both Pre-MDT SAFI and MDT-SAFI IOS are running in a multicast domain.

  For more information about MDT SAFI, see the following document:
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

  Workaround: There is no workaround.

- CSCtg57599

  Symptoms: Lots of SNMP CPUHOG messages are seen and there is a crash due to a watchdog timeout:

  ```
  %SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
  (252/37),process =SNMP ENGINE

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE
  ```

  Conditions: The symptom is observed when polling Dot3Stats.

  Workaround 1: Use the **no snmp-server sparse-tables** command.

  Workaround 2: Block the objects in dot3 mib that contains this table from being polled:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown 1.3.6.1.2.1.10.7 excluded
  ```

  Then, to apply the view, use:

  ```
  no snmp-server community your_string_here RO
  no snmp-server community your_string_here RW
  ```

and then put it back so it looks like:

```
snmp-server community your_string_here view cutdown RO
snmp-server community your_string_here view cutdown RW
```

- CSCtg59328

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCth33804

  Symptoms: Traffic is dropped at CPP with the error message “noipv4route” after RP switchover, and traffic on few sessions is dropped.

  Conditions: This symptom occurs when the VRF is configured for PPPoE sessions and RP switchover is done with traffic flowing.

  Workaround: Do not configure the VRF.

- CSCth74953

  Symptoms: The SPI value is shown as 0x0. Hence, the ipsec sa validation is failing.

  Conditions: This symptom is observed when the crypto profiles are being applied. The symptom is not observed with simple crypto maps.

  Workaround: There is no workaround.

- CSCth87458

  Symptoms: Memory leak is detected in 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

- CSCti04919

  Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.

  Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.

  Workaround: Toggle the default MDT.

- CSCti23324

  Symptoms: With some L2 DEC configurations, recirculation may be added during packet forwarding.

  Conditions: This symptom is seen with L2 DEC and PFC3B configurations.

  Workaround: This is not a forwarding issue. Remove L2 DEC or use PFC3C in the L2 DEC.

- CSCti42671

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

  Conditions: This symptom occurs under the following conditions:

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

  Workaround: Reload the standby RP.

- CSCti82670

  Symptoms: An RSP will crash when the CFM automated test script (consisting of 53 tests) is run twice in succession. With Cisco SUP720, the crash is seen with a single run.

  Conditions: The automated test script must be run on three connected routers.

  Workaround: Adding a **no shut** on the UUT interface with UP-MEPS before doing the LeakConfig seems to prevent the crash and provide a clean run.

  Further Problem Description: Other problems observed are:

  - The CFM MIB will return infinite results for getmany.
  - A **show** command will crash the router.
  - Stale Earl Adjacency entries remain while adding or removing EVCs. The workaround is to reload the LC.

- CSCti87194

  Symptoms: The last fragment causes a crash because of an invalid zone value.

  Conditions: This symptom occurs when a Big IPC message is fragmented. Then, the last fragment causes the crash because of an invalid zone value.

  Workaround: There is no workaround.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

Workaround: There is no workaround.

- CSCtj94490

  Symptoms: The Route Processor (RP) reloads after 30 RP switchovers.

  Conditions: This symptom occurs after 30 RP switchovers during 28000 PPPoEoA sessions while traffic is flowing.

  Workaround: There is no workaround.

- CSCtk18404

  Symptoms: Per-user route is not installed after IPCP renegotiation.

  Conditions: The symptom is observed with the following conditions:

  1. A PPP session comes up, and NAS installs static routes that are sent as an attribute from the RADIUS server.
  2. After a while, if CPE asks for IPCP renegotiation, IPCP is renegotiated, but the static routes are lost.

  Workaround: There is no workaround.

- CSCtl67150

  Symptoms: PPP multilink interfaces fail to come up on the serial interface in Cisco ASR1K series routers.

  Conditions: This symptom occurs under the following conditions:

  1) When you create one or more than one t1 channel groups in a CT3 interface.

  2) When you create a multilink interface.

  3) When you create one link per channel group.

  4) When the encapsulation for every link is PPP, authentication CHAP.

  5) When the multilink interfaces fail to come up.

  Workaround: There is no workaround.

- CSCtl82681

  Symptoms: IPv6 configuration is blocked in the subinterface when xconnect is configured in the main interface under a service instance.

  Conditions: This symptom is seen if the xconnect is configured under a service instance that has its encapsulation configured as untagged, default or dot1q *vlan range*.

  Workaround: Change the encapsulation of the service instance that has the xconnect.

- CSCtl90292

  Symptoms: The following error messages are displayed:

  ```
  an 18 08:00:16.577 MET: %SYS-2-MALLOCFAIL: Memory allocation of 9420 bytes failed from
  0x42446470, alignment 32
  Pool: I/O Free: 11331600 Cause: Memory fragmentation Alternate Pool: None
  Free: 0 Cause: No Alternate pool -Process= "BGP I/O", ipl= 0, pid= 564
  -Traceback= 417E8BEC 4180FA6C 42446478 42446B64 42443984 40FC18C8 40FCCB4C
  40FD1964 403BDBFC 403BCC34 40344508 403668AC
  ```

  Conditions: This symptom is observed when several hits and failures are seen for medium buffers. All are linktype IPC.

  For example:

  ```
  Buffer information for Medium buffer at 0x4660E964
  ```

```
...
    linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
    if_input 0x481DEA50 (EOBC0/0), if_output 0x0 (None)
```

Workaround: There is no workaround.

- CSCtl97230

  Symptoms: When configuring 42 MLPP bundles, each bundle has two members. In 10 members, interleave is enabled and the policy is attached. After SSO is done under traffic, the LC crashes continuously in new active.

  Conditions: This symptom is observed when LC crash occurs with the Cisco 7600 software data plane environment. This issue is seen with SSO with the following conditions:

  1. PPP multilink interleave.
  2. Policy with priority feature.

  Workaround: There is no workaround.

- CSCtn16855

  Symptoms: The Cisco 7200 PA-A3 cannot ping across ATM PVC.

  Conditions: This symptom occurs due to a high traffic rate, and the output policy applied under PVC.

  Workaround: There is no workaround. Removing the policy will resolve this issue, but the QoS functionality will not be present in this case.

- CSCtn19444

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

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

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

- CSCtn31333

  Symptoms: CPU utilization is high due to the process Net Background.

  Conditions: This symptom is observed on a router used for LNS with an L2TP application after upgrading to Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCtn58128

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

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

  Workaround: Ensure that “no logging console” is configured.

- CSCtn62287

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

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

  Workaround: There is no workaround.

- CSCtn95122

  Symptoms: The ECC double-bit error is seen and the line card crashes. The following error message is reported by the LC:

  ```
  %NP_DEV-DFC5-3-ECC_DOUBLE: Double-bit ECC error detected on NP ... Mem 17
  ```

  Conditions: This symptom occurs when several sessions are deleted at the same time. In addition, there are other unknown race conditions that can cause this.

  Workaround: There is no workaround.

- CSCtn97451

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

  Conditions: This symptom occurs with the following conditions:

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

  ROUTER1:

  ```
  --------

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

  router ospf 100
      network 0.0.0.0 255.255.255.255 area 0
  !

  router bgp 1
      bgp log-neighbor-changes
      network 0.0.0.0
      neighbor 10.1.1.2 remote-as 1
      neighbor 10.1.1.3 remote-as 11 !
  ```

  ROUTER2:

  ```
  --------

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

```
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

ROUTER3:

```
-------

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

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

Crash reproduce steps are as follows:

1. Traffic travel from ROUTER3 to ROUTER2.
2. “clear bgp ipv4 unicast 10.1.1.1” on ROUTER2.

Workaround: There is no workaround.

- CSCtn99858

  Symptoms: Crashinfo is seen.

  Conditions: This symptom is observed during an 8k session.

  Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending the RT extended community for one of the redistributed VPNv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

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

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

- CSCto07586

  Symptoms: An IPv4 static BFD session does not get established on a system which does not have IPv6 enabled.

  Conditions: This symptom occurs with the following conditions:

  1. Create an IOS image that does not IPv6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPv4 static route with BFD routing through the above interface.

  The IPv4 BFD session does not get established, so the static route does not get installed.

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

- CSCto11957

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

```
%CWAN_RP-6-SESS_LIMITS_PORT_GROUP: Exceeded max number of sessions supported on
port-group
%SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
[ADJ:PPPoE:5789] - hardware platform error.

Mismatch in sessions on RP and ES+:
BRAS#sh pppoe summary
    PTA : Locally terminated sessions
    FWDED: Forwarded sessions
    TRANS: All other sessions (in transient state)
                                  TOTAL   PTA   FWDED   TRANS
TOTAL                                57    56       0       1
Port-channel100 57 56 0 1

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

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

Workaround: Change the port-channel number to port-channel 2. Configure sessions to terminate on standalone ports.

- CSCto31265

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

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

  Workaround 1: Delete/readd the static route that generates Type7.

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

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

- CSCto41165

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

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

  Workaround: There is no workaround.

- CSCto46716

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

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

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

- CSCto52194

  Symptoms: With the P2MPTE scenario, some of the met3 entries are not programmed properly.

  Conditions: This symptom occurs with shut/no shut of the interface.

  Workaround: There is no workaround.

- CSCto55567

  Symptoms: The ES+ card goes to a major error state because of fabric CRC errors.

  Conditions: This symptom occurs after SSO with multicast traffic flowing through the line card.

  Workaround: Soft reload the line card.

- CSCto63720

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

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

  Workaround: Reconfiguring port-security fixes the problem.

- CSCto70633

  Symptoms: Packets get punted to the RP because the default ACL does not get programmed on the Distributed Feature line card (DFC), which causes high RP CPU.

  Conditions: This symptom is observed upon removal and reinsertion of the line card when there are VRF-scale configurations on the ES+ card as given below:

  ```
  More than 800 subinterfaces with VRF configurations
  ```

  Workaround: Reload the router.

- CSCto71075

  Symptoms: High CPU usage is seen on changing the root node multiple times in an MLDP setup. Loss of PIM neighborship is also seen when changing the path in a P2MP setup.

  Conditions: This symptom occurs when ptcam redirection being enabled for LSPVIF can cause unexpected results. By default, LSPVIF ptcam redirection is disabled. This fix ensures that this is taken care of in scenarios of PIM state change.

  Workaround: There is no workaround.

- CSCto72629

  Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

  Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

  Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto79174

  Symptoms: A Cisco 7600 router crashes with the following logs:

  ```
  Frames of RPC pm-cp process (pid 325) on 6 (proc|slot) after blocking rpc
  call failed: 8331CD0 855F3F4 8546A58 85E3F98 85E4910 86009E4 86BF18C 86BC44C
  86BDE8C 8601090 8601394 835B498 8355774
  ```

```
Failed to send card online to CP, slot 2

%Software-forced reload

Unexpected exception to CPU: vector 1500, PC = 0xAF8765C , LR
= 0xAF87620
```

Conditions: The conditions are not known.

Workaround: There is no workaround.

- CSCto88660

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

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

  Workaround: There is no workaround.

- CSCto99523

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

  Conditions: This symptom occurs when convergence takes more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. This issue is seen when massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

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

  Conditions: This symptom occurs under the following conditions:

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

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

- CSCtq06538

  Symptoms: The RP crashes due to bad chunk in MallocLite.

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

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

  Workaround: There is no workaround.

- CSCtq09638

  Symptoms: The router crashes upon reconfiguration of the existing frame-relay subinterface with applied QoS.

  Conditions: This symptom is observed during reconfiguration of the existing frame-relay subinterface with applied QoS.

  Workaround: There is no workaround.

- CSCtq21435

  Symptoms: Some specific s,g entries do not pass traffic with MLDP during root node redundancy switchover.

  Conditions: This symptom occurs in case of MLDP + RNR. This issue is seen when Accept Vlan is programmed as zero in the platform.

  Workaround: Clear the mroute.

- CSCtq29547

  Symptoms: The router crashes on watchdog timeout while processing the SNMP request for ciscoEigrpMIB.

  Conditions: This symptom occurs while processing the SNMP request for ciscoEigrpMIB.

  Workaround: Exclude ciscoEigrpMIB from being polled by using the following SNMP view:

  ```
  snmp-server view NOCRASH internet included
  snmp-server view NOCRASH ciscoEigrpMIB excluded
  ```

  Then, apply the view to your SNMP community string:

  ```
  snmp-server community test view NOCRASH
  ```

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

  Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

  Workaround: Reload the failing line card to recover it.

- CSCtq34807

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

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

  Workaround: Remove and reapply the service group.

- CSCtq36241

  Symptoms: ISG session setup fails when per-user IPv4 ACLs are used and IPv6 routing is configured.

  Conditions: This symptom is observed when both IPv6 routing and per-user IPv4 ACLs are configured.

  Workaround: Remove either IPv6 routing or per-user ACLs.

- CSCtq37538

  Symptoms: Duplicate traffic is seen during route changes with P2MP TE for multicast or MLDP.

  Conditions: This symptom occurs during LSM configuration and route changes.

  Workaround: Clear the problematic mroute using the **clear ip mroute** command.

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq62759

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

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

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

- CSCtq64072

  Symptoms: A DHCP release received on a different member link of a PC other than the one on which it was requested is considered as fake and dropped.

  Conditions: This symptom occurs with the DHCP client release/decline message. The binding interface must match before the binding entry is removed to prevent someone from faking these messages to delete others’ valid binding.

  Workaround: There is no workaround.

  Further Problem Description: In case of a port-ch, the stored hwidb for a binding is that of the bridge interface. When a release is received on the other member-links, the hwidb does not match.

- CSCtq66679

  Symptoms: After “power cycle/red reload shelf”, the active PW stays in DOWN state forever in the case of a BFD-enabled protected PW. The standby PW is in UP state and traffic flow is through standby.

  Conditions: This symptom occurs in the PW redundancy scenario.

  Workaround: There is no workaround.

- CSCtq67680

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

  1. 1. Configure policy-maps as shown below: policy-map mul1 class GOLD priority 1000 class SILVER bandwidth 1000 policy-map mul2 class GOLD priority 7000 class SILVER bandwidth 7000 class class-default random-detect
  2. Apply it on multilink interfaces multilink1 and multilink2.
  3. Reload the SPA.

  Conditions: This symptom is observed only with QoS policy applied on multilink bundle on serial SPA.

  Workaround: There is no workaround.

- CSCtq80603

  Symptoms: Newly created SVIs are in down/down state.

  Conditions: This symptom occurs when SW VLAN RP process is stuck.

  Workaround: The following workarounds may work:

  1. Set the memory location of l2vlanifmib_access_count to zero after warm restart of the snmp-server.
  2. Perform SSO and/or LC OIR.
  3. Perform an active reload.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP IPv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

```
  interface Ethernet1/0
   vrf forwarding vpn1
    ipv6 address 1::1/64
!
  router bgp 65000
   address-family ipv6 vrf vpn1
    neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

  If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

  Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support the config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

  Conditions: This symptom occurs when a user changes the VRF assignment.

  Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq82715

  Symptoms: When the VPLS VC goes up/down, the DHCP snooping LTL has not been updated, resulting in DHCP packet drop.

  Conditions: This symptom occurs when the VPLS VC goes up/down, indicating that the DHCP snooping LTL has not been updated.

  Workaround 1: Enable/disable snooping.

  Workaround 2: Clear the xconnect peer for the newly elected peer.

  Further Problem Description: In such an event, the GPI is now passed onto DHCP snooping code to program its LTL.

- CSCtq83629

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

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

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

- CSCtq86216

  Symptoms: Multicast traffic flows over both primary and backup interfaces during TEFRR reopt.

  Conditions: This symptom occurs when multicast traffic flows over an MLDP core with TEFRR link protection.

  Workaround: Duplicate traffic flows only for a short period of time (20 seconds). So, the issue gets automatically resolved after 20 seconds.

- CSCtq91403

  Symptoms: High CPU can be seen during reloads under the MVPN topology.

  Conditions: This symptom occurs in an MVPN network with an S,G with an incoming interface over the MDT tunnel, when there are no forwarding interfaces for that S,G.

  Workaround: A possible workaround is to create a static join for that S,G to protect the RP CPU. Also, in some case multicast rate-limiters will be useful.

- CSCtq92182

  Symptoms: An eBGP session is not established.

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

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

- CSCtq93823

  Symptoms: Ping drops with fragment size of 256.

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

  Workaround: Flap the interfaces.

- CSCtq94418

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

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

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

- CSCtq96329

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

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

  The following releases are impacted:

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

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

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

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

- CSCtr14852

  Symptoms: A Cisco 7600 router may experience the following error conditions:

  1. The router starts displaying ICC WATERMARK messages. (This is expected if it happens for a short duration and is not associated with the second symptom mentioned below). For example:

```
Jun 7 17:31:22.422 UTC: %ICC-SP-5-WATERMARK: 1375 multicast tx pkts for
class L2-DRV(FC) are waiting to be processed

-Traceback= 81757BC 85FB874 85FC09C 85E5684 85E7CC8 85F18DC 85F1C7C 85F2050
84436A4 8443EA4 835C958 8356C34
```

  2. The above symptom would trigger a situation where the flow control mechanism is turned “ON” by the communication infra (ICC). As a result, the communication infra will fail to carry application data from one point to another within the router. This in turn would lead to failure of multiple features that are dependent on the ICC.

  For example: The ICC flow control can be verified by the following command:

```
BFW01#sh icc flowcontrol
Class Name                              FC state                  FC Counts (on/off)
                                                               [ Local ]   [ Remote ]   [ IPC ]
================================================================================
==
37 EARL_NDE(FC)                        [ OFF ]                    0/0          0/0         0/0
71 ACE_REQUESTS                        [ OFF ]                    0/0          0/0         0/0
77 ICC_FC_TEST_REQU                    [ OFF ]                    0/0          0/0         0/0
78 L3-MGR-QM(FC)                       [ OFF ]                    0/0          0/0         0/0
79 L3-MGR-FM                           [ OFF ]                    0/0          0/0         0/0
80 L3-MGR-INTF(FC)                     [ OFF ]                    1/0          0/0         0/0
```

  As shown above, the flow control is turned ON on L3-MGR-INTF, but never turned OFF.

  The ICC flow control mechanism is required to manage the ICC. If the flow control is turned on for a genuine reason, it will be turned OFF in a short while. This is expected.

  However, in this case, because of a bug in accounting, the flow control is turned ON (when not required), and never gets turned OFF, leading to the above situation.

  Conditions: This symptom occurs during “ICC MULTICAST” (not IP multicast) usage. This issue may be caused by heavy route flaps or interface flaps.

  Workaround: There is no workaround.

- CSCtr19286

  Symptoms: A “no shut” on an administratively down interface may result in overruns on other interfaces that are forwarding traffic. This occurs on ports being no shut for the first time in the same ASIC group. Subsequent shut/no shut on the same port does not cause this issue.

  Conditions: This symptom occurs under the following conditions:

  – This issue has been seen on Rohini ASIC-based DFC LAN cards such as WS-X6748-GE-TX.

  – The ports belong to the same port ASIC.

- This issue is seen only the first time you no shut an interface

Workaround: No shut all the ports in the ASIC group after bootup. Subsequent shut/no shut will not cause the overrun issue.

- CSCtr22007

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

  Conditions: This symptom is observed with MPLS-TE Tunnel Flap.

  Workaround: There is no workaround.

- CSCtr28527

  Symptoms: After a few minutes of HA cutover, DHCP snooping on a VLAN stops.

  Conditions: This symptom occurs after a few minutes of HA cutover.

  Workaround: Shut/no shut the port-channel interface.

  Further Problem Description: After SSO, the LTL consistency checker starts recomputing fpoe for each LTL. For those from the sw-mcast region, the LTL cc makes a callback to retrieve the gpid list to program the fpoe for the LTL. In this case, the DHCP snooping feature provides an incomplete list because the VPLS VC programming is done directly by the cwan_atom code and the feature is unaware of this gpid list. The VPLS VC gpid programming to LTL is now redirected to the feature itself.

- 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

- CSCtr34793

  Symptoms: The router cannot establish mVPN PIM adjacencies over an MDT tunnel. The core PIM still works normally.

  Conditions: This symptom may occur after router reload when mVPN with PIM is configured and PIM-hellos from the neighbors are coming to the line card with DFC. Another possible trigger could be removal/recreation of the MDT in a VRF definition.

  Workaround: Reload the line card.

- CSCtr37073

  Symptoms: WS-X6196-RJ-21 and WS-X6148X2-RJ-45 may fail to come online on the Cisco 7600 router when running SRC or higher images.

  Conditions: This symptom occurs when SRC or higher images are run on a Cisco 7600 router.

  Workaround: There is no workaround.

  Further Problem Description: This issue occurs due to a timing problem in the module initialization routine of the Cisco IOS.

- CSCtr37182

  Symptoms: XAUI coding errors are seen on the console.

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

Workaround: There is no workaround.

- CSCtr53677

  Symptoms: ARP failure is seen with the following **show** command:

  show arp vrf *vrf name*

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the ARP failure on the Gigabit subinterface.

  Workaround: There is no workaround.

- CSCtr53739

  Symptoms: The tunnel-encap entry is wrongly programmed. The following **show** command is used:

  show platform software multicast ip cmfib vrf *vrf-name* **tunnel-encap verbose**

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the tunnel-encap entry wrong programmed on the SP, with corrupt values.

  Workaround: There is no workaround.

- CSCtr69937

  Symptoms: The POS link flap in the core breaks the IPv4 PIC Core functionality.

  Conditions: This symptom occurs on Cisco 7600 routers running Cisco IOS Release 15.1(03)S.

  Workaround: Execute the **clear ip route** command for the affected prefix.

- CSCtr74529

  Symptoms: The following error messages are displayed:

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

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

  Workaround: There is no workaround.

- CSCtr80366

  Symptoms: Relay miscalculates the giaddr from the OFFER packet, and hence cannot find the binding.

Conditions: This symptom occurs while configuring multiple pools on the server and multiple secondary IP addresses on the relay loopback IP address.

Workaround: There is no workaround.

- CSCts15072

  Symptoms: Multicast traffic in the MVPN solution is dropped.

  Conditions: This symptom is observed on the Cisco 7600 series routers after deletion and (re)creation of a VRF.

  Workaround: Do not delete VRFs. All configuration related to a VRF can safely be removed. Only the VRF name should be retained in the configuration.

- CSCto55812

  Symptoms: The router may crash.

  Conditions: This symptom occurs on entering VLAN mode from a different mode, for example, VFI, without exiting from the previous command mode.

  Workaround: Always exit from the current command mode while entering into another command mode.

- CSCtn52529

  Symptoms: After the TE tunnels are recovered and resignaled, a timer is started to wait for the RESV to come in. If the RESV does not arrive, the timer is restarted and the PATH is sent out again. In this DDTS, the PATH was not being sent out after the timer expired.

  Conditions: This symptom occurs after the TE tunnels are recovered and resignaled and the RESV does not arrive after the timer is started.

  Workaround: There is no workaround.

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts51980

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

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

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRE4

Cisco IOS Release 12.2(33)SRE4 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE4 but may be open in previous Cisco IOS releases.

- CSCsc84683

  Symptoms: A crash is observed, along with a HASH_TABLE collision message, when a MAC address table entry for non-IP multicast MAC is removed.

  Conditions: This symptom occurs only with non-IP multicast MAC addresses. The crash is seen when the ports belonging to that entry are removed one by one from the MAC address table entry.

  Workaround: There is no workaround.

- CSCsl63149

  Symptoms: If you repeatedly use the **test mcast ltl** command on a switch processor (SP), a buffer leak is introduced. The SP may finally run out of buffers and the system crashes.

  Conditions: This symptom occurs when the **test mcast ltl** command is used repeatedly on an SP.

  Workaround: There is no workaround.

- CSCsq02771

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

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

  Workaround: There is no workaround.

- CSCsw32280

  Symptoms: Cisco Catalyst 6500 WS-X6148x-RJ-45 line cards report the following error:

  ```
  CONST_DIAG-SP-4-ERROR_COUNTER_WARNING: Module X Error counter exceeds
  threshold, system operation continue.
  %CONST_DIAG-SP-4-ERROR_COUNTER_DATA: ID:60 IN:0 PO:1 RE:2206 RM:0 DV:50
  EG:2 CF:2 TF:120
  ```

  Conditions: This symptom is observed when the interface (Po=Port number) reported in the error message receives traffic with the wrong CRC and is reported under “show interface”.

  Workaround: The only workaround is to turn off the test as follows:

  ```
  Router# diagnostic stop module <mod#>
  ```

  The fix is available in Cisco IOS Release 12.2(33)SXI1 or later releases.

  Further Problem Description: The following are sample logs:

  ```
  Router# show diagnostic result module 9 detail

   9) TestErrorCounterMonitor ---------> F <<== shows the result for last
                                                 execution of this test.

          Error code ------------------> 1 (DIAG_FAILURE)
          Total run count -------------> 54
          Last test testing type ------> Health Monitoring
          Last test execution time ----> Dec 17 2008 21:35:22
          First test failure time -----> Dec 17 2008 21:33:46
          Last test failure time ------> Dec 17 2008 21:35:22
          Last test pass time ---------> Dec 17 2008 21:33:15
          Total failure count ---------> 14
          Consecutive failure count ---> 13

  The error records are as follows:
          ID -- Asic Identification
          IN -- Asic Instance
          PO -- Asic Port Number
  ```

```
RE -- Register Identification
RM -- Register Identification More
EG -- Error Group
DV -- Delta Value
CF -- Consecutive Failure
TF -- Total Failure

   ID   IN    PO      RE      RM      DV   EG      CF      TF
-------------------------------------------------------------
   60    0     0    2206       0    2982    2      13      14
   60    0     1    2206       0    2982    2      13      13
```

- CSCsz39222

  Symptoms: A Cisco router reloads and the crashinfo file indicates a cache error. CPO_ECC has the following value:

  ```
  Cache error detected! CPO_ECC (reg 26/0): 0xC0000000
  ```

  This was a hardware corrected cache error that should not result in a router reload.

  Conditions: This symptom is observed when register 26/0 contains 0xC0000000.

  This issue affects the RAN SVC card, NPE-G1 on a Cisco 7200 platform, NSE-150 on a Cisco 7300 platform, Sup32 for Cisco 6500/7600 platforms, SIP line cards for the Cisco 6500/7600, Cisco 67XX lan line cards for the Cisco 6500/7600 platforms, Cisco AS5400XM, Cisco UBR10K/PRE4, and other platforms using the same memory controller chip. Sup720 is not affected. NPE-G2 is not affected. NSE-100 is not affected. While rare, there is no specific trigger for this failure other than having a single bit parity error on ECC memory.

  Workaround: There is no workaround. The router will reload and continue normal operation. The fix prevents a crash after a single bit parity error occurs on ECC memory.

  Further Problem Description: This symptom does not cause a parity error or actually cause the crash. This symptom is just to add an error handler for the specific case of a single bit correctable parity error in ECC memory. The crash results from the parity error itself. The following is an example of the beginning of a crashinfo collection for a hardware corrected cache error:

  ```
  Cache error detected!
      CPO_ECC (reg 26/0): 0xC0000000
      CPO_CACHERI (reg 27/0): 0x34001DE0
      CPO_CACHERD (reg 27/1): 0x10800580
      CPO_CCHEDPA (reg 27/3): 0x017B4580
  ```

- CSCta62394

  Symptoms: A Cisco Catalyst 6000 router that is running Cisco IOS Release 12.2(18)SXF16 with ipsec HA and dynamic crypto maps reloads when the standby tears down all the IPSEC SAs.

  Conditions: This symptom occurs with the following conditions:

  1. The Cisco Catalyst 6000 router is running Cisco IOS Release 12.2(18)SXF16.
  2. IPSEC HA is enabled.
  3. Dynamic crypto maps are configured.
  4. SAs are torn down on the standby (for example, when using the **clear crypto session** command or deleting a VLAN with crypto on it).
  5. A dynamic crypto map is configured on the router. 6) The user attempts to clear the dynamic crypto map's SAs using the **clear crypto sa spi** command.

Workaround: Under conditions 1 through 4 that apply to the Cisco IOS Release 12.2SXF throttle, use static crypto maps instead of dynamic crypto maps. Under conditions 5 and 6 that apply to the Cisco IOS Release 12.2SR throttle, do not use the **clear crypto sa spi** command or do not use a dynamic crypto map.

- CSCtc49086

  Symptoms: When configuration changes are performed within a multicast-enabled VRF that cause the PIM register tunnel interface to go down and up again, spurious memory access appears when traffic is sent at the same time.

  Conditions: This symptom occurs when traffic is sent when configuration changes are performed.

  Workaround: There is no workaround.

- CSCtd14703

  Symptoms: High CPU at Net Background is seen for around 3 minutes after SSO. Unicast protocol such as ospf may be flapping due to high CPU.

  Conditions: This symptom is observed when scale P2P GRE tunnels are configured on Cisco Catalyst 6500 LAN switching.

  Workaround: There is no workaround.

- CSCtf07365

  Symptoms: The vrf oif tunnel interface is missing for several seconds after SSO on the source side PE.

  Conditions: This symptom occurs when you configure the Cisco Catalyst 6500 as MVPN PE. The mfi/mrib and HW entry works fine for the fist 3 minutes after SSO and after BGP convergence is completed. The vrf oif tunnel interface is missing for 20 seconds in the mrib/mfib table when the system does reconstruction, causing vrf traffic to be dropped on the source side PE for several seconds.

  Workaround: There is no workaround.

- CSCtf08317

  Symptoms: Unable to connect to line card after switchover.

  Conditions: This symptom occurs while connecting to line card after switchover.

  Workaround: There is no workaround.

- CSCtf50944

  Symptoms: Active or standby RP crash is seen when configuring dot1q/QinQ non-access subinterfaces.

  Conditions: This symptom is observed with the following conditions:

  1. Configure around 10 non-access subinterfaces, bring session and delete the subinterfaces.
  2. Configure same subinterfaces (subinterface #), with a different encapsulation.

  Crash is seen with the following message:

  ```
  % idbman_if_set_vlan_id: GigabitEthernet12/8.4 has vlan 1022, vlan 1023 not set
  ```

  The crash occurs very rarely and is triggered by timing idiosyncrasies. The issue is only seen when the configuration is done using scripts.

  Workaround: There is no workaround.

- CSCtf91692

  Symptoms: When a WS-X6708-10GE module or a WS-X6716-10GE module is inserted into a 6509 or 6513 chassis, it may cause the module in slot N-8 to reload. For example, inserting the module into slot 9 may reset the module in slot 1, inserting the module into slot 10 may reset the module in slot 2, inserting the module into slot 13 may reset the module in slot 5, and so on.

  Conditions: This symptom occurs with the following conditions:

  1. The 6708/6716 module is inserted in slots 9 to 13.
  2. Module insertion is done slowly.

  Workaround: This problem has been fixed.

- CSCtg91572

  Symptoms: A router with an SSM (S,G) entry consisting of a NULL outgoing list sends a periodic PIM Join message to the upstream RPF neighbor, thereby pulling unnecessary multicast traffic.

  Conditions: This symptom is observed when the router has a NULL outgoing list for an SSM (S,G) entry either due to PIM protocol action (Assert) or when the router is not the DR on the downstream access interface receiving IGMPv3 reports.

  Workaround: There is no workaround.

- CSCth15353

  Symptoms: Incorrect result codes are displayed in vpdn sys logging. The CDN message for admin down was reported in the syslog as “Result Code=2, Error Code=6” instead of “Result Code=3, Error Code=6”.

  Conditions: This symptom is observed when a session is cleared by a clear command (for example, **clear interface virtual-access 3.1**).

  Workaround: There is no workaround.

- CSCth37674

  Symptoms: A crash happens when the **show ip dhcp vrf** *vrf-name* command is executed.

  Conditions: This symptom occurs when the **show ip dhcp vrf** *vrf-name* command is executed.

  Workaround: There is no workaround.

- CSCth52444

  Symptoms: When the strict priority is configured in the policy, the policing action allows to configure exceed action as transmit.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(0.9)S.

  Workaround: There is no workaround.

- CSCth66177

  Symptoms: The standby route processor (RP) triggers an active RP crash.

  Conditions: This problem is observed when the standby RP crashes due to a memory parity error.

  Workaround: There is no workaround.

- CSCth84714

  Symptoms: With scaled number of MLP bundles on SIP200 which has Distributed Link Fragmentation and Interleaving (dLFI) enabled, the SIP200 crashes.

  Conditions: This symptom occurs with the following conditions:

  1. Reload the SPA having MLP bundles.

2. Shut/no shut the controller.
3. Flap the links by any other means.

Workaround: The issue is not seen without high traffic and without dLFI enabled.

- CSCti18615

  Symptoms: Reloading a router which has multicast forwarding configured can result in the standby RP being out of sync with the active RP. The A and F flags are missing from the multicast forwarding base entries.

  Conditions: This symptom occurs when multicast forwarding is operational and configured in the startup configuration, and when the router is in HA mode SSO and is reloaded from the RP.

  Workaround: Perform a shut/no shut of the affected interfaces.

- CSCti81177

  Symptoms: Features like Videomon do not work on a routed port.

  Conditions: This symptom occurs when an interface is configured as a switch port and reconfigured as a routed port.

  Workaround: Reload the line card.

- CSCti92812

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

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

  Workaround: There is no workaround.

- CSCtj11497

  Symptoms: The Shared Port Adapter (SPA) crashes after receiving the "%INTR_MGR-3- INTR: PL3 RX Sequence" error.

  Conditions: This symptom occurs under normal working conditions.

  Workaround: The SPA reloads automatically and clears the problem.

- CSCtj20776

  Symptoms: Accounting-stop record is sent for radius proxy session when reauthentication happens for that session.

  Conditions: This symptom is seen in the following scenarios:

  1. The authentication request comes from AP.
  2. The accounting request comes from AZR and the session on ISG is associated to AZR.
  3. ISG receives a reauthentication request from AP. The Accounting-stop record is sent for Radius-Proxy session and the services under the session, but the radius-proxy session is still active and no stop record is sent for the session on clearing the session. Also, acct-terminate-cause in the stop record is set to none.

  Workaround: There is no workaround.

- CSCtj61748

  Symptom: Service activation fails occassionally.

  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.

- CSCtj65692

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

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

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

- CSCtj79676

  Symptoms: The router crashes sometimes once CEF is enabled.

  Conditions: This symptom occurs when CEF is enabled.

  Workaround: There is no workaround.

- CSCtj87846

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

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

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

- CSCtk07240

  Symptoms: When a member-link is removed from an L2 port-channel (a port-channel with switchport configured under it), the traffic stops flowing.

  Conditions: This symptom occurs when a member link of L2 port-channel that is passing traffic is removed from the port-channel.

  Workaround: Remove and add the port-channel configurations again.

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: This symptom is observed only if DUT has an eBGP-VPNv4 session with a peer and a same-RD import happens on the DUT for the route learned from the VPNv4 peer.

  Workaround: A hard reset of the session will remove the dampening information.

- CSCtk59347

  Symptoms: CPU is busy and console is locked up for minutes after entering the **clear counter** command.

  Conditions: This symptom occurs with a large-scale configuration with hundreds of interfaces and service groups configured on the system.

  Workaround: Instead of clearing all counters of all interfaces, clear the counters of specific interfaces as needed.

- CSCtk64538

  Symptoms: The **ip igmp join-group** and **ipv6 mld join-group** commands will not work as expected on the Cisco 7600 platform.

  Conditions: This symptom occurs with basic configurations of join group on Cisco 7600 series routers.

Workaround: Use the **ip igmp static-group** or **ipv6 mld static-group** commands instead.

Futher Problem Description: The **ip igmp join-group** and **ipv6 mld join-group** commands are not normal configurations on the Cisco 7600 router. They cause traffic to be punted to RP CPU and cause problems.

- CSCtk67658

  Symptoms: Traceback and infrequent crash of the new active are seen when SSO is performed on a router .

  Conditions: This symptom occurs when SSO is performed on a router.

  Workaround: There is no workaround.

- 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.

- CSCtk68890

  Symptoms: The router configured with an empty export-map crashes upon sending out refreshed routes using the **clear ip bgp * soft** command.

  Conditions: This symptom occurs in a rare situation when the router is configured as a PE and ASBR, and crashes upon configuring an empty export-map without any ext-community RTs.

  Workaround: Do not configure an empty export-map.

- CSCtk76697

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

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

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

- CSCtk83376

  Symptoms: The subscriber is not able to get authorized after initial access-reject.

  Conditions: This symptom occurs when a subscriber supplies wrong credentials and access is rejected. Then, the subscriber provides correct credentials, but the access is rejected. The subscriber is not able to log on even with the correct credentials after initial access-reject.

  Workaround: Add the following to reset the session:

  ```
  class type control always event access-reject
      1 service deny
  ```

- CSCtk95106

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

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

Workaround: There is no workaround.

- CSCtk97082

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

  Conditions: This symptom occurs with the following conditions:

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

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

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

- CSCtl00127

  Symptoms: The output of **show ip int** command does not indicate whether the “ip security ignore-cipso” option is configured and/or operational.

  Conditions: Configure “ip security ignore-cipso” on an interface. This was not indicated on the **show ip interface** *interface-name* output of that interface.

  This symptom is observed on the following devices:

  - Cisco IOS Catalyst 6500 router that is running Cisco IOS Releases 12.2(33)SXH and 12.2(33)SXI.
  - Cisco IOS Catalyst 7600 router that is running Cisco IOS Releases 12.2(33)SRA7, 12.2(33)SRB, 12.2(33)SRC, 12.2(33)SRD, and 12.2(33)SRE.
  - Cisco IOS Catalyst 4500 router that is running Cisco IOS Release 12.2(40)SG.

  The output is indicated correctly when it is enabled on Cisco IOS Release 12.2(18)SXF17a.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: This symptom is observed on a router running BGP, configured with new style IPv4 MDT and peering with an old style IPv4 MDT peer. Affected releases are Cisco IOS Release 12.2(33)SRE, 15.0M, and 12.2(33)XNE and later releases.

  Workaround: There is no workaround.

- CSCtl05785

  Symptoms: Connectivity is broken on Cisco 7600 L3 subinterfaces upon reconfiguration of the assigned VRF. Directly connected devices are no longer reachable. Input path is broken (packets are seen in netdr but do not reach the RP).

Conditions: This symptom is observed on Cisco 7600 routers that are running Cisco IOS Release 12.2(33)SRE2. This issue is seen on Sip-400 subinterfaces.

Workaround: Reload the router.

- CSCtl21695

  Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million. Debug vpdn l2x ev/er shows:

```
PPTP _____:________: TCP connect reqd from 0.0.0.0:49257
PPTP _____:________: PPTP, no cc in l2x
```

  Conditions: This symptom occurs when LNS is configured for PPTP aggregation and over one millions tunnels have been accepted (on VPDN level).

  Workaround: Reload LNS.

- CSCtl54033

  Symptoms: Resignaling sub-LSPs for P2MP TE tunnels may take up to 10 seconds, after the sub-LSP has been pruned or torn down.

  Conditions: This symptom occurs when a P2MP TE tunnel is configured to request FRR protection, but for the physical link down the path on the tunnel headend, there is no backup tunnel configured at the failure point (TE tunnel headend) to protect the sub-LSP. The TE tunnel headend will take 10 seconds for sub-LSP resignaling.

  Workaround: Configure FRR backup tunnels at the TE tunnel headend to provide link protection for P2MP TE tunnels for the physical link that is connected to the TE tunnel headend in the TE tunnel path.

- CSCtl67195

  Symptoms: The following three BGP debug commands are not allowed to enable:

  - **debug ip bgp vpnv4 unicast**
  - **debug ip bgp vpnv6 unicast**
  - **debug ip bgp ipv6 unicast**

  Conditions: This symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- 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.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: This symptom is observed when BGP is configured and you issue one of the following commands:

  - **show ip bgp all attr nexthop**
  - **show ip bgp all attr nexthop rib-filter**

Workaround: Do not issue either of these commands with the **all** keyword. Instead, issue the address family-specific version of the command for the address family you are interested in.

For example, the following are safe:

- **show ip bgp ipv4 unicast attr nexthop**
- **show ip bgp attr nexthop**
- **show ip bgp vpnv4 vrf** *vrfname* **attr nexthop**

Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multitopology routing or which are derived from versions which included multitopology routing, and where this fix is not integrated are impacted.

The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl93514

  Symptoms: QoS configurations do not get applied on the interfaces when the router is upgraded from ES20 to ES+.

  Conditions: This issue happens when the ES20 is replaced with ES+. Remove the ES20 LC and insert the ES+ LC on the same slot.

  Workaround: Remove all QoS policies applied on the ES20 interfaces. Insert ES+ and reapply all QoS policies once the ES+ interfaces are up.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

  Conditions: This symptom occurs when a double failure, such as SSO switch and FRR cutover, causes XDR CPU hog and crashes the system.

  Workaround: There is no workaround.

  Further Problem Description: The crash can be avoided if the system has no double failure.

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  - **config check syntax**
  - **route-map hello**
  - **match local-preference**
  - **no match local-preference**

  Conditions: This symptom is observed with the commands mentioned above.

  Workaround: There is no workaround.

- CSCtn10922

  Symptoms: A router configured with “atm route-bridged ip” on an ATM subinterface may drop multicast traffic, and in some cases, may undergo a software initiated reload due to memory corruption. This issue is also evidenced by the presence of an incomplete multicast adjacency on the ATM subinterface.

  Conditions: This symptom is observed on ATM subinterfaces that are configured with “atm route-bridged ip” and forwarding multicast traffic.

  Workaround: Configure the **ip pim nbma-mode** command on the point-to-point ATM subinterfaces.

- CSCtn15317

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

  Conditions: This symptom occurs with the following conditions:

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

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

  Workaround 2: Change the BGP update source.

- CSCtn16840

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

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

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

- CSCtn17680

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

  ```
  %EARL_L2_ASIC-SP-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. Error occurred. Ctrl1
  0xB88D0E3D Then, the following message is displayed: %CPU_MONITOR-SP-2-NOT_RUNNING:
  CPU_MONITOR messages have not been sent for 60 seconds [*Sched* 41%/0% (00:01:00.244
  99%/99%)] Finally, a timeout occurs, followed by the crash:
  %CPU_MONITOR-SP-3-TIMED_OUT: CPU_MONITOR messages have failed, resetting system (self)
  [5/0]
  ```

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

  Workaround: There is no workaround.

- CSCtn19178

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

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

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

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

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

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

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

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

- CSCtn21561

  Symptoms: A crash occurs following DNS translation by NAT.

  Conditions: NAT is configured.

  Workaround: Identify the responding server of the DyDNS updates and block traffic destined to it to prevent it from being NATted. This server may be the IANA “blackhole” server address.

- CSCtn22728

  Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ? <cr>
Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)# Config Sync: Line-by-Line sync verifying failure on command:
destination int g11/48 due to parser return error
```

  Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between active and standby-RP, therefore reloading standby-RP.

  Workaround: Do not issue not applicable commands.

- CSCtn26307

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

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

  Workaround: A reboot will resolve this issue.

- CSCtn41245

  Symptoms: Subinterface ingress stats do not work for access subinterfaces.

  Conditions: This symptom is observed only for the access subinterface. Interface stats and regular subinterface stats work as expected.

  Workaround: There is no workaround.

- CSCtn41662

  Symptoms: Standby RP crashes sometimes when policymap configuration is done. This crash happens randomly with the following crash decode:

```
0xA65C01C:qm_make_final_vmr(0xa65bf14)+0x108
0xA64799C:qm_send_merge_replace_request(0xa647834)+0x168
0xA6471B0:qm_tm_merge_replace(0xa646ee4)+0x2cc
0xA63B3FC:qm_tcam_modify_service_policy(0xa63adbc)+0x640
0xA63A8AC:qm_process_mqc_event_hdlr(0xa63a51c)+0x390
0xA63BE7C:qm_process_events_q_hdlr(0xa63bad0)+0x3ac
0xA63CAA0:qm_process(0xa63c9cc)+0xd4
```

  Conditions: This symptom occurs randomly when policy-map, class-map is modified and applied on different interfaces. This does not happen consistently.

  Workaround: There is no workaround.

- CSCtn45777

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

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

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

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

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

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

- CSCtn53222

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

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

  Workaround: There is no workaround.

- CSCtn59698

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

  Conditions: This symptom is observed with the following conditions:

  1. Only for MLP sessions on LNS.
  2. When you configure per-user attributes in the user'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>".

- CSCtn62250

  Symptoms: After upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3, there may be a problem with PIM MDT neighbors, which do not get brought up, though the configuration is not changed.

Conditions: This symptom is observed after upgrade on the Cisco 7600 router from Cisco IOS Release 12.2(33)SRD5 to Cisco IOS Release 12.2(33)SRE3.

Workaround: Remove/reinsert the **mdt default** command in ip vrf configuration mode.

- CSCtn68329

  Symptoms: When source and receivers are in the same VLAN, receivers are unable to receive multicast traffic unless IGMP snooping is disabled for the VLAN.

  Conditions: This issue is not seen when VLAN is in global routing table (no MVPN).

  Workaround: Disable IGMP snooping for the VLAN.

- CSCtn73941

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

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

Router#sh run int ten4/1
Building configuration...
Current configuration : 64 bytes
!
interface TenGigabitEthernet4/1
  no ip address
  shutdown
end
```

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

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

- CSCtn74673

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

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

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

- CSCtn80120

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

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

  Workaround: There is no workaround

- CSCtn89179

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

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

  - Hardware: SIP: 7600-SIP-400, SPA: 7/1 8xCHT1/E1 SPA
  - Software: Cisco IOS c7600rsp72043-adventerprisek9-mz.122-33.SRD or later releases

  Workaround:

  1. Apply a service policy similar to below:

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

  2. Reload the LC.

- CSCtn90664

  Symptoms: On a Cisco 7600 router, which has globally configured “mls qos protocol arp police <value>”, packets which are received on an ES+ switchport/SVI interface bypass the policer and cause high CPU.

  Conditions: This symptom is observed on an ES+ switchport/SVI interface with “mls qos protocol arp police <>” enabled on the router.

  Workaround 1: Broadcast storm control could be used to rate-limit arp broadcast packets.

  Workaround 2: The following policy can be configured on the interfaces (applicable only after Cisco IOS Release 12.2(33)SRE3, 15.0(01)S2, 15.1(01)S01, and 15.1(2)S onwards):

  Policy-map ingress_policy-map

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

class-map cos0
 match cos 0
class-map cos1
 match cos 1
class-map cos2
 match cos 2
class-map cos3
 match cos 3
class-map cos4
 match cos 4
class-map cos5
 match cos 5
class-map cos6
```

```
 match cos 6
class-map cos7
 match cos 7
```

And then dscp-transparency enabled using the following CLI:

```
no mls qos ip rewrite dscp slot <module>
```

- CSCtn95344

  Symptoms: After RPR downgrade from SRE2 CCO to SRE1 CCO, the standby RSP gets stuck in cold bulk and reboots every 50 minutes.

  Conditions: This symptom occurs after RPR downgrade from SRE2 CCO to SRE1 CCO.

  Workaround: Perform reload on the router.

- CSCtn98966

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

  Topology:

  ------------------------------POA-1(active)

  | |

  DHD |(L3 ICC link and L2 Trunk)

  | |

  ----------------------------POA-2(standby)

  In Cu's environment: When DHD sends an ARP request to ask for MAC of an HSRP virtual IP, it will receive the ARP reply from the standby PoA, causing MAC flapping on DHD. In the lab test environment: When you configure static ARP on PoAs to bind an IP address with a nonexistent MAC address, ping this IP, so it will do unicast flooding within VLAN. When you ping, POA-2(standby) also sends out the unicast packet to DHD via its port-channel link.

  Conditions: This symptom occurs both on SRE2 and SRE3 with MLACP deployment.

  Workaround: There is no workaround.

- CSCto02448

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

  Conditions: This symptom is observed with the following conditions:

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

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

- CSCto04593

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

  Conditions: This symptom is seen only with scale.

  Workaround: There is no workaround.

- CSCto04953

  Symptoms: On a multilink with strict priority, after several hours of traffic load, the traffic gets dropped to 50 to 70 percent. At the same time, there is a 100 percent drop on default class. At worst, 100 percent of the strict priority queue can be dropped.

  Conditions: This symptom is observed when the traffic load is close to the given bandwidth.

  Workaround 1: Stop the traffic; the issue goes away for several hours.

  Workaround 2: Remove and add the policy back; the issue goes away for several hours.

  Workaround 3: Unconfigure and reconfigure the impacted interface multilink.

- CSCto07919

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

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

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCto10336

  Symptoms: The LNS router hangs up at the interrupt level and goes into an infinite loop.

  Conditions: This symptom occurs during control channel cleanup.

  Workaround: There is no workaround. This symptom can be only removed through power cycle.

- CSCto15040

  Symptoms: When configuring a service instance under the physical interface, the service instance may not be programmed properly on the Switch Processor or the line card, leading to loss of connectivity.

  Conditions: This symptom is observed when configuring the service instance under the physical interface of an ES+/ES20/SIP-600 card. This issue is seen with Cisco IOS Release 12.2(33)SRE or later releases.

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

- CSCto16106

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

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

  Workaround: There is no workaround.

- CSCto29720

  Symptoms: Packets drop in the LLQ queue without any congestion on the link when the line card is SIP-400.

  Conditions: This symptom occurs when LLQ is configured under Shaper on the physical interface and the line card is SIP-400.

Workaround: There is no workaround.

- CSCto43154

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

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

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

  Workaround: There is no workaround.

- CSCto55643

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

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

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

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

- CSCto55983

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

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

  Workaround: There is no workaround.

- CSCto64240

  Symptoms: Port-channel access sub-interface with three memberlinks cannot be configured.

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

  Workaround: There is no workaround.

- CSCto70972

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

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

  Workaround: There is no workaround.

- CSCto74038

  Symptoms: After an upgrade to SRE3, the CESoPSN (clock) pseudowire stays down due to payload size value mismatch.

  Conditions: This symptom occurs when, before the upgrade to SRE3, the payload size is configured to 80 and dejitter value is the default (5). After the upgrade, the payload size 80 and dejitter 5 combination is not accepted anymore as it is not the recommended value, so the payload size is

removed from the configuration. The pseudowire is therefore configured with the default payload size. The default value is not accepted by the remote end of the pseudowire, thus leading to payload size mismatch.

Workaround: Configure an acceptable dejitter value, and then reconfigure the payload size.

- CSCto80714

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

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

  Workaround: There is no workaround.

- CSCto83073

  Symptoms: A Cisco 7600 router running Cisco IOS Release 12.2(33)SRE3 crashes when installing a new certificate or when authenticating a trustpoint.

  Conditions: This symptom occurs with the following conditions:

  1. If the router loads the CA certificate. If the trustpoint has been already authenticated, this symptom will occur usually after a reload.
  2. After you configure a new trustpoint and try to authenticate it.

  Workaround: There is no workaround.

- CSCtq10019

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

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

  Workaround: There is no workaround.

- CSCtq09088

  Symptoms: The router crashes while trying to unconfigure “ip rsvp sender-host 10.0.0.5 10.0.0.1 UDP 11 11 10 10 identity bogusID”.

  Conditions: This symptom is observed on the Cisco 7200 router running the c7200-adventerprisek9-mz.122-33.3.13.SRE image.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE3

Cisco IOS Release 12.2(33)SRE3 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE3 but may be open in previous Cisco IOS releases.

- CSCsb87956

  Symptoms: A software loop enters the IKE_CONFIG_MODE state.

  Conditions: This symptom is observed when the following events occur:

  1. A user is normally connected to the IPSec gateway trough a NAT-T device.

2. The physical connection goes down on the user side, the interface is shut down, and SafeNet disconnects, but the connection is still up on the IPSec gateway.
3. The physical connection goes up on the user side and a new connection is attempted before DPD causes the old connection to go down on the IPSec gateway.

Workaround: After a disconnection, wait for DPD to tear down the IPSec/ISAKMP sessions. In a production network, there is no workaround.

- CSCsj70622

  Symptoms: Cisco router running Cisco IOS Release 12.2(33)SRD or 12.2(33)SRE may experience a memory leak due to crypto processes using MallocLite.

  Conditions: The symptom is observed when crypto is configured.

  Workaround: There is no workaround.

- CSCsl18054

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

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

  Workaround: There is no workaround.

- CSCso20810

  Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. This sympotm occurs when multicast subsequently flows out a crypto-enabled interface.

  Conditions: This symptom will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

  Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsq40621

  Symptoms: Accounting fails due to No Acct-Input/output-Octets/packets field in the STOP accounting records. Many sub-test cases are failing for the same reason in the ipsec accounting script. A session startID and stopID exists, but it shows as “0” and does not have the following fields:

  `Acct-Input-Octets Acct-Output-Octets Acct-Input-Packets Acct-Output-Packets`
  The traffic is flowing successfully but the outputs are not available in the stop accounting records stored in the radius server.

  Conditions: This symptom does not affect IKE/ipsec functionality.

  Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv70157

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

```
"Warning: Overriding existing carrier delay value to 0"
```
Conditions: No special conditions are required to reproduce this defect. Simply configure any interface with a carrier delay and execute **wr mem**:

```
Router#conf t Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f2/12 Router(config-if)#carr Router(config-if)#carrier-delay 2
Router(config-if)#end Router#wr Building configuration... Warning: Overriding existing
carrier delay value to 0
%SYS-5-CONFIG_I: Configured from console by console[OK] Router#
```
Workaround: There is no workaround.

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

- 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: This symptom is observed under the following conditions:

  - ASR is set as a dhcp relay agent
  - 8kvlan configuration
  - 8port-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.

- CSCsy16092

  Symptoms: A router running Cisco IOS or Cisco IOS XE may unexpectedly reload due to watchdog timeout when there is a negotiation problem between crypto peers. The following error will appear repeatedly in the log leading up to the crash:

  ```
  .Mar 1 02:59:58.119: ISAKMP: encryption... What? 0?
  ```
  Conditions: When a malformed payload (Transform payload with vpi length =0) is received and "debug crypto isakmp" is enabled, the error messages are repeatedly seen leading up to the crash.

  Workaround: Remove this debug command.

- CSCsy61302

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

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

  snmp-server community public ro snmp-server packetsize 17940

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

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

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

- 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.

- CSCta26520

  Symptoms: The following traceback is seen:

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

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

  Workaround: There is no workaround

- 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.

- CSCta43825

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

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

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

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

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

- CSCta53372

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

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

Workaround: Reset the RRI session.

- CSCtb07984

  Symptoms: A Cisco ASR router acting as LNS fails to apply D2 QoS on the first few sessions after every new reboot and configures the D2 QoS on all subsequent sessions.

  Conditions: The symptom is observed when multiple routes exist on an LNS router to reach LAC router. PPPoX sessions are brought on LNS with D2 QoS model after new reboot of router.

  Workaround 1: LNS router configures D2 QoS on all subsequent sessions in Cisco IOS Release 12.2XND images.

  Workaround 2: In Cisco IOS Release 12.2XNE images, LNS router should have a single route to reach LAC router.

  Workaround 3: Wait until CEF is converged before bringing up a second session on the LNS router.

- CSCtb32043

  Symptoms: CPUHOG messages may be displayed or Cisco IOS might crash when executing **no ipv6 multicast-routing** in a configuration with more than 20,000 IPv6 multicast-enabled interfaces or sub-interfaces.

  Conditions: This symptom is observed only rarely when an alternate software path is taken. It is not known what causes this alternate path to be taken.

  Workaround: There is no workaround.

- CSCtb32892

  Symptoms: Tracebacks such as:

  ```
  %MFIB-3-DECAP_OCE_CREATION_FAILED: Decap OCE creation failed
  ```
  may be seen on a router console when loading an image or during an RP SSO.

  Conditions: The symptom is observed upon reloading a Provider Edge (PE) router with an mVPN configuration or during a simple SSO. It is observed on the standby RP.

  Workaround: There is no workaround.

- CSCtb47647

  Symptoms: Active RP crashes at pim_send_join_prune.

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

  Workaround: There is no workaround.

- CSCtb78752

  Symptoms: A Cisco device crashes when module 1 is reset.

  Conditions: This symptom is observed when the adjacency for the destination IPv6 address lookup is not formed for packets coming into the tunnel interface (leaving the tunnel).

  Workaround:There is no workaround.

  Further Problem Description: After an IPv6 automatic tunnel is established between 2 UUT, when reflexive acl is applied in one of the uuts, and after telneting the ping device configured with the IPv6 address attached to each UUT (ping--uut1--uut2--ping), temporary entries are created in one of the UUTs if the session-closed entries are removed as expected. When module 1 is reset and the telnet session is established, the device crashes.

- CSCtb99914

  Symptoms: The EIGRP VRF configuration is missing in named mode.

  Conditions: This symptom happens only after a power cycle.

  Workaround: Use other modes instead of naming modes. For example:

  ```
  router eigrp 1 address-family ipv4 vrf XX autonomous 1 passive-interface default no
  passive-interface gig1/0/1 no passive-interface vlan133 network ...
  ```
- CSCtc20254

  Symptoms: When the PTA sessions are disconnected from a Cisco router, the active RP logs display an error message and subsequent tracebacks.

  Conditions: This symptom is seen in a prepaid scaling scenario.

  Workaround: There is no workaround.
- CSCtc33679

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

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

  Workaround: There is no workaround.
- CSCtc55897

  Symptoms: R2 will not advertise the routes.

  Conditions: The symptom is observed under the following conditions:

  1. R2 has two IBDG neighbors in the same update-group, one neighbor with 4BAS and the other with 2BAS capability.
  2. The locally originated routes or routes without any AS_PATH will not be advertised to this kind of group.

  Workaround: Try to make the 2BAS and 4BAS neighbors fall into different update-groups by configuring dummy route-maps.
- 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.
- 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: Make sure SESM Account Logon Timeout > RADIUS timeout.

Alternate workaround: Decrease load on external AAA (RADIUS) machines.

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtd33166

  Symptoms: A Cisco router may crash at "parse_call_action_func."

  Conditions: This symptom occurs in "before and after" mode when configuring the Call Home feature.

  Workaround: Turn off "before and after" mode.

- CSCtd45085

  Symptoms: Stale RPs are shown as BIDIR PIM Designated Forwarders.

  Conditions: This symptom is observed after a configuration change, where the same RP is configured as BIDIR mode first, then sparse-dense mode.

  Workaround: Reconfigure the RP in BIDIR mode.

- CSCtd57788

  Symptoms: A dynamic IP ACL is created when a session comes up and is together with the policy private route created according to the "Ascend-Private-Route" downloaded from the user profile. When the session goes down, the route is cleared but the dynamic ACL is not cleared:

  ```
  dge2-18#sh ip access-lists dynamic Extended IP access list pbr#1 10 permit ip any host 10.1.1.1 (5 matches) Extended IP access list pbr#2 10 permit ip any host 10.1.1.1 (5 matches) Extended IP access list pbr#3 10 permit ip any host 10.1.1.1 (25 matches) Extended IP access list pbr#4 10 permit ip any host 10.1.1.1 (25 matches) Extended IP access list pbr#5
  ```

  Conditions: The symptom is observed with routes downloaded from the radius server.

  Workaround: There is no workaround.

- CSCtd57876

  Symptoms: A Cisco router may experience process switching and high CPU utilization.

  Conditions: This symptom is triggered by the removal of **ip nbar protocol-discovery**.

Workaround: Reconfigure **ip nbar protocol-discovery**.

- CSCtd78587

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

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

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

  Workaround: Disable err-disable recovery.

- CSCte01606

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

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

  Workaround: Disable BFD

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

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

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

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

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

- CSCte15193

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

  Conditions: The symptom is observed under the following conditions:

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

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

- CSCte39707

  Symptoms: Supervisor crashes unexpectedly when IPv6 multicast is configured.

  Conditions: This symptom is observed when IPv6 multicast is configured.

  Workaround: There is no workaround.

- CSCte52419

  Symptoms: When an SSS session is created and the command **show sss session identifier authenticated-username** <*string*> is executed, a memory leak is seen.

  Conditions: The symptom is observed when an SSS session exists in the router.

  Workaround: There is no workaround.

- CSCte56437

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

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

  Workaround: There is no workaround.

- CSCte60787

  Symptoms: A 528-byte memory leak is observed for every radius-proxy session.

  Conditions: This symptom is observed upon bringing up and clearing radius- proxy sessions.

  Workaround: There is no workaround.

- CSCte65688

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

  Conditions: The symptom is observed when:

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

  Workaround: There is no workaround.

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

- CSCte74705

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

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

  Workaround: There is no workaround.

- CSCte78406

  Symptoms: The following error message is logged at the new standby RP when PTA sessions are established:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access2.1
  linked to wrong idb Virtual-Access2.1
  ```

  Conditions: The symptom is observed when PTA sessions are established, then an RP switchover is performed. After both RPs sync up, flap the sessions. The error messages are logged at the new standby RP.

  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.

- CSCte89292

  Symptoms: There are ping failures on a Cisco 7600 series router with a linecard.

  Conditions: The symptom is observed on any linecard having a subinterface connection. The following steps trigger the issue:

  1. Have a back-to-back subinterface connection
  2. The local interface should be down/down. (i.e.: admin shutdown on the remote interface)
  3. Do two consecutive **redundancy force-switchover**(s)
  4. "No shutdown" on remote interface
  5. Then ping the remote end from local router on the subinterface.

  Workaround:

  1. Do admin shutdown followed by no shutdown on remote interface
  2. Then ping the remote end from local router on the subinterface. Ping works.

- 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

- 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.

- 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.

- 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 ISGs 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.

- CSCtf34720

  Symptoms: DR will not send a periodic join for an SSM group with a "static- group" configuration on the RPF interface. This will result in the S,G states expiring in the upstream routers and may result in traffic loss.

  Conditions: The symptom is observed when the static-group join is configured on the RPF interfaces and the output interface list of the mroute is NULL.

  Workaround: Add a local join by using **ip igmp join-group** for the same group and source, so that it adds a local interested receiver and sends a periodic join upstream.

- CSCtf36402

  Symptoms: A Cisco router crashes when the user telnets and Transmission Control Block is cleared for that session before entering the password.

  Conditions: This symptom is observed when aaa authentication protocol is set to TACACS.

  Workaround: Do not clear the Transmission Control Block for a session before entering the password.

- CSCtf52106

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

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

  Workaround: There is no workaround.

- CSCtf54561

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

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

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

- 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.

- CSCtf71990

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

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

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

  Workaround: Remove “source-ip-address”.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

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

  ```
  Router 1: interface e0/0 ip address 192.168.1.1 255.255.255.0 bfd interval 51 min_rx
  51 multiplier 4 bfd echo no shut exit
  interface loopback 0 ip address 10.10.1.1 255.255.0.0 exit ip route static bfd e0/0
  192.168.1.2 ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2
  Router 2: interface e0/0 ip address 192.168.1.2 255.255.255.0 bfd interval 51 min_rx
  51 multiplier 4 bfd echo no shut exit
  interface loopback 0 ip address 10.20.1.1 255.255.0.0 exit
  ip route static bfd e0/0 192.168.1.1 ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1
  interface e0/0 no ip route static bfd e0/0 192.168.1.1
  ```

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

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

- CSCtf77047

  Symptoms: Ping ATM subinterface peer IP address has packet loss from Cisco 7206.

  Conditions: This symptom occurs with the following:

  1. NPE-G2+PA-MC-STM-1SMI+PA-A6-OC3SML
  2. Enable EIGRP on ATM subinterface

  Workaround: There is no workaround.

- CSCtf80105

  Symptoms: When basic SIP-SIP calls are placed using automation scripts, calls start failing due to UDP socket connection error

  Conditions: The symptom is observed when the router is configured with a dial peer and with SNMP. A dial peer is most likely required to reproduce the issue, but it is possible that a different UDP protocol other than SNMP could also cause the symptom. Once a call failure occurs, all the calls placed later will fail with a UDP socket connection error.

  Workaround: Use the following steps:

  1. Under sip-ua, configure **connection-reuse** (which is a hidden command)
  2. Configure the use of TCP.

- CSCtf98801

  Symptoms: Tracebacks are seen while doing ISSU:

  ```
  %BIT-SP-STDBY-4-OUTOFRANGE: bit 56073 is not in the expected range of 512 to 8703
  ```
  Conditions: This symptom is observed with ISSU from SRD4 to SRE1

  Workaround: There is no workaround.

- 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.

- CSCtg13269

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

  Conditions: The symptom is observed with BGP RRs.

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

- CSCtg18555

  Symptoms: A memory leak is observed with process_online_diag_pak.

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

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

- CSCtg25798

  Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

  Conditions: The symptom occurs when all of the following conditions are met:

  1. The prefix does not have a label bind (BGP prefixes for example)
  2. There is a static route for the next-hop address pointing to the tunnel only
  3. The router imposes two labels for the next-hop address.

  Workaround: There are three potential workarounds:

  1. Explicit next hop avoiding recursive research: "ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4" (i.e.: breaking rule 2)
  2. Use "neighbor 192.168.1.1 send-label" on both PEs (i.e.: breaking rule 1)
  3. Use "mpls traffic-eng signaling interpret explicit-null verbatim" on P (i.e.: breaking rule 3).

  Further Problem Description: In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

```
PE1#sh mp ld bin 192.168.200.200 32 lib entry: 192.168.200.200/32, rev 35 local
binding: label: 31
PE1#sh ip route 192.168.200.200 Routing entry for 192.168.200.200/32 Known via
"static", distance 1, metric 0 Routing Descriptor Blocks: * 192.168.100.100 Route
metric is 0, traffic share count is 1
```

The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1#sh ip route 192.168.100.100 Routing entry for 192.168.100.100/32 Known via
"static", distance 1, metric 0 (connected) Routing Descriptor Blocks: * directly
connected, via Tunnel10 Route metric is 0, traffic share count is 1
PE1#sh ip cef 192.168.100.100 192.168.100.100/32 attached to Tunnel10 label 26
PE1#sh mp ld bin 192.168.100.100 32 lib entry: 192.168.100.100/32, rev 30 local
binding: label: 29 remote binding: lsr: 192.168.2.2:0, label: 26 remote binding: lsr:
192.168.4.4:0, label: 26 <<<<< tunnel head-end
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1#sh ip cef 192.168.200.200 192.168.200.200/32 nexthop 192.168.100.100 Tunnel10
label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1#trace 192.168.200.200 Type escape sequence to abort. Tracing the route to
192.168.200.200 1 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec 2
192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec 3 192.168.34.4 4 msec 0 msec
0 msec 4 192.168.48.8 4 msec * 4 msec
```

- 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**.

- CSCtg29219

  Symptoms: QoS not working when switching to backup pseudowire.

  Conditions: This symptom is observed on a multi-chassis LAG set up. When switching over from primary to backup pseudowire, QoS applied on the evc is not working. This is because of a mismatch in QoS programming on the member link and the actual member link used for evc flow.

  Workaround: There is no workaround.

- CSCtg35298

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

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

  Workaround: There is no workaround.

- CSCtg37885

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed with 25k VCs when the RSVP and OSPF neighbors are cleared in succession.

  Workaround: Do not clear the RSVP and OSPF neighbors in succession when a high number of VCs exist.

- CSCtg45099

  Symptoms: Router crashes.

  Conditions: The symptom is observed when the **show cca** command is issued.

  Workaround: There is no workaround.

- CSCtg49331

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

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

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

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

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

- CSCtg58786

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

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

  Workaround: There is no workaround.

- CSCtg60065

  Symptoms: DLFIoATM back-to-back ping fails for AAL5MUX encapsulation.

  Conditions: The symptom is observed when you configure DLFIoATM with encapsulation AAL5MUX.

  Workaround: There is no workaround.

  Further Problem Description: Issue is not seen when you configure for AAL5SNAP.

- CSCtg60201

  Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.

  Conditions: This symptom is observed if addition-path install is configured along with the **maximum-path** command.

  Workaround: Reconfigure “bgp additional-path install.”

- CSCtg64175

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

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

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

- CSCtg65989

  Symptoms: Only the first user is able to get authenticated successfully and browse the internet. All subsequent users are constantly redirected to the web portal after successful authentication. The **show sss sess uid xxx** command shows that the internet service is not applied to the account even though the session is authenticated.

  Conditions: The symptom is observed with customers using web logon with a session applying an auto service.

Workaround: Remove “autoservice” and apply static service at account logon.

- CSCtg73456

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

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

  Workaround: There is no workaround.

- CSCtg74946

  Symptoms: QoS counters are stuck at “0.”

  Conditions: This symptom is observed with SSO and when dlfi is configured over ATM.

  Workaround: Detach and re-attach the service-policy.

- CSCtg76688

  Symptoms: An active Cisco route processor reloads in a scale scenario (16k - 24k sessions) when the **clear subscriber session all** command is entered.

  Conditions: This symptom is observed only when there are 16k-24k sessions and the **clear subscriber session all** command is entered.

  Workaround: Do not enter the **clear subscriber session all** command when more than 16k sessions are up on the router.

- 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.

- CSCtg89555

  Symptoms: There is no forwarding interface seen in the mfib output on a DFC.

  Conditions: This symptom is observed when configuring an ip address after multicast has been configured on a dot1Q interface.

  Workaround: Performing a **shut/no shut** of the interface will fix the problem.

- 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).

- CSCtg98116

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

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

  Workaround: There is no workaround.

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

- CSCth00317

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

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

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

  Alternate Workaround: Reset the linecard on configuration of the port-channel.

- CSCth01394

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

  Conditions: This issue is consistently reproducible.

  Workaround: There is no workaround.

- CSCth01526

  Symptoms: MDT interface deactivated and activated after an SSO.

  Conditions: After an SSO switchover, the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

  Workaround: There is no workaround.

- CSCth02725

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

  Conditions: The symptom is observed in the following scenario:

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

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

- CSCth02812

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

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

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

- CSCth05476

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

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

  Workaround: There is no workaround.

- 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.

- CSCth11747

  Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

  Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

  Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTS CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- 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.

- CSCth15105

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

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

  Workaround: There is no workaround.

- CSCth16011

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

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- CSCth18571

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

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

  Workaround: There is no workaround.

- CSCth23787

  Symptom: A Cisco router crashes at mcast_aaa_send_stop_acct_event.

  Conditions: This symptom is observed while unconfiguring “ipv6 mld join-group FF1E:7777:7777::1” in the client after configuring within 15-20 seconds.

  Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth29393

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

  Conditions: The symptom is observed with the **show sss session detail** command with PXF output.

  Workaround: Clear the affected SSS session.

- CSCth31271

  Symptoms: A Cisco ASR router crashes with next-hop recursive.

  Conditions: This symptom is observed after the following tasks are executed:

  1. Configure a route-map with recursive next-hop clause for ip address (for example, 1.2.3.4)
  2. Change the recursive next-hop to ip address (for example, 5.6.7.8)
  3. Apply PBR with this route-map to an interface
  4. Delete the route-map
  5. Shut the interface.

  Workaround: There is no workaround.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

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

  Workaround: There is no workaround.

- CSCth35356

  Symptoms: DHCP relay/server stops working and multiple DHCP processes are created.

  Conditions: The symptom is observed when fragmented DHCP packets are received.

  Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4. - eBGP + VPNv4 peer session is established and DUT.
  - Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth37998

  Symptoms: WEB logon always fails after one failed account logon.

  Conditions: The symptom is observed after a failed account logon.

  Workaround: There is no workaround.

- CSCth38699

  Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

Workaround: Configure static RP-to-Group mappings.

- 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.

- CSCth42798

  Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

  Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

  Workaround: There is no workaround.

- CSCth46888

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

  Conditions: The 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.

- CSCth47888

  Symptoms: In a Hot-Standby psuedowire redundancy setup, traffic is forwarded on the Standby psuedowire instead of the Active psuedowire which is in up/up state.

  Conditions: This symptom is seen in a Cisco 7600 router that is running Cisco IOS Release 15.0(1)S with hot psuedowire redundancy configuration.

  Workaround: There is no workaround.

- CSCth55383

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

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

  Workaround: There is no workaround.

- CSCth55689

  Symptoms: If you do a **clear xconnect** before the primary VC has come up, the system erroneously brings up PW on the backup VC.

Conditions: The symptom is observed if you do a **clear xconnect** before PW establishment.

Workaround: Use the following command:

clear xconnect peer *peer-ip* **vcid** *vcid-id*.

- CSCth60232

  Symptoms: The port-channel interface may flap when adding or removing a VLAN from the trunk on a port-channel interface when one or more interfaces are in a state other than P or D.

  Conditions: This symptom is observed only when the port-channel interface has interfaces in states other than P or D.

  Workaround: Shut down the non-P members and make the vlan changes.

- CSCth62854

  Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

  Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

  Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth65072

  Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

  Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

  Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth66246

  Symptoms: A configuration sync issue and stand-by reload occur when configuring and removing the ip slb sticky feature.

  Conditions: This symptom is observed in the Cisco IOS Release 15.1(00.10)S image.

  Workaround: There is no workaround.

- CSCth69469

  Symptoms: ICMP filtering is not working in an SACL configuration.

  Conditions: This symptom is observed when ACE is configured with icmp options.

  Workaround: There is no workaround.

- CSCth69504

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

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

  Workaround: Disable IGMP snooping either globally or per VLAN.

- CSCth69364

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCth69588

  Symptoms: Disposition traffic does not flow across ES+ cards. Imposition traffic for sceompls works fine.

  Conditions: This symptom is observed with ES+ card mainly on switchover, reprovisioning of circuits, etc.

  Workaround: Enter the **clear xconnect all** command on the device and wait for reprovision. Once all circuits are up, traffic will flow across fine.

- 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.

- CSCth71349

  Symptoms: Some SSS sessions are staying in “attempting” state for a while when using ISG Static Session Creation.

  Conditions: The symptom is observed when using ISG Static Session Creation.

  Workaround: Stop incoming traffic from subscribers and wait until the sessions recover, then re-apply the traffic.

- CSCth72290

  Symptoms: Traffic over PPPoMPLS drops continuously on a SIP400 with microcode reload.

  Conditions: The symptom is observed when PPPoMPLS is configured over any interface on a channelized SPA on SIP400 and following a microcode reload of the linecard.

  Workaround: Reload the SPA.

  Further Problem Description: When PPPoMPLS is configured on an channelized interface the encapsulation for that interface on the linecard is PPP where as the SPA encapsulation is HDLC as the SPA just tunnels the packets through. After the microcode reload, the linecard queries the SPA for a connection ID for the channelized interface with encapsulation as PPP but as the SPA encapsulation set is HDLC the SPA does not give any connection ID to the SIP400 and hence the traffic starts to drop after a reload.

- CSCth72565

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

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

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

  Workaround 2: Avoid ECMP by altering link cost.

- CSCth72765

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

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

Workaround: There is no workaround.

- CSCth73173

  Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

  Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

  Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCth75354

  Symptoms: There is an intermittent problem when a SPAN source is set to be a VLAN. The destination in the SPAN session does not receive the data.

  Conditions: The symptom is observed on a Cisco 7600 series router with an ES+20 card that is running Cisco IOS Release is 12.2(33)SRE0.

  Workaround: Reload the module.

- CSCth77531

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU utilization in the BGP-related processes for several hours (more than 2.5).

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process uses the most CPU; also, the number of routemap-cache entries should be very high.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
  main routing table version 1228001 604000 network entries using 106304000 bytes of
  memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
  attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
  of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
  cache entries using 4565920 bytes of memory
  ```

  Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results, and the issue will not be observed.

- CSCth78148

  Symptom: Cannot attach to 8XCHT1/E1 SPA console.

  Conditions: This issue is observed after configuring SSO.

  Workaround: Reload the SPA.

- CSCth79336

  Symptoms: Ingress QoS policy, when applied on an EVC configured on port- channel, is getting configured for only one of the NPs, instead of all of the NPs that have member-links belonging to the port-channel. If traffic enters the port-channel via multiple member-links, provided the member-links belong to different NPs, ingress QoS will be applied on only one of the member-links.

  Conditions: This symptom is observed when EVC is configured on port-channel.

  Workaround: There is no workaround.

- CSCth80166

  Symptoms: EVCs belonging to the same group are mapped to different member links, and the packets are forwarded over different member links.

  Conditions: This symptom is observed when dynamic changes such as adding an EVC to a group or removing it are made; all the group members are not mapped to the same member link.

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

- CSCth81950

  Symptoms: A memory leak occurs in ES+ cards.

  Conditions: This symptom is observed on a Cisco 7600 with the cac enabled.

  Workaround: There is no workaround.

- CSCth82486

  Symptoms: A SIP600 crashes.

  Conditions: The symptom is observed following an OIR of the active supervisor.

  Workaround: There is no workaround.

- CSCth84995

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

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

  Workaround: There is no workaround.

- CSCth85294

  Symptoms: A PIM neighborship not established with the remote PE and RP for the MVRFs.

  Conditions: This symptom is observed with traffic, after removal and restoration of mvrfs. Traffic does not flow properly since the PIM neighborship is not established with the remote PE and RP for those MVRFs.

  Workaround: There is no workaround.

- CSCth85449

  Symptoms: Interfaces on SIP-400 may experience .9% packet loss in the LLQ when priority percent is configured.

  Conditions: This symptom is observed on a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRE when the low latency queue traffic is allowed to grow past its configured percentage. This condition only occurs when the interface has greater than 85% utilization.

  Workaround: There is no workaround.

- CSCth86402

  Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

  Conditions: This happens when flapping a WAN interface after a few hours of working.

  Workaround: Disable multicast routing, then enable it again.

- CSCth87132

  Symptoms: Diagnostic tests may fail on an ES+ linecard with the following message:

  ```
  Mandatory.go_fabrich0.tcl: GOLD EEM TCL policy for TestFabricCh0Health
  ```

  Conditions: This symptom is observed when 802.1 TAP MIB is used to tap based on an if_index belonging to an “access” interface.

  Workaround: IP-TAP mib may be used instead of 802.1 TAP MIB.

- CSCth87195

  Symptoms: Flexwan ATM interface goes down.

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

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

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth90001

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

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

  Workaround: Use L3 802.1q subinterface configuration.

- CSCth92171

  Symptoms: The serial interface stays down longer if a switchover is done while flapping the multilink interface from the far end.

  Conditions: This symptom is observed when switching over to the standby while flapping the multilink interface from the far end.

  Workaround: Shut the flapping links, then perform the switchover.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” displays on PfR BR.

  Conditions: The symptom is observed in a scale setup with many PfR application prefixes and when PfR optimizes the application prefixes.

  Workaround: There is no workaround.

- CSCth94814

  Symptoms: Crash is seen in static route component.

  Conditions: The symptom is observed when changing IVRF on a virtual-template when there are about 100 active sessions.

  Workaround: There is no workaround.

- CSCth94827

  Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima-group on a SONET-ACR controller.

  Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

  Workaround: There is no workaround.

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

Conditions: The symptom is observed under the following conditions:

1. If the client starts to send LCP echo requests during the PPP Authentication phase
2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

Workaround: There is no workaround.

- 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.

- CSCti01036

  Symptoms: A Cisco ASR1000 series router crashes on the Radius Process.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router with Radius AAA services enabled. When the Radius server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

  Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti01971

  Symptoms: The active router crashes during a switchover in a scaled BFD IPv6 setup.

  Conditions: The router is configured with a larger number of IPv6 routes with BFD sessions configured. (The test was done with 500 BFD IPv6 sessions.)

  Workaround: There is no workaround.

- CSCti04678

  Symptom: 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 attempting state forever.

  Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

  Workaround: Clear attempting state sessions by the **clear** command from box.

- CSCti05663

  Symptoms: A DHCP ACK which is sent out in response to a renew gets dropped at relay.

  Conditions: The symptom is observed in the case of an numbered relay.

  Workaround: There is no workaround.

- CSCti08115

  Symptoms: The removal of a port-channel interface associated with **mpls ldp advertise-labels interface Port-channelN** can cause a “config sync” error upon an SSO.

  Conditions: The symptom is observed after doing an SSO following the removal of the port-channel interface.

Workaround: Before the SSO, remove the offending advertise-labels command when removing the port-channel command with:

no interface Port-channelN no mpls ldp advertise-labels interface Port-channelN

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are "IN" policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go "Out" of policy.

  Workaround: There is no workaround.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip version 2 no validate-update-source network 10.0.0.0 no auto-summary !
  address-family ipv4 vrf test no validate-update-source network 172.16.0.0 no
  auto-summary version 2 exit-address-family
  ```
  and doing a reload causes the "no validate-update-source" statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

  Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti14290

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

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

  1. Determine the BGP VPN Label for the prefix

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

  ```
  router# sh ip cef vrf test 10.1.1.1 detail 10.1.1.0/24, epoch 13 local label info:
  other/4828 <=== label is 4828 recursive via 10.100.1.2 attached to GigabitEthernet1/1
  ```
  2. Determine the hardware forwarding for the prefix on the Supervisor

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

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

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

show mls cef adjacency entry *entry id*

```
DRCORL02#sh mls cef adjacency entry 213683 detail
Index: 213683 smac: 0000.0000.0000, dmac: 00d0.2b12.5500 mtu: 65535, vlan: 1024,
dindex: 0x7FFA, l3rw_vld: 1 format: MPLS, flags: 0x1000008600 label0: 0, exp: 0, ovr:
0 label1: 0, exp: 0, ovr: 0 label2: 0, exp: 0, ovr: 0 op: POP packets: 0, bytes: 0
```

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

remote login module *module number*

```
Router# remote login module 1 Trying Switch ... Entering CONSOLE for Switch Type
"^C^C^C" to end this session
Router-dfc1#sh mls cef mpls label 4828 detail Codes: M - mask entry, V - value entry,
A - adjacency index, P - FIB Priority D - FIB Don't short-cut, m - mod-num, E - ELSP?
Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2 eos2)
V(1301 ): B | 1 0 0 0 0 4828 0 1 0 0 0 0 (A:147570 ,P:0,D:0,m:0 :E:1) M(1301 ): F | 1
FFF 0 0 1 FFFFF 0 1 0 0
0 0 Router-dfc1#sh mls cef adjacency entry 147570 detail Index: 147570 smac:
0000.0000.0000, dmac: 0000.138b.0000 mtu: 65535, vlan: 1024, dindex: 0x7FFA, l3rw_vld:
1 format: MPLS, flags: 0x1000008600 label0: 0, exp: 0, ovr: 0 label1: 0, exp: 0, ovr:
0 label2: 0, exp: 0, ovr: 0 op: POP packets: 59, bytes: 24025
```

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

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

hw-module module <module number> reset

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message "learning writing data". The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti24657

  Symptoms: Fabric CRC errors, fabric sync errors, fabric minor/major errors, Signal Integrity issues over the fabric channel, as well as Blackwater queue stall. Sample error messages:

```
%FABRIC_INTF_ASIC-DFC9-5-FABRICSYNC_DONE: Fabric ASIC 0 Channel 1: Fabric sync done.
%FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 5 reported timeout error for channel 8
(Module 9, fabric connection 0)
%DFCWLC-DFC9-3-GEN_DEV_ERR: Blackwater unexpected error: PXF(0) Feature Queue(23)
wedged. Initiating LC reset to recover.
```

  Conditions: These symptoms are observed on ES20 linecards with Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload when receiving certain SNMP packets from an authenticated user. Successful exploitation may cause the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Conditions: Cisco IOS device configured for SNMP. Authentication is required to cause a device reload.

  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

- 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.

- CSCti26768

  Symptoms: A Cisco 6500 router configured with a PKI trustpoint could reload due to bus error.

  Conditions: This symptom is observed when following the steps for a trustpoint configuration: removal, reconfiguration, authentication, enrollment.

  Workaround: There is no workaround.

- CSCti32641

  Symptoms: A Cisco ASR 1004 (RP2) router is not able to establish an LDP session to a 3rd-party device and receives an Error Notification (0x07) Bad TLV Length message from that device.

  Conditions: This symptom is observed on a Cisco ASR 1004 with Cisco IOS Release 15.0(1)S when LDP ICCP capability TLV (0x405) is supported on the router.

  Workaround: There is no workaround.

  Further Problem Description: It seems that Cisco ASR 1004 routers send to the peer a malformed ICCP capability TLV (0x405).

- CSCti34396

  Symptoms: The router distributes an unreachable nexthop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: The symptom is seen when "next-hop-unchanged allpaths" is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is an unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the nexthop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10 match source-protocol static set ip
next-hop <router ip address> ! router bgp <asn> address-family ipv4 vrf <vrf name>
redistribute static route-map static-nexthop-rewrite exit-address-family exit exit
```

Alternate Workaround: Instead of configuring static routes with a next-hop, specify an interface name.

For example, if you had: ip route x.x.x.x 255.255.255.0 y.y.y.y And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with: ip route x.x.x.x 255.255.255.0 interface serial2/0

Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

When used in conjunction with the newly added configuration:

router bgp *<asn>* **address-family vpnv4 unicast bgp route-map priority**

The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti34462

  Symptoms: After FPD upgrade, a **shut** on the active shows **no shut** on the standby.

  Conditions: The symptom is observed after an FPD upgrade.

  Workaround: Perform a **no shut** then shut the interface on the active to sync it properly.

- CSCti34627

  Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

  Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

  Workaround: Disable GR.

- CSCti35170

  Symptoms: With REP over EVC configured and a high volume of traffic, REP could flap due to REP Hellos getting dropped.

  Conditions: This condition is observed only when a high volume of traffic (mostly priority traffic) is sent on the interface.

  Workaround: There is no workaround.

- CSCti37533

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed with a half-inserted standby card that generates an internal stall; if this stall continues for more than 30 seconds, a crash occurs.

  Workaround: Remove or fully insert the standby card.

- CSCti41910

  Symptoms: Changes to the spanning-tree mst instance configuration are not synced to a standby SP. Hence, after a switchover, the new Active will have old MST instance configuration on SP.

  Conditions: The symptom is observed after completing the following steps:

  1. Configure MST instance configuration

(config)#spanning-tree mst configuration (config-mst)#instance 1 vlan 102

2. Do HA switchover
3. “Show spanning-tree mst configuration” on active SP will not show ’instance 1’ in configuration.

Workaround: Reload the standby.

Further Problems Description: Bulk sync for MST configuration works fine. Only the incremental configuration sync is broken.

- CSCti43395

  Symptoms: Tracebacks are seen during DHCP message exchange. Crash may also be seen with the tracebacks.

  Conditions: This symptom is seen when DHCP relay agent is configured with “ip dhcp relay information option vpn” and clients with duplicate MAC address are coming in at the same time.

  Workaround: Unconfigure “ip dhcp relay information option vpn”. Or, disallow clients with duplicate MAC.

- CSCti45732

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

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

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

- CSCti47158

  Symptoms: When configuring the T1 channels on the SPA-2CHT3-CE-ATM/CHOC3-ATM on a SIP-400 on a Cisco 7600 series router, the T1 remains in a “Down” state.

  Conditions: The symptom is observed under the following conditions:

  – Seen on a Cisco 7600 series router with SIP-400 and SPA-2CHT3-CE-ATM/CHOC3- ATM.
  – Seen when the configuration is done using copy and paste, or using a script.

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

- CSCti47550

  Symptoms: With a scaled L3 ACL on EVC on ES+ linecards, some of the ACEs do not work, while others work as normal.

  Conditions: The symptom is observed when the linecard or router is reloaded with the ACL configuration present.

  Workaround: Remove and add ACL on the EVC.

- CSCti49508

  Symptoms: The command **show platform isg session all** displays stale entries on a Cisco 7600 series router for ISG sessions that are not on the router.

  Conditions: This symptom is observed under the following conditions:

  1. A number of port channel subinterfaces are configured with ISG
  2. ISG sessions are active on the subinterfaces

3. The main port channel is removed without removing the sessions or ISG configuration from the individual port channel subinterfaces, using the “no interface port-channel <>” command

Workaround: There is no workaround.

To avoid this symptom, Delete the session/ISG configuration from the individual port channel subinterface, then delete the port channel.

- CSCti50419

  Symptoms: For PPPoMPLS/HDLCoMPLS pseudowires, after you perform the switchover, traffic loss is seen and CE interfaces stay down.

  Conditions: The symptom is observed on performing an SSO switchover with PPPoMPLS and HDLCoMPLS pseudowires. The control word gets programmed incorrectly on the linecard leading to traffic loss.

  Workaround: Unprovision and provision the pseudowire.

  Alternate Workaround: Perform a SPA OIR.

- CSCti50607

  Symptoms: A Cisco 7200 SRE1 router drops GRE packet size 36-45.

  Conditions: The symptom is observed on a Cisco 7200 series router with SRE1 code.

  Workaround: There is no workaround.

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  – The non-reloading device must have a “neighbor x.x.x.x transport connection- mode passive” configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword ’established’ or “eq bgp”

  – It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload

  – When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages

  – Both peers must be multisession capable

  – “transport multi-session” must not be configured on either device, or enabled by default on either device

  – “graceful restart” must not be configured.

  Workarounds:

  1. Remove the configuration “neighbor x.x.x.x transport connection-mode passive” or edit the corresponding filter or ip access list to permit the active TCP opens in both directions
  2. Configure “neighbor x.x.x.x transport multi-session” on either the device or its neighbor
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the **neighbor x.x.x.x timers 1 holdtime** command
  4. Configure graceful restart using the command **neighbor x.x.x.x ha- mode graceful-restart**

5. 5. If the issue occurs, use the **clear ip bgp *** command to cause all sessions stuck in the NoNeg state to restart. You can also use **clear ip bgp x.x.x.x addressFamily** to bring up individual stuck sessions without resetting everything else.

Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where "neighbor x.x.x.x transport single-session" is configured and NSF is not configured.

The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS 12.2(33)SB-based releases if the 12.2(33)SB router is the one not reloading.

- CSCti53664

  Symptom: CoPP hardware counters not incrementing when **sh policy-map control-plane** command is run for traffic coming on ES20+ cards.

  Conditions: This symptom is observed when CoPP is configured and traffic is coming in on ES20+, which is destined to switch the ip address.

  Workaround: Move the l3 interface from the switch for the traffic coming in on ES20+ line cards.

- CSCti56980

  Symptoms: Applying a service-policy under an interface or subinterface on an ES+ card in a Cisco 7600 series router may fail with the following error:

  random-detect aggregate is not supported in output direction for this interface Configuration failed!

  Conditions: The symptom only occurs when a SIP400 is being replaced by an ES+ card on which the QoS configuration will be applied.

  Workaround: Reload the router with the ES+ card installed.

- CSCti61949

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

  Conditions: The symptom is observed when receiving BGP updates from a speaker for a multicast-enabled VRF.

  Workaround: Disable multicast routing on VRFs participating in BGP or reduce the number of extended communities used as route-target export.

- CSCti62125

  Symptoms: When a Cisco 67XX card is inserted in slot 2 of a Cisco 7606-S chassis, then other cards (such as ES+, ES, and SIP) in the other slot face fabric CRC errors. The ES+ in the other slot gets hung and leads to a crash.

  Conditions: The symptom is observed when a Cisco 67XX card is inserted in slot 2 of a Cisco 7606-S chassis.

  Workaround: There is no workaround.

- CSCti65716

  Symptoms: The access interface connecting to the client is on global routing domain. If a service logon profile on a VRF is downloaded to the client, the client could potentially stay on a VRF even when a service logoff is performed later. The client traffic has to return to global domain when a service logoff is performed.

  Conditions: This symptom is see when access interface is on global routing domain. Service logon is on a VRF.

  Workaround: There is no workaround.

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used
  - Use HSRP with sub-interfaces on ES20 module
  - Reload the ES20 module

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. Reconfigure HSRP on all subinterfaces
  2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti67429

  Symptoms: A REP segment configured on 7600-ES+20G3CXL interfaces on a Cisco 7600 series router that is running Cisco IOS Release 15.0(1)S is not recovering as expected upon link failure recovery of the edge port configured on the 7600. A traffic storm triggered by ISIS protocol configured between 7600 and the MWR 2941s in the REP ring is occurring when the failed REP edge port becomes operational again.

  Conditions: The symptom is observed with a REP ring including two Cisco 7600 series routers equipped 7600-ES+20G3CXL and running Cisco IOS Release 15.0(1) S configured with ISIS and MPLS LDP. The problem is also present in Cisco IOS Release 12.2(33)SRE1.

  Workaround: Configure static routes between the 7600 routers and the MWR 2941s instead of ISIS.

- CSCti67447

  Symptoms: During an SSO, an 8 to 12 second packet drop may occur on EoMPLS VCs.

  Conditions: The symptom is observed under the following conditions:

  1. EoMPLS port-based or VLAN-based configuration; VC between PE1 and PE2
  2. Enable MPLS LDP GR.

  Workaround: There is no workaround.

- CSCti68153

  Symptoms: QinQ packet header is modified, breaking QinQ.

  Conditions: This occurs when you use an ES+ card on a Cisco 7600 series router where the pseudowire encapsulation begins.

  Workaround: Use double VLAN tagging before the packet gets to the ES+ card so that when it pops the first VLAN tag it will modify the second dummy tag and not the actual payload.

Further Problem Description: This issue is not seen on ES20 card.

- CSCti68721

  Symptoms: The output of show performance monitor history interval <all | given #> will appear to have an extra column part way through the output.

  Conditions: This symptom is observed sporadically while traffic is running on a performance monitor policy at the time when a user initiates the CLI show command.

  Workaround: If the symptom occurs, repeat the command.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: Dampening configuration changes for VRFs.

  Workaround: There is no workaround.

- CSCti72498

  Symptom: A crash occurs on a device acting as DHCP Server.

  Conditions: This symptom is observed when a requested IP address option is present in DHCP requests.

  Workaround: Disable the DHCP ping check with the help of CLI “ip dhcp ping packets 0."

- CSCti74736

  Symptoms: A traffic drop might appear on a GREoMPLS tunnel after an SSO switchover in an egress direction. If an ingress interface is located on a SIP400 series linecard, the following error message will be continuously printed:

  `%INTR_MGR-3-BURST: HY_FD_PP_EC_EC_ERR_INT[0x1] bad payload CRC exceeds threshold`
  Conditions: The presence of “mls mpls tunnel-recir” is required for the GREoMPLS feature to work. After the second SSO switchover since bootup, the command will be inactive and the feature broken. The issue is applicable to Cisco IOS Release 12.2(33)SRE2, but not to Release 12.2(33)SRE1.

  Workaround: Reload the router.

- CSCti74962

  Symptoms: `“%PM-SP-4-PORT_BOUNCED: bounced by Consistency Check IDBS UP”` message seen on A3-1 new active router after linecard OIR followed by an SSO switchover.

  Conditions: This symptom will occur only with a linecard OIR followed by an SSO switchover.

  Workaround: There is no workaround.

- CSCti77521

  Symptoms: Policy-map is not attached to a DLFIoATM interface after a SPA OIR.

  Conditions: The symptom is observed upon performing a SPA OIR. The issue is seen with ATM SPA on a SIP400.

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

- CSCti81444

  Symptoms: Traffic does not flow in egress direction over VPLS PW on router reload.

  Conditions: The symptom is observed after a router reload. POE bits for the imposition interface are not getting programmed on the egress linecard.

  Workaround: There is no workaround.

- CSCti83705

  Symptoms: IPv4 unicast traffic not forwarded out of a Cisco 7600 series router's GREoMPLS in VRF tunnel.

  Conditions: The symptom is observed with an IPv6 Address Family (AF) configured under VRF. If the IPv6 AF is in the startup configuration then the feature is broken straight after boot up. If the IPv6 AF is configured after boot up, then feature gets broken after this configuration.

  Workaround: Remove IPv6 AF from the tunnel's VRF.

- CSCti83737

  Symptom: SIP-600 will crash with a software-forced crash:

  ```
  Aug 29 06:11:05 UTC: DFC7: sip10g_tefrr_program_vc_list() TMEM_ASSERT failed on line
  5692 %Software-forced reload
  06:11:05 UTC Sun Aug 29 2010: Breakpoint exception, CPU signal 23, PC = 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on SIP-600.

  Workaround: There is no workaround.

- CSCti85446

  Symptoms: A nexthop static route is not added to RIB even though the nexthop IP address is reachable.

  Conditions: The symptom is observed with the following conditions:

  1. Configure a nexthop static route with permanent keyword
  2. Make the nexthop IP address unreachable (e.g.: by shutting the corresponding interface)
  3. Change the configuration in such a way that nexthop is reachable
  4. Configure a new static route through the same nexthop IP address used in step 1.

  Workaround: Delete all the static routes through the affected nexthop and add them back.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the "no service dhcp" command is configured.

  Workaround: There is no workaround.

- CSCti88062

  Symptoms: Traffic stops flowing through ports configured with REP over EVC BD when an ES20 linecard is replaced by an ES+ in the same slot.

  Conditions: The symptom is observed on a router running MST, having an ES20 card configured with EVC BD which is replaced by an ES+ in the same slot with an EVC BD configuration. MST puts the BD VLAN in a disabled state and the traffic on that VLAN stops flowing.

  Workaround: Reload the router.

- CSCti97759

  Symptoms: IPSG configuration with DHCP snooping entry configuration causes the RP to crash.

  Conditions: This is seen when DHCP static entry is configured.

  Workaround: There is no workaround.

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj01623

  Symptoms: REP topology stays incomplete after manual preemption. When the issue occurs, REP preemption will not take effect.

  Conditions: The symptom can be observed for EVC or switchport.

  Workaround: There is no workaround.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj05591

  Symptoms: Memory corruption and SP crash seen.

  Conditions: The symptom is observed when creating 600 subinterfaces as OIF for Mroute entries.

  Workaround: There is no workaround.

- CSCtj08533

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

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

  Workaround: Use only one path between PE and CPE.

- CSCtj15265

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

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

  Workaround: There is no workaround.

- CSCtj15805

  Symptoms: Keepalive functionality not working. An ICMP echo reply coming back from a client is ignored by ISG.

  Conditions: The symptom is observed when a VRF mapping service is used.

  Workaround: There is no workaround.

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP- FIN to the receiving speaker, when receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: The symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  template peer-session ce-v4 transport connection-mode passive

- CSCtj17561

  Symptoms: Description for T1 broken in Prowler/Chopper SDH > C-11 mode. This might lead to sync issues while switching over.

  Conditions: The symptom is observed in SDH > C-11 mode.

  Workaround: There is no workaround.

- CSCtj18622

  Symptoms: The “disperser” feature is not working when it is pushed through AV_Pair by a RADIUS server; either Cisco ACS or a third party vendor’s server.

  Conditions: The symptom is observed with non-multilink PPP users.

  Workaround: There is no workaround.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is done:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0 data 5905A0A8
  chunkmagic 120000 chunk_freemagic 4B310CC0 -Process= “BGP Scanner”, ipl= 0, pid= 549
  with call stack 0x41AC033C:chunk_refcount(0x41ac02ec)+0x50
  0x403A44E0:bgp_perform_general_scan(0x403a3e2c)+0x6b4
  0x403A4E84:bgp_scanner(0x403a4c50)+0x234
  ```

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

  ```
  Router# show ip bgp sum
  BGP router identifier 10.0.0.1, local AS number 65000 BGP table version is 1228001,
  main routing table version 1228001 604000 network entries using 106304000 bytes of
  memory 604000 path entries using 31408000 bytes of memory 762/382 BGP path/bestpath
  attribute entries using 94488 bytes of memory 381 BGP AS-PATH entries using 9144 bytes
  of memory 382 BGP community entries using 9168 bytes of memory 142685 BGP route-map
  cache entries using 4565920 bytes of memory
  ```

  The **clear ip bgp *** command is not a very common operation in production network.

  Workaround: Use **no bgp route-map-cache**. This will not cache the route-map cache results and the issue will not be observed.

- CSCtj25243

  Symptoms: If non-LLQ or parent (logical) is rate-limited and oversubscribed, this can cause some policer drops in the LLQ queue, if LLQ exceeds the bandwidth allocated to it.

  Conditions: The symptom is observed if non-LLQ or parent (logical) is rate- limited and oversubscribed and if LLQ exceeds the bandwidth allocated to it.

  Workaround: There is no workaround.

  Further Problem Description: This issue is caused by CSCth85449. That caveat was intended to detect congestion on the physical interface and police LLQ traffic if it exceeds the configured bandwidth and the physical link is congested.

- CSCtj28696

  Symptoms: Session QoS will not get applied after an OIR of the linecard.

  Conditions: The symptom is observed with sessions (with QoS) on a port- channel subinterface.

  Workaround: Clear session and bring up again.

- CSCtj28747

  Symptoms: Route control of prefix and application are out-of-order thereby making application control ineffective. As a result, an “Exit Mismatch” message will be logged on the MC and the application will be uncontrolled for a few seconds after it is controlled.

  Conditions: The symptom is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR. PIRO control is used when the routing protocol is not BGP, STATIC, or EIGRP, or when two BRs have different routing protocol, i.e.: one has BGP and the other has EIGRP.

  Workaround: There is no workaround.

- CSCtj30155

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

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

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  router eigrp 1 redistribute connected no redistribute connected

  The **no redistribute connected** command is not being backed up to the standby.

  Conditions: The symptom is observed with any redistribute-related commands.

  Workaround: There is no workaround.

- CSCtj35573

  Symptoms: When an interface is configured as an access interface, back-to-back ping will fail.

  Conditions: The ping failure is seen only for access interfaces intermittently. This issue is observed with the SRE2 image with SUP720 and ES+ card, in a situation when the ping packet coming from source has the BPDU bit set.

  Workaround: There is no workaround.

- CSCtj36521

  Symptoms: IPv4 MFIB stays enabled on interfaces even when IPv4 CEF is disabled. The output of the **show ip mfib interface** command shows the interface as configured and available, when it should be disabled.

  Conditions: The symptom is observed only if IPv6 CEF is enabled at the same time.

  Workaround: Make sure IPv6 CEF is always disabled when running only IPv4 multicast. There is no workaround if running a mixed IPv4/IPv6 environment.

- CSCtj38606

  Symptoms: The following error message is seen:

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

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

Hazard Illegal packet length = 7580

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

Workaround: There is no workaround.

- CSCtj41215

  Symptoms: On an ES+, a service instance configuration is rejected with following error:

  Service instance configuration Failed. Service-Policy has already been configured on this interface

  Conditions: The symptom is observed when an ES+ is inserted in the same slot where an ES20 was previously present.

  Workaround: Unconfigure service-policy from the interface and then create a service instance.

- CSCtj44237

  Symptom: High CPU observed in RP.

  Conditions: The symptom is observed with MVPN configurations.

  Workaround: There is no workaround.

- CSCtj45571

  Symptoms: If OAM VC state reaches to “AIS/RDI” after PVC is flapping, then OAM Loopback status gets stuck in “OAM failed” state. Loopback cell is not generated until shut/no shut is performed on the subinterface.

  Conditions: The symptom is observed when the OAM VC state reaches “AIS/RDI”.

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

- CSCtj46297

  Symptoms: Ping fails when performing a shut/no shut on the outgoing interface in an FRR setup.

  Conditions: The symptom is observed in an FRR setup when performing a shut/no shut on the outgoing interface.

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

- CSCtj50072

  Symptoms: High CPU interrupt level caused by IPv4 unicast or multicast traffic received via GREoIP or GREoMPLS tunnel if rate is high. If ingress interface is tunnel and egress is tunnel (MDT included) as well, then outer IP ToS of egress packet will be reset to 0x0.

  Conditions: The symptom is observed after a reload (under 10% probability), GRE tunnel must be in VRF:

  ```
  #show running-config interface tunnel 513 interface Tunnel513 vrf forwarding REN ip address 10.0.2.1 255.255.255.0 ip pim sparse-mode tunnel source Loopback513 tunnel destination 10.0.113.2 (via IP or MPLS interface) tunnel vrf REN end
  ```
  To confirm hit:

  ```
  #show vlan internal usage | include Tunnel513 4074 Tunnel513
  #remote command switch show mls vlan-ram 4074 4074 (If there is 256, the defect is present)
  ```
  Workaround: Reload the router.

- CSCtj52865

  Symptoms: Unable to utilize 16 queues per lowq port.

Conditions: If you remove any QoS policy on subtargets of lowq port, because of stale lowq count on the **show platform lowq** command, we will not be able to use maximum number of queues per lowq port.

Workaround: Only reloading the router resolves the issue.

- CSCtj53299

  Symptoms: Met corruption issue is observed.

  Conditions: This symptom occurs during OIF churn.

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

- CSCtj58943

  Symptoms: Standby RP reloads due to line by line sync failure for **encapsulation dot1q 1381** command:

  Config Sync: Line-by-Line sync verifying failure on command: encap dot1Q 1381 due to parser return error

  ```
  rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync, Reason:
  Configuration mismatch
  ```

  Conditions: Symptom occurs when issuing a configuration command under a sub-interface mode.

  Workaround: There is no workaround.

- CSCtj59254

  Symptoms: Data to default MDT switchover fails in highly scaled scenarios.

  Conditions: The symptom is observed during a default to data MDT switchover.

  Workaround: There is no workaround.

- CSCtj67133

  Symptoms: Standby gets stuck at “in progress to standby cold-config” state in ISSU. The following message will be seen:

  ```
  %ISSU-SP-3-FSM_MISMATCH_MTU: ISSU nego failed for client 7600 MCAST L2 ISSU
  client(6018) entity_id 1 session 65630 due to mismatch of mtu size 12 & 20.
  %ISSU-SP-4-FSM_INCOMP: Version of local ISSU client 7600 MCAST L2 ISSU client(6018) in
  session 65630 is incompatible with remote side.
  ```

  Conditions: The symptom is observed when doing an ISSU with Cisco IOS Release 12.2(33)SRE or Release 15.0(1)S.

  Workaround: There is no workaround.

- CSCtj70271

  Symptoms: Non-local replications are programmed as local replications in the MET3 (i.e.: if the replications are on slot 3 DFC module, then the supervisor is programmed with the sublsps of slot 3 as local replications). This causes a waste of TCAM resources and can cause traffic outage.

  Conditions: The symptom is observed with LSM/MLDP configurations.

  Workaround: Use this command: **clear ip mroute** *source group*.

- CSCtj72148

  Symptoms: A Cisco 7600 router might face an SP crash upon first reload after upgrade from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2. After successive reloads, the system functionality is restored.

  Conditions: This symptom is observed when upgrading from Cisco IOS Release 12.2(33)SRC5 to Release 12.2(33)SRE2.

Workaround: There is no workaround.

- CSCtj74611

  Symptoms: Active supervisor in the Cisco 7600 series router reloads.

  Conditions: The symptom is observed after a linecard is powered off due to keepalive failures. Possible sequence of syslog messages:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 7, is being power-cycled off (Module not responding
  to Keep Alive polling) <...> %C7600_PWR-SP-4-DISABLED: power to module in slot 7 set
  off (Failed to configure the line card) <...> %EM-SP-4-AGED: The specified EM client
  (EM_TYPE_FABMAN_NORMAL type=29, id=8887) did not close the EM event within the
  permitted amount of time (900000 msec). SP: em_fabman_act_event_end_cb: (timer) SWM
  event 8887 (slot 7 -> HELIOS / CARD_RUNNING) was not closed properly
  ```

  Workaround: There is no workaround.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj79085

  Symptoms: MFIB entries struck in NP HW_ERR MET-FULL:5, NP HW_ERR MET-ALLOC:6

  Conditions: This symptom is observed during slot 7 reload, UUT-CE1 interface Flap and UUT reload with traffic.

  Workaround: There is no workaround.

- CSCtj79349

  Symptoms: After swapping GE-T SFP with GE-SX, if port is at 100m, it will retain the same old speed.

  Conditions: Issue is seen only after swapping with GE-T which was at 100m with any other SFP on an ES+.

  Workaround: There is no workaround.

- CSCtj86514

  Symptoms: An SNMP walk on Cisco AAL5 MIB may not return information for all PVCs configured on the device.

  Conditions: An SNMP walk query on the Cisco AAL5 MIB may fail to return information of bundled PVCs that are in down state. Information about PVCs in UP state is returned correctly.

  Workaround: To get information of bundled PVCs in down state, you need to poll with more specific OIDs. Instead of doing an snmpwalk on “1.3.6.1.4.1.9.9.66.1.1.1.1.3”, do an snmpget on “1.3.6.1.4.1.9.9.66.1.1.1.1.3.<IfIndex>.<VPI>.<VCI>”.

- CSCtj87180

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

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

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: IOSd crash when using the command **clear crypto session** on an EzVPN client.

  Conditions: Testbed setup:

  1. RP2+ESP20 worked as the EzVPN simulator, which is configured with over 1000 clients. Then simulator is connected to Cisco ASR 1004-RP1/ESP10 (UUT) with DVTI configured
  2. Use IXIA to generate 1Gbps traffic
  3. Wait until all the SAs have been established and traffic is stable
  4. Use CLI **clear crypto session** on EzVPN simulator.

  Workaround: There is no workaround.

- CSCtj92563

  Symptoms: Interfaces take a longer time to come up.

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

  Workaround: There is no workaround.

- CSCtj94358

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

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

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

- CSCtj94835

  Symptoms: Spurious memory access and tracebacks are seen on router reload.

  Conditions: The symptom is observed when the router is reloaded.

  Workaround: There is no workaround.

- CSCtj95032

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

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

  Workaround: There is no workaround.

- CSCtj96489

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

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

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

- CSCtj96915

  Symptoms: LNS rounter hangs up at interrupt level and goes into an infinite loop.

  Conditions: Unknown at this moment, See Further Problem Description below.

  Workaround: There is no workaround; power-cycle to 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 completion by an interrupt that is raised. We believe this is a timing issue; while this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtj97360

  Symptoms: Punted datapaths are multicast flows GREoIP->DefaultMDT & GREoMPLS->Default MDT.

  Conditions: This symptom is observed with device bootup with ipv4-only VRF. After bootup IPv6 was enabled for VRF, which has triggered the problem.

  Workaround: Do not have IPv6 AF and the mcast configs in the same VRF.

- CSCtj99415

  Symptoms: Traffic is not dropped when the packet size is more than the egress interface MTU.

  Conditions: This symptom is observed when the egress interface is on SIP400. When the outgoing interface is on ES20, the packets are dropped at RP with an error message.

  Workaround: There is no workaround

- CSCtk00976

  Symptoms: File descriptor reaches the maximum threshold limit. You will be unable to save the configuration or do any file system related operation as file descriptors are exhausted. You will get "File table overflow" error.

  Conditions: The symptom is observed when running the **dir/recursive <>** command periodically using the ANA tool.

  Workaround: Do not run **dir/recursive <>** command if leaks are detected. Also, if it is running through ANA server polling, disable it.

- CSCtk02155

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

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

  Workaround: Reset the line card.

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

- CSCtk02661

  Symptoms: Bundles stop forwarding any traffic.

  Conditions: The symptom is observed when you move the SPA to a different bay on a SIP-400 and apply configurations on the new bay.

  Workaround: Reload spa on both ends.

  Alternate workaround: Unconfigure multilink before moving the SPA out.

- CSCtk02666

  Symptoms: During a graceful restart event, the peer undergoes reconfiguration. This may result in stale labels on the RRP.

  Conditions: The symptom is observed with GR + SSO + peer reprovisioning.

  Workaround: Perform a **clear xconnect** or flap the local VC.

- CSCtk05652

  Symptoms: UDLD used end-to-end across an AToM link causes the CE link on one side to be put into err-disabled state.

  This is the topology:

  ```
  SW1 (CE) <-- PE-1 <-> MPLS cloud <-> PE-2 (7600 running 12.2(33)SRE2 --> SW2 (CE)
  ```

  We are seeing UDLD errdisabling the port on SW2, though the link is not unidirectional.

  Conditions: This symptom is observed on Cisco IOS Release 12.2(33)SRE2.

  Workaround: Running Cisco IOS Release 12.2(333)SRD5 instead of Release SRE2 fixes the problem.

- CSCtk07369

  Symptoms: The buginf statement `"draco2_fastsend: PAK_BUF_ON_OBL processing vlan"` appears on the console.

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

  Workaround: There is no workaround.

- CSCtk07632

  Symptoms: Even with the filter option, traffic on a different VLAN on trunk port is getting spanned.

  Conditions: The symptom is observed when the filter vlan specified is not configured on the box.

  Workaround: Configure the vlan on the box, then configure it as SPAN filter vlan.

- CSCtk12608

  Symptoms: Route watch fails to notify client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: The symptoms are observed using Cisco IOS Release 15.0(1)M, Release 15.1 (2)T and Release 15.1(01)S and with the following configurations:

  ```
  Router 1: interface Ethernet0/0 ip address 10.0.12.1 255.255.255.0 !
  interface Ethernet1/0 ip address 10.0.120.1 255.255.255.0 ! router bgp 100 no
  synchronization bgp log-neighbor-changes neighbor 201.0.0.1 remote-as 200 neighbor
  201.0.0.1 ebgp-multihop 255 no auto-summary !
  ip route 0.0.0.0 0.0.0.0 200.0.0.1 ip route 201.0.0.1 255.255.255.255 10.0.12.2 ip
  route 201.0.0.1 255.255.255.255 10.0.120.2
  Router 2: interface Loopback200 ip address 200.0.0.1 255.255.255.0 ! interface
  Loopback201 ip address 201.0.0.1 255.255.255.0 ! interface Ethernet0/0 ip address
  10.0.12.2 255.255.255.0 !
  interface Ethernet1/0 ip address 10.0.120.2 255.255.255.0 ! router bgp 200 no
  synchronization bgp log-neighbor-changes network 200.0.0.0 neighbor 10.0.12.1
  remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route
  0.0.0.0 0.0.0.0 10.0.12.1 !
  ```

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes”.

- CSCtk13364

  Symptoms: Traffic is blackholed over EVC bridge domain interfaces on the port.

  Conditions: The symptom is observed when a subinterface is deleted and an EVC with the same encapsulation dot1q is created and configured with a bridge domain. The traffic over all the other EVCs on the interface is blackholed.

  Workaround: After the configuration, perform a shut/no shut on the interface.

- CSCtk19108

  Symptoms: MVPN traffic failing.

Conditions: The symptom is observed after an SSO switchover.

Workaround: There is no workaround.

- CSCtk31515

  Symptoms: Router or linecards crash upon removing VLAN interfaces that are in the OIF list.

  Conditions: The symptom is observed with a series of VLAN interfaces in the access and with the hosts joining groups. Configured is “ssm-mapping”. Access facing linecards can be DFC or CFC.

  Workaround: There is no workaround.

- CSCtk31615

  Symptoms: Standby crashes upon an ISSU upgrade from Cisco IOS Release 12.2 (33)SRD to Release 12.2(33)SRE.

  Conditions: The symptom is observed with an ISSU between Cisco IOS Release 12.2(33)SRD and Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCtk33682

  Symptoms: Storm control stops working.

  Conditions: The symptom is observed after a shut/no shut of the interface on an ES-20.

  Workaround: Remove/add the storm control command on the interface.

- CSCtk33784

  Symptoms: After ISSU from SRE1 to SRE3, `%CONST_MFIB_LC-SP-6-MET_MCAST_ALLOC_FAILURE` is displayed continuously for a particular group.

  Conditions: This symptom is observed after configuring 10 groups and 32 OIFs.

  Workaround: There is no workaround.

- CSCtk34026

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

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

  Workaround: Create access subinterfaces from scratch.

- CSCtk36059

  Symptoms: Active SRE does a silent reload while undergoing an ISSU from Cisco IOS Release 12.2(33)SRD to Release 12.2(33)SRE.

  Conditions: The symptom is observed with scaled configurations.

  Workaround: There is no workaround.

- CSCtk36064

  Symptoms: The cos value is not copied to exp when adding a label in l3vpn/vpls scenarios.

  Conditions: This symptom is observed On A Cisco 7600 router, ES+ LC, QoS policy-map with set cos applied on switchport interface in ingress.

  Workaround: There is no workaround.

- CSCtk36090

  Symptoms: Router crash at draco2_inband_dma_pak after a router reload with the following SRE image:

  ```
  s72033-adventerprisek9_dbg-mz.nightly_sre_2010-11-20
  ```
  Conditions: The symptom is observed following a router reload.

  Workaround: There is no workaround.

- CSCtk36377

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

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

  Workaround: Delete VRF and add it back.

- CSCtk37068

  Symptoms: Policing is not happening.

  Conditions: This symptom is observed when copp is enabled.

  Workaround: There is no workaround.

- CSCtk39301

  Symptoms: Tracebacks such as the following can appear on the RP:

  ```
  %C6K_MPLS_RP-STDBY-3-INFINITE_OCE: In label: 17 Invalid OCE previous oce type: 29 prev
  ptr: 0x5648A2B0, next oce type: 29 next oce ptr: 0x0 -Traceback= 42319368z 42322E68z
  42BA0EF0z 438DCE10z 438D17F0z 405A209Cz 405AC198z 405A7900z 405EA768z 405EA9E0z
  438D06B4z 438D0EE4z 438DAF98z 438FFE40z 422200D0z 4222123Cz
  ```
  Conditions: The symptom is observed if there are more than eight or 10 ECMP paths for any prefix (i.e.: when there is a load balanced object in the forwarding OCE chain).

  Workaround: Reduce the number of paths and do a **clear ip route** to re-initiate hardware programming.

- CSCtk47739

  Symptoms: IPSec tunnels can be established even though the certificate of remote peer has been revoked and the current router's CRL has been updated.

  Conditions: The symptom is observed on a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRD4.

- CSCtk47891

  Symptoms: Traffic might be blackholed on lc reset if FRR is in use.

  Conditions: This symptom is observed with an FRR configuration in ACTIVE state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk47960

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

  Remote side will generate the following:

  ```
  %CLNS-3-BADPACKET: ISIS: L1 LSP, packet (902) or wire (896) length invalid
  ```
  Conditions: This symptom is seen on Cisco 7600 switch with SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

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

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

- CSCtk53463

  Symptoms: When configuring "shape average <cir value> <bc value>" currently across all platforms, <bc value> is limited by 4ms * <cir value>. 4ms here represents the minimum interval time for bursts. ES+ LC, however can support an interval value that is faster (smaller) than 4ms. This has been an expected behavior with the exception of ES+ LC.

  Conditions: This symptom is observed on all platforms.

  Workaround: There is no workaround.

- CSCtk53763

  Symptoms: Traffic for some of the SubLSPs is not flowing with P2MP TE or MLDP.

  Conditions: The symptom is observed with LSM and MLDP configurations with multiple SubLSPs.

  Workaround: Use the following command: **clear ip mroute ***.

- CSCtk54318

  Symptoms: VC creation fails on disabling and re-enabling the card for SIP-400 with 4XT3E3 SPA with below messages on console:

  ```
  SLOT 2: %NP_CLIENT-3-INITFAIL: NP Client Initialization Failed - fr_npc_vc_add: vc
  creation failure, np: 0, hwidb: 0x4ACA3500, dlci: 0 SLOT 2: %NP_CLIENT-3-INITFAIL: NP
  Client Initialization Failed - fr_npc_vc_add: vc creation failure, np: 0, hwidb:
  0x4ACA3500, dlci: 1023
  ```

  Condition: This issue is seen when the below commands are executed on a T3 serial interface of the SPA 4XT3E3 configured as DTE with frame relay encapsulation:

  no card type t3 *slot bay* **card type t3** *slot bay*

  Then unconfigure and reconfigure frame relay enacapsulation.

  Workaround: Reload the SPA.

- CSCtk55382

  Symptoms: A SPA-OC192POS-VSR or SPA-OC192POS-XFP may fail boot diagnostic test.

  Conditions: The symptom is observed when Control Plane Policing (CoPP) is configured on the system. The diagnostic test that fails is the “TestACLPermit” test displayed in “show diagnostic result”. The output of “show module” will indicate a “Minor error” on the subslot.

  Workaround: Before a system reload or module reset, disable the CoPP feature. After the module is booted, CoPP can be enabled again.

- CSCtk55573

  Symptoms: On SIP-600 and SIP-400 linecards, disposition drops are observed for software EoMPLS or VPLS traffic.

  Conditions: The symptom is observed with SIP-400/600 linecards.

  Workaround: Perform a shut/no shut on the VLAN where xconnect is configured.

- CSCtk57049

  Symptoms: Traffic is not sent over data mdt even though the vrf selects the data mdt for encapsulation. After access interface flap on encap PE in MVPN setup, the traffic is not sent over data mdt even though the vrf selects the data mdt for encap.

  Conditions: This symptom is observed after access interface flap on encap PE in an MVPN setup.

Workaround: There is no workaround.

- CSCtk62680

  Symptoms: A Cisco 7600 series router may experience a sudden failure upon attempting to upgrade the software from Cisco IOS Release 12.2(33)SRD3 to Release 12.2 (33)SRE3 using the ISSU procedure.

  Conditions: The symptom is observed with a multicast configuration with multiple hosts distributed across subinterfaces, main interfaces, EVC service instances, and port-channel interfaces on CFC and DFC cards.

  Workaround: None for ISSU. Upgrade using a reload.

- CSCtk64020

  Symptoms: A Cisco 7600 may crash.

  Conditions: This symptom is observed when the **clear ip subsriber** command is entered.

  Workaround: There is no workaround.

- CSCtk69810

  Symptoms: The rw index is set to “invalid” in the catch-all entry. Because of this, the PIM neighbor on MDT is not up and traffic is not flowing.

  Conditions: This symptom is observed after ISSU from SRE1 image to SRE3.

  Workaround: Delete and add MDT under vrf.

- CSCtk76190

  Symptoms: The RSP/SUP fails to switchover automatically when the “TestSPRPInbandPing” fails for more than 10 instances.

  Conditions: The symptom is observed when the “TestSPRPInbandPing” fails for more than 10 instances.

  Workaround: There is no workaround.

- CSCtk95904

  Symptoms: RP crash at oce_to_sw_obj_type.

  Conditions: The symptom is observed with a route flap with 2K P2MP_TE sLSPs.

  Workaround: There is no workaround.

- CSCtk98030

  Symptoms: After replacing an ES20 linecard with an ES+ linecard or vice versa in the same slot, some service groups reject new members to join if the old linecard had ethernet service instances in these groups. Similarly, a named EVC rejects new ethernet service instances if it had association with the old linecard. The named EVC cannot be deleted, complaining that it still has service instances.

  Conditions: The symptom is observed if an ES20 linecard has been replaced with an ES+ linecard or vice versa in the same slot. The old linecard had ethernet service instance members in some service groups and/or named EVCs. The old associations between ethernet service instances and service groups or named EVCs are not cleaned up properly, blocking new association to these groups and EVCs.

  Workaround: Configure new service groups and named EVCs with same configuration as the problematic ones. Abandon the use of the old groups and EVCs. Assign ethernet service instances from the new linecard to the new groups and EVCs.

- CSCtl05684

  Symptoms: Xauth user information remains in “show crypto session summary” output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.

  Workaround: Use save-password feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl05926

  Symptoms: Packets of size exceeding MTU are dropped with the following error messages.

  ```
  *Dec 17 08:24:39.795: %CONTROLLER-3-TOOBIG: An attempt made to send giant packet on
  GigabitEthernet7/3/1 (1491 bytes from 10010046, max allowed 1476
  ```

  Conditions: This symptom is observed when the outgoing interface is on SIP400

  Workaround: There is no workaround.

- CSCtl07955

  Symptoms: BFD neighbor goes down and never comes up again

  Conditions: This is symptom is observed when we power down an unrelated LC by "no power enable module X."

  Workaround: There is no workaround.

- CSCtl10395

  Symptoms: CoPP stops dropping packets in hardware on a Cisco 7600 after double switchover.

  Conditions: This symptom is observed on a Cisco 7600 platform with CoPP configured on the router. SSO (HA Switchover) is done twice.

  Workaround: Remove and reconfigure the CoPP policy.

- CSCtl18652

  Symptoms: After replacing an ES20 with an ES+ linecard on the same slot, or vice versa, adding ethernet service instance members from the new linecard to an existing service group that was associated with the old linecard may cause a reload of the standby RP in SSO mode. This is due to stale configuration on the standby RP.

  Conditions: An ES20 linecard has been replaced by a different type of linecard or vice versa, on the same slot. New members are assigned to a service group that had members from the old linecard. There is a standby RP in SSO mode.

  Workaround: Create a new service group with the same configuration as the existing group and assign new members to the new group. Abandon the use of the old group.

- CSCtl19347

  Symptoms: On configuring more bundles, LC crashes with sip-400.

  Conditions: This is symptom is observed upon trying to copy the dlfi configs from disk to running config to make bundle up the LC crashes.

  Workaround: There is no workaround.

- CSCtl22871

  Symptoms: Cos value (applied from setcos policy) is not copied to EXP while adding label in one of the VPLS cases (VPLS cfgd on EVC BD Vlan).

  Conditions: This symptom is observed On ES+, QoS policy-map with set cos applied on EVC BD with VPLS configured on BD Vlan.

Workaround: There is no workaround.

- CSCtl41921

  Symptoms: Traffic duplication occurs.

  Conditions: This symptom is observed with a boot-up scale of 2000 slsps.

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

- CSCtl43925

  Symptoms: Having P2P GRE tunnels in vrf on the access side causes multicast traffic for the vrf to be dropped.

  Conditions: This symptom is observed after removal of tje GRE header and encapsulation changes from Tunnel vlan to QoS vlan. The next entry to be hit has incoming vlan as VPN QoS vlan. Here CR=1 is necessary. However when tunnels are suddenly brought up in vrf, CR=0 gets programmed and packets get bridged and dropped.

  Workaround: There is no workaround.

- CSCtl46903

  Symptoms: The VLAN mapping/translation feature does not work.

  Conditions: This symptom is observed on ES+ when the port is configured as an L2 switchport.

  Workaround: The feature works properly only if it is configured under EVC framework or L2 switchport in the LAN cards.

- CSCtl82922

  Symptoms: Fast memory leak occurs on the Standby Switch Processor (SP) of Supervisor in the "mfib-const-lc" process. Once this process depletes memory, the system will generate "MALLOC" errors for any other process requesting memory at that time. Eventually, the standby SP will crash and system operation will recover.

  To identify observe "Holding" number over time in Standby SP, can grow with speed of 60kB/s:

  ```
  #remote command standby-sp show proc mem | i mfib-const-lc|Holding PID TTY Allocated
  Freed Holding Getbufs Retbufs Process 281 0 106300144 4061004 103339316 0 0
  mfib-const-lc Pr
  ```

  Conditions: This symptom is observed with multicast stream timeout & restart in a mVPN environment. Stream S,G entry might not be installed in HW, and following MFIB Platform flags error might be seen for this stream along with memory leak:

  ```
  #show ip mfib vrf <vrf_name> verbose | i HW_ERR (176.2.76.2,229.2.76.2) Flags: ET K
  DDE Platform Flags: NP RETRY RECOVERY HW_ERR HAL:5
  ```

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE2

Cisco IOS Release 12.2(33)SRE2 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE2 but may be open in previous Cisco IOS releases.

- CSCsa76212

  Symptoms: Group Manager or Alternate may reload if compactflash is re- inserted into the disk0: slot too quickly after extraction.

Conditions: This symptom is observed when Group Manager and Alternate are both up and in their respective active states.

Workaround: After extracting compactflash from the disk0: slot, wait 30 to 60 seconds before re-inserting disk.

- CSCsb09867

  Symptoms: While querying SNMP with IPv6, some traceback errors may be seen.

  Conditions: This symptom is observed with a Cisco 7200 router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsl64247

  Symptoms: Router crashes 20-30 minutes after configuring “mode route control”.

  Conditions: The symptom is observed when the router is configured as OER master.

  Workaround: There is no workaround.

- CSCsm17983

  Symptoms: Router experiences memory corruption.

  Conditions: Unknown conditions. Appears to be random.

  Workaround: There is no workaround.

- CSCso53741

  Symptoms: Duplicate IPSec SA may appear during rekey.

  Conditions: This symptom occurs during rekey.

  Workaround: There is no workaround.

- CSCso60442

  Symptoms: A crash occurs.

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

  Workaround: There is no workaround.

- CSCsr17680

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

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

  Workaround: There is no workaround.

- CSCsu49066

  Symptoms: In SSM when no receivers have joined yet and the source becomes active, a CPU spike on the RP will be seen.

  Conditions: This symptom happens only when there are no receivers joined to receive the multicast traffic.

  Workaround: Configuring “mls rate-limit multicast ip fib-miss <>” will help alleviate the problem and keep the CPU utilization on the RP down.

- CSCsw21852

  Symptoms: The **show proc mem** command indicates that the process “Laminar Icc Eve” consumes a lot of memory.

Conditions: The process handles all communication messages between CSM and Sup/MSFC including snmptrap, syslog. The more messages that are exchanged, the more memory will be leaked.

Workaround: There is no workaround.

- CSCsx13442

  Symptoms: After performing a **shut** then a **no shut** on the hub tunnel interface, the spoke cannot trigger IKE SA.

  Conditions: The symptom is observed after performing the reset sequence of **shut** and **no shut** commands to the tunnel interface on the hub.

  Workaround: Use a smaller ISAKMP keepalive, or do a shut/no shut on the spoke tunnel.

  Further Problem Description: After doing a shut/no shut on the hub tunnel, the hub sends message to spoke to bring down the IKE SA but not the IPSec SA. That keeps the staled IPSec SA on spoke and traffic tries to use it. However on the hub side, since there is no IPSec SA, the hub drops the packets due to no established SA (IpsecInput Drops). Therefore traffic from the hub side will not be able to trigger the IKE SA and will keep using the staled IPSec SA.

- CSCsx56362

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

  Conditions: The symptom is observed when:

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

  Workaround: There is no workaround.

  Further Problem Description: The selection of non-oldest paths as multipaths is only problematic in releases which include CSCsk55120, because in such releases it causes changes with respect to whether paths are considered multipaths.

- CSCsy47987

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

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

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

- CSCsy56433

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

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

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

  1. Upgrade the standby ROMMON F1 region.

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

Workaround: There is no workaround.

- 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.

- CSCsz18634

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

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

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

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

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

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

  Or, execute reload.

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

- CSCta00692

  Symptoms: A router crashes.

Conditions: This symptom is seen with ipv6+mcast.

Workaround: There is no workaround.

- CSCta18596

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

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

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

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

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

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

 map-class frame-relay BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725
  frame-relay cir 768000
  frame-relay mincir 768000
  no frame-relay adaptive-shaping
  service-policy input BANKOFIRE-IN-S1/0.1/1/4/2:0
  service-policy output BANKOFIRE-OUT-S1/0.1/1/4/2:0
  frame-relay fragment 600
 !
```

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

- CSCta21771

  Symptoms: Because of a hardware fault on the standby supervisor card, 4 WS- X6148A-45AF line cards were powered down. This is due to the “bus stalled” condition in the system due to a faulty hardware.

  Conditions: Faulty hardware can trigger the bus stalled condition.

  Workaround: By removing the faulty HW, a bus stalled condition can be eliminated.

  Further Problem Description:

```
%SNMP-5-MODULETRAP: Module 9 [Down] Trap
%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at
0 error on module 9!
%C6KPWR-SP-4-DISABLED: power to module in slot 9 set of
f (Diagnostic Failure)
%SNMP-5-MODULETRAP: Module 7 [Down] Trap
%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at
0 error on module 7!
%C6KPWR-SP-4-DISABLED: power to module in slot 7 set of
f (Diagnostic Failure)
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking por
t GigabitEthernet5/1 on VLAN0010.
%SNMP-5-MODULETRAP: Module 8 [Down] Trap
%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at
0 error on module 8!
%C6KPWR-SP-4-DISABLED: power to module in slot 8 set of
f (Diagnostic Failure)
%EARL-SP-2-SWITCH_BUS_IDLE: Switching bus is idle for 2
 seconds. The card grant is 6
%SNMP-5-MODULETRAP: Module 3 [Down] Trap
```

  The above error/SYSLOG clearly indicates that the module is receiving flowcontrol on the backplane. As a result this module will not be able to transmit any packets on to the back plane which can result in HM diag failures. However, we must understand that this module is a victim of FCI and any resultant diag-failure actions on this module are not correct and will not mitigate/resolve the FCI problem. So the module should not be powered down.

- CSCta58068

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

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

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

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

  1. OSPF routing protocol is enabled on all the networks in the topology.

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

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

1. On PE and RR routers: IGP states = 100 OSPF routes.
2. BGP states = 200,010 VPNv4 routes.

On PE routers ONLY:

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

Workaround: There is no workaround.

- CSCtb23840

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

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

  Workaround: There is no workaround.

- CSCtb44031

  Symptoms: An LDP session goes down and does not re-establish.

  Conditions: This symptom is observed when the password is removed from the LDP session on both peers with the **no mpls neigh** *ip- address* **password** *password* command.

  Workaround: There is no workaround.

- CSCtb54422

  Symptoms: An MFR bundle moves from SW to HW mode and flaps after reload.

  Conditions: This symptom is observed on a Cisco 7200 router when an MFR is configured on CJ-PA, then one member is added from MCTE1 and the following commands are entered: **wr mem** and **reload**.

  Workaround: Create a new MFR after reload and add members to it.

- CSCtb59842

  Symptoms: MFIB entries are stuck in NP HW_ERR MET-ALLOC:5 for the platform flags.

  Conditions: The problem of MFIB entries stuck in NP HW_ERR MET-ALLOC:5 is seen during reload of the UUT reload (per-prefix/per-vrf) (with/without traffic) and OIR.

  Workaround: There is no workaround.

- CSCtb75413

  Symptoms: IGMP membership is lost for multiple groups on multiple interfaces. After a few minutes, membership is reestablished. Hosts are observing loss of multicast streams during the loss of membership.

Conditions: This issue will be seen only when the SSM mapping is enabled and when the DNS lookup for the SSM source mapping fails due to the unavailability of the DNS server.

Workaround: Disable the DNS lookup for the SSM mapping by the **no ip igmp ssm-map query dns** command

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

Further Problem Description: If SSM Static Mapping command is used and router processes SSM groups outside the configured Static SSM Mapping range, then routers falls to DNS based lookup to find SSM mapping. If DNS servers are not reachable or DNS servers not configured to provide mapping, input interface Q builds up leading to control plane instabilities affecting other protocols also.

- CSCtb85661

  Symptoms: On doing multiple switchovers or after ISSU completion followed by a failover, the hardware programming of bidir entries does not show the correct dest_index (0xFFFF) leading to a drop in traffic.

  Conditions: This symptom only affects Cisco IOS Release 12.2(33)SRE. This issue may hit only in case of multiple failovers.

  Workaround: The dest_index can be set to the correct value using a test CLI, and traffic will resume.

- CSCtb92791

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

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

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

- CSCtc00851

  Symptoms: The output of the **show mfib table** command on a line card can show tables not in “sync” state, instead being in “disconnecting” or “connecting” state for some time (minutes). In this state the multicast forwarding tables are not being updated and may be out of sync with the active RP.

  Conditions: The problem may occur on line cards or the redundant RP on a distributed router. It is usually associated with conditions of high CPU due to large numbers of routing updates in a scaled configuration.

  Workaround: The **clear mfib table** command may clear the problem. Alternatively the affected line cards may need to be reloaded.

  Further Problem Description: Often the problem will be accompanied with error messages relating to MFIB connectivity to the multicast routing information base.

- CSCtc13664

  Symptoms: With an IPv6 Policy Based Routing (PBR) configuration, the route-map clause “set interface null0” may cause a router to crash.

  Conditions: The symptom is observed with IPv6 PBR. The trigger traffic is traceroute packets (ping packets will not cause the crash).

  Workaround: Configure “oute-map” as (set interface loop0).

- CSCtc40111

  Symptoms: When a large number of service groups are configured with multiple EVCs in them, the following anomaly can be observed. On doing online insertion and removal (OIR), some of the service groups (Layer 2 nodes) are configured in TMC which instead of in TMB. Before and after OIR output differs as below

Before OIR

```
***************

Evee-dfc4#sh platform hardware qos np 0 queue resources
 np   tm  level    groups     entity
 ---------------------------------------------
  0  0     L4     4096/6    32768/16
  0  0     L3      256/4     4096/6
  0  0     L2       16/1      256/1
  0  0     L1       32/1       32/1
 ---------------------------------------------
  0  1     L4     4096/4081    32768/11732
  0  1     L3      256/256     4096/4081
  0  1     L2        8/1      256/256
  0  1     L1       32/1       32/1
 ---------------------------------------------
  0  2     L4     4096/3    32768/5
  0  2     L3      256/2     4096/3
  0  2     L2        8/1      256/2
  0  2     L1       32/1       32/1
```

After OIR

```
*************
Evee-dfc4#sh platform hardware qos np 0 queue resources
 np   tm  level    groups     entity
 ---------------------------------------------
  0  0     L4     4096/6    32768/16
  0  0     L3      256/4     4096/6
  0  0     L2       16/1      256/1
  0  0     L1       32/1       32/1
 ---------------------------------------------
  0  1     L4     4096/1043    32768/2996
  0  1     L3      256/67     4096/1043
  0  1     L2        8/1      256/67
  0  1     L1       32/1       32/1
 ---------------------------------------------
  0  2     L4     4096/3041    32768/8741
  0  2     L3      256/191     4096/3041 <<<<<<<<<<<<<<<<<<<<<<<<<<
  0  2     L2        8/1      256/191    <<<<<<<<<<<<<<<<<<<<<<<<<<
  0  2     L1       32/1       32/1
```

Conditions: This happens with Ten Gigabit Ethernet interface and a large number of service groups and EVCs.

Workaround: One option is to keep scale below 250. Aside from that there is no workaround.

- 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.

- CSCtc53929

  Symptoms: An IPSec/GRE tunnel is running between Hub and Spoke. Pim is enabled on the GRE interfaces. MCAST traffic is sent from source 10.0.1.2 connected to Hub to the grp 224.1.1.1. HA is on the Hub. On doing SSO, the platform flag is set to NP RETRY RECOVERY HW_ERR and packets are s/w forwarded.

  Conditions: This symptom is seen when the platform flag is set to NP RETRY RECOVERY HW_ERR and packets are s/w forwarded.

  Workaround: Reload the router.

  Further Problem Description:

```
Hub1#sh ip mf vrf ivrf1 ver | b 10.0.1.2
 (10.0.1.2,224.1.1.1) Flags: K DDE
   Platform Flags:  NP RETRY RECOVERY HW_ERR :5
   Slot 6: HW Forwarding: 0/0, Platform Flags:  NP
   Slot 5: HW Forwarding: NA/NA, Platform Flags:  NP
   Slot 2: HW Forwarding: 0/0, Platform Flags:  NP
   SW Forwarding: 33199746/51309/46/18439, Other: 56670704/0/56670704
   HW Forwarding:   9512319/74406/46/26739, Other: 0/0/0
   GigabitEthernet1/5 Flags: RA A
     Platform Flags:
   Tunnel1 Flags: RF F NS
     Platform Flags:
     CEF: Adjacency with MAC: 4500000000000000FF2F52AF041E5A010B00000100000800
     Pkts: 5354452/0
```

- 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.

- CSCtc78200

  Symptoms: A Cisco router may crash in parse_configure_idb_extd_args routine.

  Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

Workaround: As the PPP session is being established on the LNS, Cisco IOS will momentarily use one of the available VTYs from the router. After initial configuration, it is immediately released to the system pool.

If all VTY connections are in use, an RP crash will occur if a new PPP session is established and there are no free VTYs in the system.

To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect using multiple VTY connections at the same time, reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

```
ip access-list extended VTY_ACL
 deny   ip any any
!
line vty 5 9
 access-class VTY_ACL in
 exec-timeout 1 0
 login authentication local1
```

Alternate Workaround: Do not configure “interface range” CLI using ios_config from tclsh mode. When in tclsh mode, use normal “interface cli” in a “for loop.”

- CSCtd08797

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

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

  Workaround: Flap the interface.

- 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.

- CSCtd34887

  Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

  Conditions: SSM VRF mroute present in the table:

```
cce#show ip mroute vrf management
(Src 1  IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
```

Configuration of the interface:

```
int FastEthernet4.3
 encapsulation dot1Q 33
 ip vrf forwarding management
 ip address <IP addr>  255.255.255.252
 ip pim sparse-mode
 ip igmp join-group <group addr> source 10.32.178.56
 ip igmp join-group <group addr> source 10.32.178.23
```

Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- CSCtd49742

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

  Conditions: This symptom is seen when IEDGE is configured.

  Workaround: There is no workaround.

- CSCtd58314

  Symptoms: Switch may crash when using the **show ip arp inspection log** command.

  Conditions: This symptom occurs under normal operation.

  Workaround: There is no workaround.

- CSCtd66046

  Symptoms: Router stops generating IGMP query messages for four minutes.

  Conditions: This symptom occurs when IGMP process is blocked while resolving the DNS query through blocking call.

  Workaround: There is no workaround.

- CSCtd67010

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

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

  Workaround: There is no workaround.

- 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”.

- CSCtd87788

  Symptom: Traceback is seen when serial from second CJ-PA controller is added and removed from multilink. This interface remains up/down until a reload.

  Conditions: This symptom is seen when serial from second controller in unchannalized mode is added to multilink.

  Workaround: Reload the box to bring up the interface.

- CSCtd94144

  Symptoms: Ethernet OAM packets are not terminated locally.

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

  Workaround: There is no workaround.

- CSCte00934

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

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

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

- CSCte02089

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

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

  Workaround: There is no workaround.

- CSCte02973

  Symptoms: Routing protocols like EIGRP may be dropped in the global table.

  Conditions: The symptom is observed when multicast is configured for a VRF and no multicast is configured for the global table.

  Workaround: Enable “ip multicast routing” and create a loopback interface with “ip pim sparse-mode” enabled.

  Further Problem Description: The problem should not occur for MVPN since this is not a valid configuration, as multicast in the core is a requirement.

  However, it can occur for a feature called MVPN-lite, where multicast traffic is routed between VRF tables without the tunneling and therefore without the requirement for multicast in the global table.

- 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.

- CSCte10790

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

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

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

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

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

```
no 110
no 120
no 130
```

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

```
120 ACE
130 ACE
```

CRASH will happen

Follow the same order:

```
ip access-list extended vlan959-out
 permit ip 128.227.128.52 0.0.0.3 any
 remark - Standard out ACL -
 permit tcp any any established
 deny   tcp any any eq 707
 deny   tcp any eq 707 any
 deny   tcp any any eq 4444
 deny   tcp any eq 4444 any
 deny   udp any any eq 31337
 deny   tcp any any eq 12345
 deny   tcp any any eq 12346
 deny   tcp any any eq 20034
 deny   tcp any any eq 7597
 deny   ip host 0.0.0.0 any
 remark - allow cns & UFAD networks
 permit ip 128.227.212.0 0.0.0.255 any
 permit ip 10.227.212.0 0.0.0.255 any
 permit ip 10.228.212.0 0.0.0.255 any
 permit ip 10.249.10.0 0.0.0.255 any
 permit ip 128.227.74.0 0.0.0.255 any
 permit ip 128.227.156.0 0.0.0.255 any
 permit ip 128.227.0.240 0.0.0.15 any
 permit ip 10.5.187.240 0.0.0.15 any
 permit ip 10.241.28.240 0.0.0.15 any
 permit ip 128.227.128.112 0.0.0.3 any
 permit udp 128.227.128.0 0.0.0.255 eq ntp 10.241.33.0 0.0.0.255
 permit udp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
 permit tcp 128.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
```

```
 permit tcp 128.227.156.0 0.0.0.255 host 10.241.33.11 eq www
 permit tcp 128.227.128.0 0.0.0.255 host 10.241.33.29 eq cmd
```

Then follow the order:

```
no 110
no 120
no 130
120 permit udp 128.227.128.0 0.0.0.255 eq domain any
130 permit tcp 128.227.128.0 0.0.0.255 eq domain any
```

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

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

- CSCte14955

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may experience an unexpected reload.

  Conditions: The symptom may occur when multiple tunnel interfaces are configured with **mpls bgp forwarding**, if the tunnel interfaces are flapping.

  Workaround: Configure the eBGP sessions on interfaces other than tunnel interfaces.

- CSCte20187

  Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1)
  ```

  The label advertised may be different but it is always a reserved label (0- 15).

  Additionally, the local PE will see “No Label” as the “Outgoing Label" in the MPLS forwarding table.

  Conditions: This symptom is observed when bgp next-hop is configured under an interface.

  Workaround: There is no workaround.

- CSCte39643

  Symptoms: If PfR receives an EIGRP route change, the router may unexpectedly reload.

  Conditions: The symptom is observed with PfR and EIGRP configurations. It is observed some time after PfR receives an EIGRP route change, but before the previous EIGRP route is removed in the routing table, when PfR tries to recycle a previous EIGRP route.

  Workaround: There is no workaround.

- CSCte48877

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

  The PVC gets a negative circuit id.

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

  Conditions: Following is the sample show output when this happens:

  ```
  PE1#sh atm pvc 11/900
  ```

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

Workaround: There is no workaround.

- CSCte49283

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

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

  Workaround: There is no workaround.

- CSCte49641

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

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

  Workaround: There is no workaround.

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

- CSCte52369

  Symptom: 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.

- CSCte53365

  Symptoms: The connected EIGRP-owned global addresses are put into the EIGRP topology database after the IPv6 router eigrp <as> process is configured to “no shutdown.”

  Conditions: This symptom is observed when the router is reloaded with an IPv6 EIGRP instance configured “shutdown,” then the configuration is changed to “no shutdown.”

  Workaround: Configure “shutdown” then “no shutdown” on the interfaces.

- CSCte56594

  Symptoms: Seeing two dips of traffic drop after SSO, the first dip is about 80 milliseconds, the second traffic dip up to about 30 seconds.

  Conditions: This symptom is observed on the PE (Cisco 7609-S) that is configured with OSPF NSF and both MPLS and RSVP GR. Also 4K vlans, 20K virtual circuit is configured peering with another 5 PEs on the VPLS domain. Generate 60M unidirectional traffic across this VPLS domain, then execute redundancy switchover via CLI.

  Workaround: There is no workaround.

- CSCte62453

  Symptoms: Performing a shut and no-shut on a subinterface with igmp-join causes SSM VRF mroute to disappear.

  Conditions: This symptom is observed when SSM VRF mroute is present in the table:

```
ce#show ip mroute vrf management
(Src 1  IP, Grp IP), 00:10:48/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
(Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr 10.32.178.117
  Outgoing interface list: Null
```

  In addition, the interface is configured as follows:

```
int FastEthernet4.3
 encapsulation dot1Q 33
 ip vrf forwarding management
 ip address <IP addr>  255.255.255.252
 ip pim sparse-mode
 ip igmp join-group <group addr> source 10.32.178.56
 ip igmp join-group <group addr> source 10.32.178.23
```

  Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, the **no ip igmp-join** and **ip igmp join** commands are entered on the interface.

- 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”).

- CSCte66450

  Symptoms: Router crashes and may reload when running snmpwalk query on cevcUniCEVlanEvcTable table.

  Conditions: This symptom is observed when there are scale configurations (4k) for service instance evcs in a single interface.

  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.

- CSCte79112

  Symptoms: When swapping to ISG, the final Access-Accept received from the AAA server triggers an authentication that fails at the Access-Point. ISG is not transparent to EAP authentication.

  Conditions: This symptom is seen when migrating from SSG to ISG. ISG is proxy radius.

  Workaround: There is no workaround.

- CSCte83888

  Symptoms: If PoD request contains target Acct-Session-Id prepended with NAS- Port-ID, it will not be honored.

  Conditions: This symptom occurs when PoD is prepended with NAS-Port-Id for target session.

  Workaround: Use only the Session-Id which is located after the “_” in the Account-Session-ID to specify the session needing disconnect.

- CSCte86038

  Symptoms: High CPU utilization for ATM OAM timer process.

  Conditions: The symptom is observed with a scaled L2 VC configuration.

  Workaround: Increase the AIS RDI timeout with higher number of up and down retries.

- CSCte87809

  Symptoms: Cisco NetFlow Collector does not receive the NetFlow export if it is traversing through a GRE over IPSec tunnel.

  Conditions: This symptom is observed on a Cisco 2811 integrated services router (ISR) with Cisco IOS Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCte92581

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

  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.

- 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.

- CSCte98082

  Symptoms: PPPoE session is not coming up on some clients due to a malformed PADO. PPPoE relay sessions are failing to come up on an LAC.

  Conditions: The symptom is observed with a few clients which are unable to process malformed PADO and also when “pppoe relay service” is configured on the LAC.

  Workaround: There is no workaround.

- CSCte98144

  Symptoms: The standby reloads with spurious memory access during resource policy configuration.

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

  Workaround: There is no workaround.

- 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.

- CSCtf00427

  Symptoms: A router may experience a severe memory leak issue when the following command is configured:

  privilege exec level *level* **show ip ospf neighbor**

  Conditions: The symptom is observed when running Cisco IOS Release 12.2(33)XNE or 12.2(33)XNE1. The issue is not platform dependent.

  Workaround: Reload the router.

- 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.

- CSCtf06436

  Symptoms: Continuous high CPU usage.

  Conditions: The symptom occurs after the formation of a recursion loop in the FIB, when the prefixes in the loop are labeled.

  Workaround: There is no workaround.

- CSCtf06442

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

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

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

- CSCtf06486

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

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

  Conditions: The following error message can be seen:

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

  Workaround: There is no workaround.

- CSCtf07513

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

  Conditions:

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

  Workaround: Do not remove loopback interface before stopping traffic.

- CSCtf07907

  Symptoms: RP crash observed when doing RP switchover after deleting some tunnel configurations.

  Conditions: The symptom is observed when a switchover occurs after deleting some tunnel configurations and traffic is flowing in the background.

  Workaround: There is no workaround.

- CSCtf08239

  Symptoms: If heavy configuration is applied on box and SIP400 module gets reset with the **hw-module reset** command, the SP timer fails:

  ```
  %ONLINE-SP-6-TIMER: Module 1, Proc. 0. Failed to bring online because of
  timer event
  %C6KPWR-SP-4-DISABLED: power to module in slot 1 set off (Module  Failed SCP
  dnld)
  ```

Conditions: This symptom occurs when the CPU is very busy when the command is issued.

Workaround: There is no workaround.

Further Problem Description: SIP400 cards will reload twice.

- CSCtf13704

  Symptoms: Memory leak on graceful restart of BGP session.

  Conditions: The symptom is observed on branches with the fix for CSCte78958.

  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.

- CSCtf17273

  Symptoms: A Cisco router crashes during startup when receiving an AS_SET attribute from its peer.

  Conditions: This symptom is observed when the BGP peer sends an AS_PATH or AS4_PATH containing an AS_SET attribute.

  Workaround: There is no workaround.

- CSCtf19387

  Symptoms: CPU hogs may be seen for IP Input process when NHRP is configured.

  ```
  %SYS-3-CPUHOG: Task is running for (5000)msecs, more than (5000)msecs (11/5),process
  = IP Input.
  ```

  Conditions: This symptom is seen when packets are punted due to incomplete CEF adjacency and processed switched to resolve the next-hop address.

  Workaround: Configure “ip nhrp server-only” under DMVPN tunnel.

- CSCtf20154

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

  Conditions: This symptom is specific to RSP720.

  Workaround: There is no workaround.

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

- CSCtf21136

  Symptoms: A policy contains one or more user classes, and some queueing features are enabled in at least one of the user classes. Then the policy is applied to a target or a session.

  When the policy is unconfigured from the target, or the session goes down dynamically, memory leak is observed for 144 bytes per target or per session on each direction where the policy was applied.

  Conditions: A policy contains one or more user classes, and some queueing features are enabled in at least one of the user classes. Then the policy is applied to a target or a session.

When the policy is unconfigured from the target, or the session goes down dynamically, memory leak is observed for 144 bytes per target or per session on each direction where the policy was applied.

Workaround: There is no workaround.

- CSCtf21945

  Symptoms: DHCP based IP session on ISG, with ISG acting as DHCP server also, does not go down when DHCP server functionality is disabled by using the **no service dhcp** command, or DHCP binding is cleared by the **clear ip dhcp binding** *ip address* command.

  Conditions: This symptom is seen when ISG is acting as DHCP server also.

  Workaround: There is no workaround.

- CSCtf22243

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

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

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

- CSCtf27303

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

  Conditions: The symptom is observed under the following conditions:

  - Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.
  - Third-party: only capability IPv6 labeled unicast advertised.

  Workaround: There is no workaround.

- CSCtf29654

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

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

  Workaround: There is no workaround.

- CSCtf33203

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

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

  Workaround: There is no workaround.

- CSCtf35224

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

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

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

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

- CSCtf39455

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

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

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

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

- CSCtf40673

  Symptoms: All OIFs are reset when there is a **shutdown** on one of the interfaces followed by a **no shutdown**.

  Conditions: This symptom occurs when there is a **shutdown** on one of the interfaces followed by a **no shutdown**.

  Workaround: There is no workaround.

- CSCtf40731

  Symptoms: A routing loop is unexpectedly formed when PIRO and an OER-generated static route works together.

  Conditions: The symptom is observed under the following conditions:

  1. PIRO generates a more specific prefix for the static route it has created.
  2. OER-generated static route is redistributed into other IGP protocol in order to get traffic.

  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.

- CSCtf47146

  Symptoms: Policy-map that is attached to interface seems not to be working in HW.

Conditions: This symptom is seen when NBAR is configured after the last reload being unsupported on the platform. NBAR left a trace of it being supplied even though not further configured. This prevents QoS from working on that interface. This issue is specific to LAN cards on the Cisco 7600 router.

Workaround: Reload the router.

- CSCtf48413

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

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

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

- CSCtf50075

  Symptoms: A traffic blackhole can occur.

  Conditions: The symptom is observed following shut/unshut/shut of the redundant forwarding interface.

  Workaround: There is no workaround.

- CSCtf50306

  Symptoms: The **show mpls l2 vc** *vc-id* **detail** command display shows an empty label stack.

  Conditions: The symptom is observed when xconnect is configured under EVC, main interface, or subinterface and there are multiple core interfaces to reach the xconnect peer.

  Workaround: There is no workaround.

  Further Problem Description: This is a display issue. There is no functionality impact.

- CSCtf50894

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

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

  Workaround: Disable FRR protection.

- CSCtf51332

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

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

  Workaround 1: Disable VPN-CAM lookup.

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

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


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

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

```
interface GigabitEthernet2/3.104
      description SAK/PAM Turku C-FI-20709-8416
      encapsulation dot1Q 104
      ip vrf receive sak-pam
      ip vrf receive sak-voip
      ip address 10.100.220.177 255.255.255.252
      no ip redirects
      no ip proxy-arp
      ip policy route-map sak-vrfs-in1
      arp timeout 300
    !
     interface GigabitEthernet2/3.505
      description SAK/PAM Turku C-FI-20709-8416
      encapsulation dot1Q 505
      ip vrf receive sak-pam
      ip vrf receive sak-voip
      ip address 10.100.220.26 255.255.255.254
      no ip redirects
      no ip proxy-arp
      ip mtu 1500
      ip policy route-map sak-vrfs-in2
      arp timeout 300
     !
```

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

- CSCtf51541

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

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

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

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

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

- 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.

- CSCtf53672

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

  Conditions: The symptom is observed with a Supervisor 32.

  Workaround: There is no workaround.

- CSCtf56105

  Symptoms: Memory leak is seen at “dhcpd_vend_data”.

  Conditions: The symptom is observed when EAP authentication fails (possibly due to the wrong password).

  Workaround: There is no workaround.

- CSCtf64235

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

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

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

- CSCtf74073

  Symptoms: Enhanced FlexWAN resets upon copying a scaled configuration.

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

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

- CSCtf75053

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

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

  Workaround: There is no workaround.

- CSCtf75064

  Symptoms: MAC withdrawal is not sent to remote VPLS peer.

  Conditions: The symptom is observed with a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE0a upon receiving a TCN BPDU on an L2GP port.

  Workaround: There is no workaround.

- CSCtf77037

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

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

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

- CSCtf78196

  Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

  Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface. (It is seen on many images)

  Workaround: Statically configure “ipv6 mtu *mtu*” on tunnel interfaces.

- CSCtf78662

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

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

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

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

- CSCtf79154

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

  Conditions: The symptom is observed after an SSO switchover.

  Workaround: Do a **shutdown** and **no shutdown** on the corresponding subinterface.

- CSCtf80408

  Symptoms: Enhanced FlexWAN crashes.

  Conditions: The symptom is observed with following steps:

  1. Have scaled DLFIoATM (256 bundles) on a single PA.
  2. Have traffic flowing through all the bundles.
  3. Do a switchover.
  4. When standby comes up, do a **shutdown** and **no shutdown** on ATM interface.

  Workaround: There is no workaround.

- CSCtf82671

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

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

Workaround: There is no workaround.

- CSCtf82883

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

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

  Workaround: There is no workaround.

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

- CSCtf83092

  Symptoms: Standby resets continuously while ISSU upgrade from a non-componentized Cisco IOS image to a componentized Cisco IOS image.

  Conditions: The issue is seen with an MPLS VC configuration.

  Workaround: There is no workaround.

- CSCtf84237

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

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

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

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

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

- CSCtf85661

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

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

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

- CSCtf86240

  Symptoms: Enhanced FlexWAN with scaled DLFI setup crashes.

  Conditions: The symptom is observed with the following steps:

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

  Workaround: There is no workaround.

- CSCtf86865

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

  Conditions: The symptom is observed with the following steps:

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

  Workaround: There is no workaround.

- CSCtf90970

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

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

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

- CSCtf92354

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

  Conditions: The following steps cause this issue:

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

  Workaround: There is no workaround.

- CSCtf95905

  Symptoms: A router may crash in the BGP HA SSO process. The following error message is shown when the standby RP is booted:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk <hex-addr> data
  <hex-addr> chunkmagic <hex-addr> chunk_freemagic <hex-addr> -Process= "BGP HA SSO"
  ```

  Conditions: The symptom is observed with the following conditions:

  - The router is configured for SSO redundancy mode.
  - BGP is configured.
  - Some BGP peers have NSR configured (using the **neighbor ha-mode sso** command) and NSR is active for those peers.
  - The standby RP is loaded and progresses to hot standby state after NSR sessions are already established on the active RP.

  Workaround: Configure peers intended to be enabled for NSR for passive open only (using the **neighbor transport connection-mode passive** command) and then enable NSR on the BGP peers after the router has already reached hot standby state.

- CSCtf96659

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

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

Workaround: Use a single link configured as switchport trunk.

- CSCtf98985

  Symptoms: MAC withdrawal is not sent to the remote VPLS peer for MST instances other than MST0.

  Conditions: The symptom is observed on a Cisco 7600 series router with Cisco IOS Release SRE0a upon receiving a TCN BPDU on an L2GP port.

  Workaround: There is no workaround.

- CSCtg01296

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

  Conditions: The symptom is observed with the following steps:

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

  Workaround: There is no workaround.

- CSCtg08523

  Symptoms: The following message is seen at random intervals on the console and/or in the syslogs:

  ```
  %CONST_DIAG-SP-3-HM_TEST_FAIL:TestIPSecEncrypDecrypPkt
  ```

  Conditions: This issue is seen on a Catalyst 6500 with an SPA-IPSEC-2G module running Cisco IOS version 12.2SXI.

  Workaround: There is no workaround.

  Further Problem Description: The root cause appears to be the SPA not replying to the diagnostic packets from the supervisor from time to time. User traffic is not affected.

- CSCtg11217

  Symptoms: Standby crashes when doing an SSO.

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

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

- CSCtg11421

  Symptoms: The following issues are observed:

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

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

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

Workaround 2: Remove LLQ configuration.

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

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

- CSCtg13413

  Symptoms: ESP tunnel establishment with VPNLB is unsuccessful.

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

  Workaround: There is no workaround.

- CSCtg14446

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

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

  Workaround: There is no workaround.

- CSCtg14755

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

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

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

- CSCtg16191

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

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

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

  Conditions: The symptom is observed only with PPPoE sessions.

  Workaround: There is no workaround.

- CSCtg17600

  Symptoms: The configured “egress-method negotiated-return” does not work.

Conditions: The symptom is observed with VRF-aware WCCP and with Cisco IOS Release 15.1(1)T. The WCCP return traffic arrives on a sub-interface.

Workaround 1: Do not configure “egress-method negotiated-return”.

Workaround 2: If “egress-method negotiated-return” is configured ensure that the interface on which return traffic arrives is not configured with sub-interfaces.

Workaround 3: Change the Cisco IOS Release from 15.1(1)T to 15.0M.

- CSCtg22349

  Symptoms: Real reassign is not working in the ASNLB Vserver.

  Conditions: The symptom is observed when the real server is configured with reassign.

  Workaround: There is no workaround.

- CSCtg22774

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

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

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

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

- CSCtg26538

  Symptoms: CoPP over MPLS is not working and is failing to classify any packets.

  Conditions: The symptom is observed with CoPP over MPLS. CoPP will not be applied for any MPLS packet.

  Workaround: There is no workaround.

- CSCtg29252

  Symptoms: Certain EVCs do not have QoS applied on Excalibur card.

  Conditions: This symptom is seen after flapping a port-channel interface that is carrying 4000 EVCs with QoS configured.

  Workaround: Reload the card.

- CSCtg29783

  Symptoms: Egress policy-map on ES+ line card may not classify traffic for scalable EoMPLS. Traffic will fall into class default rather than specific classes matching based on MPLS EXP.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE1.

  Workaround: Use Cisco IOS Release 12.2(33)SRE0a.

- CSCtg40901

  Symptoms: Crash seen while authenticating with TACACS.

  Conditions: The symptom is observed if the TACACS server does not respond.

  Workaround: Use multiple connections.

Alternate Workaround: Configure a dummy TACACS server.

- CSCtg44661

  Symptoms: A router crashes when unconfiguring a route-map.

  Conditions: The symptom is observed when a policy route-map with “set ip next-hop recursive” is removed from an interface, then the route-map is unconfigured.

  Workaround: There is no workaround.

- CSCtg44996

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

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

  Workaround: Increase the access facing MTU.

- CSCtg45576

  Symptoms: ISIS adjacencies are down.

  Conditions: The symptom is observed when the IP layer 3 interface for adjacent routers is across an SVI (VLAN interface) and the underlying switchport trunk is on an ES+ line card. Following this, the ISIS adjacencies will not form.

  Workaround: Use a non ES+ line card port for the switchport trunk.

- CSCtg47874

  Symptoms: SIP-200 line card crashes.

  Conditions: This symptom is seen when you try to attach a map-class consisting of a flat policy (strict priority configured) to FR DLCI.

  Workaround: Configure a map-class consisting of H-QoS policy to FR DLCI.

- CSCtg58001

  Symptoms: Enhanced FlexWAN line card may crash.

  Conditions: The symptom is observed with scaled dLFIoATM sessions (256 sessions) on an Enhanced FlexWAN line card, upon configuring and unconfiguring a service policy on all the virtual templates followed by a shut/no shut of the ATM physical interface.

  Workaround: There is no workaround.

- CSCtg59956

  Symptoms: Active supervisor crashes when doing an SSO switchover.

  Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

  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.

- CSCtg70117

  Symptoms: A newly added EVC cannot receive multicast traffic.

  Conditions: The symptom is observed with ES20/ES+ configured with EVC mode. There are two METs in ES20/ES+ line cards. When a service instance is configured under Met0 and it starts receiving a multicast flow, and then you configure another interface under Met1 with service instance in same BD, the newly added service instance will not receive the multicast traffic.

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

- CSCtg72735

  Symptoms: In MPLS VPN, CE-CE traffic and PE-CE traffic experience high packet loss from 10%-50%.

  Conditions: The symptom is observed under the following conditions:

  1. There is access configuration on the sub-interface.
  2. Some sub-interfaces belong to same VRF.
  3. There is a frequent interface flapping on a sub-interface with this VRF.

  Workaround: Cancel access configuration on sub-interface.

- CSCtg73314

  Symptoms: After an mLACP failover, SVI and corresponding VCs on previous active PoA remain up.

  Conditions: The symptom occurs when MTP EVCs are configured on mLACP port-channel after the port-channel comes up as active.

  Workaround: Configure the MTP EVCs after bringing down the port-channel.

- CSCtg73691

  Symptoms: You cannot configure “route-target import” or other BGP extended community values with values greater than 65535 to the right of the “:” even though you are using a value less than 65536 to the left of the “:”.

  Conditions: This is seen when you issue a route-target import command with a value less than 65536 to the left of the “:” (and no “.” to the left of the “:”) and a value greater than 65535 to the right of the “:”.

  Workaround: There is no workaround.

  Further Problem Description: This problem was introduced by CSCtf13343.

  The following formats are supposed to be accepted:

  1. <IPv4 address>:<16-bit number>.

2. <2-byte ASN>:<32-bit number>.
3. <4-byte ASN in asplain format>:<16-bit number>.
4. <4-byte ASN in asdot format>:16-bit number.

- CSCtg83578

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

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

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

- CSCtg83800

  Symptoms: Entries in TCAM Region 5 of ES+ are not programmed correctly. The VLAN ID field and VLAN valid bits are not set up in TCAM entry. As a result, this entry can behave as a catch all entry.

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

  Workaround: Remove ISG configurations from the interface where this problem is seen.

- CSCtg84969

  Symptoms: The output of **show ip mfib vrf** *vrf name* **verbose** may show the following line "Platform Flags: NP RETRY RECOVERY HW_ERR" and multicast traffic may not be hardware switched.

  Conditions: The symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSO switchovers. When the issue occurs the output of **show ip mfib vrf** *vrf name* **verbose** on the standby SP will show some lines preceded with "###" where an interface name is expected.

  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.

- CSCtg91336

  Symptoms: A Cisco router may crash during show command **show ip ospf rib**.

  Conditions: This symptom is observed on Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

  – A user enters the **show ip ospf rib** command and stops in the middle
  – OSPF local rib is significantly changed; for example, routes are removed
  – A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

  Workaround: Do not enter the **show ip ospf rib** command. If it is necessary use the command, enter terminal length 0 and print the entire output.

- CSCtg92105

  Symptoms: IPv6 CLI is missing under the sub-interface after EVC is configured on the main interface on SRE.

Conditions: The symptom is observed when EVC is configured on the main interface.

Workaround: Remove the EVC configuration on the main interface then IPv6 can be configured.

- CSCtg94498

  Symptoms: Traffic rate driven switchover from Data MDT to Default MDT results in about a 200 second tail drop of multicast stream. After this time period, the stream recovers over Default MDT.

  Conditions: The symptom is seen with Cisco IOS Release 12.2(33)SRE1 and Release 12.2(33)SRE0a on a Cisco 7600 series router with a scaled number of mVRFs in mVPN.

  Workaround: Eliminate occurrence of this switchover, for example by setting the threshold to 0.

- CSCtg98501

  Symptoms: Memory leak is seen with EAP component every time the EAP system times out and retransmits the message back to policy component.

  Conditions: This symptom can occur with any Dot1x subscribers.

  Workaround: There is no workaround.

- CSCth01288

  Symptoms: ES+ 10G interface can flap (up and then down) during boot-up and SSO.

  Conditions: The symptom is observed when the interface is not administratively down and when XFP is connected with no cable.

  Workaround: Admin down (shut) the interface.

- CSCth01339

  Symptoms: ES20 line card on a Cisco 7600 series router may reload on switchover.

  Conditions: The symptom is observed when there is a SSC-400 card in the system It is seen when the ES20 has a reasonable scale configuration and an SSO switchover is performed.

  Workaround: There is no workaround.

- CSCth02479

  Symptoms: Router crashes.

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

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

- CSCth08661

  Symptoms: QoS is not working in an MPLS core. Packets marked with DSCP=EF in VPN are treated as default-class with EXP=0.

  Conditions: The symptom is observed when an ES20+ card is used as core-facing card pushing MPLS labels. Only a VPN label is marked with MPLS EXP=5 but transport label (LDP label) is pushed with MPLS EXP=0.

  Workaround: There is no workaround.

- CSCth11062

  Symptoms: When two or more sessions share a common layer4 service, if one session is cleared, the service may not work correctly for the other existing session.

  Conditions: This symptom occurs when the layer4 service is configured by an access list, and two or more layer4 redirected traffic streams, corresponding to the different sessions, originate from same client. For example, the sessions exist on ISG for a single client.

Workaround: Use different services or access lists.

- CSCth15790

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

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

  Workaround: There is no workaround.

- 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.

- CSCth20959

  Symptoms: Not able to attach to ES40 line card using the **attach module** *number* command.

  Conditions: The following steps will cause above stated problem:

  1. Do SSO switchover.
  2. Perform OIR of ES+ line card.
  3. Attach line card when it comes up.

  Workaround: Use the **remote command module** *1* command instead of attaching to ES+.

- CSCth25647

  Symptoms: Policy-map is not getting installed in ATM PVC.

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

  Workaround: There is no workaround.

- CSCth33457

  Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

  Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

  - ip accounting precedence input
  - ip accounting mac-address input
  - WCCP -Flexible NetFlow
  - BGP accounting
  - uRPF -mpls accounting experimental input

  Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth37793

  Symptoms: High CPU utilization caused by process switching of multicast traffic after IPv6 Address Family (AF) is configured for VRF.

Conditions: The symptom is observed on a Cisco 7600 series router that is acting as a PE router in mVPN. It is seen with multicast traffic forwarded inside a VRF for which IPv6 AF is configured. The issue can be seen when you:

1. Bootup with VRF configured only with IPv4; configure IPv6 AF after bootup.
2. Booutp with VRF configured with both IPv4 and IPv6 AF; unconfigure IPv6 AF after bootup.

Workaround 1: Unconfigure IPv6 AF from VRF.

Workaround 2: Clear mroute for VRF.

Workaround 3: Reload device.

Further Problem Description: Problem can be identified on a device following those steps:

1. High CPU seen using **show proc cpu**.
2. **sh redundancy** used to identify slot with active supervisor as <*X*>.
3. Attach <*X*>.
4. **sh platform software vpn mapping | i <***VRF-NAME-HERE***>**:

   IOS | <*VRF-NAME-HERE*> | 4 || <*NUMBER1*> | 0x0004 | 0x0000 | R[2]:4
5. **show platform software multicast ip cmfib vrf REN <***SOURCE GROUP***> verbose**:

   Multicast CEF Entries for VPN#4 (<*SOURCE*>, <*GROUP*>) IOSVPN:<*NUMBER2*> (1) PI:1 (1) CR:0 (1) Recirc:0 (1)

6. If <*NUMBER1*> and <*NUMBER2*> do not match, the defect is hit.

(Note: Values in "<>" are variables fitting your configuration.)

- CSCth39054

  Symptoms: Multicast packets received via a SIP-200 or SIP-400 interface have IP ToS set to 0x0 in the outer IP header of egress MDT packet. Because of this, the packets are not matched into proper queues if output QoS is present.

  Conditions: The symptom is observed with SIP-200 or SIP-400 as the ingress line card. Packets are destined to remote PE via MDT (mVPN). It is seen on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRE1. The following MLS QoS configuration is present:

```
mls ip multicast replication-mode ingress
no mls qos recirc untrust
no mls qos rewrite ip dscp
mls qos
mls cef tunnel fragment
mls mpls recir-agg
mls mpls tunnel-recir
```

  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.

- CSCth49989

  Symptoms: Vidmon functionality will stop working even though the packets are flowing through the interface.

  Conditions: The symptom is observed with a **shut** and **no shut** of the main interface.

  Workaround: Do one more **shut** and **no shut**.

- CSCth50096

  Symptoms: Crash occurs under certain EAP to DHCP communications.

  Conditions: The symptom is observed when the memory leak fix for CSCtg98501 is present.

  Workaround: There is no workaround.

- CSCth64439

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

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

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

- CSCti00020

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

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

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE1

Cisco IOS Release 12.2(33)SRE1 is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE1 but may be open in previous Cisco IOS releases.

- 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.

- CSCsi51649

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

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

  Workaround: There is no workaround.

- CSCsm26063

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

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

Workaround: There is no workaround.

- CSCso07705

  Symptoms: Tracebacks seen on Cisco 7200 router.

  Conditions: Occurs when SSH is used to connect to Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) multilink IP address.

  Workaround: There is no workaround.

- 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.

- CSCso86544

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

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

  Workaround: There is no workaround.

- 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: This symptom 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.

- CSCsq68156

  Symptoms: FRF12 packets are dropped by a PE router.

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

  Workaround: There is no workaround.

- CSCsq82663

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

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

Workaround: There is no workaround.

- CSCsq83789

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

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

  Workaround: There is no workaround.

- CSCsu45210

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

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

  Workaround: Remove the port security configuration on all ports.

- CSCsu99270

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

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

  Workaround: There is no workaround.

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

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

- CSCsv18579

  Symptoms: The logging buffer fills with this message:

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

  Note: The counter always increments by one.

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

  Workaround: There is no workaround.

- CSCsw18636

  Symptoms: High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

  Conditions: This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

  Workaround: Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

- CSCsx09110

  Symptoms: Cisco voice gateway may be unable to establish IPSec tunnel to a Cisco Call Manager (CCM)

  Conditions: Occurs when the gateway is running Cisco IOS Release 12.4(23.15)T3 or later.

  Workaround: There is no workaround.

- 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.

- CSCsx39263

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

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

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

- CSCsx87562

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

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

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

  Workaround:

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

- CSCsy74023

  Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory regions blocks.

  Conditions: This symptom is observed with a large number of IPSec peers (greater than 100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- CSCsz23099

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

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

  Workaround: There is no workaround.

- CSCsz68709

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

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

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

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

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

  Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

  Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** *IP- address* command listen for IP protocol 91 packets and UDP port 2067.

  Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  dlsw remote-peer 0 fst *ip-address*

  It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

  Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

  As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

  dlsw remote-peer 0 fst *ip-address*

  If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command.
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
    !--- configured on all interfaces of the affected device so that
    !--- it will be allowed by the CoPP feature.

    access-list 111 deny udp host 192.168.100.1 any eq 2067
    access-list 111 deny 91 host 192.168.100.1 any

    !--- Permit all other DLSw traffic sent to all IP addresses
    !--- configured on all interfaces of the affected device so that it
    !--- will be policed and dropped by the CoPP feature.

    access-list 111 permit udp any any eq 2067
    access-list 111 permit 91 any any

    !--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
    !--- traffic in accordance with existing security policies and
    !--- configurations for traffic that is authorized to be sent
    !--- to infrastructure devices.
    !--- Create a Class-Map for traffic to be policed by
    !--- the CoPP feature.

    class-map match-all drop-DLSw-class
     match access-group 111

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

    policy-map drop-DLSw-traffic
     class drop-DLSw-class
      drop
```

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

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

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic
     class drop-DLSw-class
      police 32000 1500 1500 conform-action drop exceed-action drop
```

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

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
    !--- from trusted hosts destined to infrastructure addresses.

    access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK eq 2067
    access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK

    !--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
    !--- all other sources destined to infrastructure addresses.

    access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
    access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK

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

    access-list 150 permit ip any any
```

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

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

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

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in customers environment.

- 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.

- CSCsz76616

  Symptoms: PPP negotiation does not occur.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.4(22)T2.

  Workaround: There is no workaround.

- CSCsz83570

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

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

  Workaround: Use 3DES for encryption.

- CSCta03194

  Symptoms: An IP packet gets corrupted in the disposition path of EoMPLS over ES+ cards when the VC is type 4.

  Conditions: The symptom is observed with an ScEoMPLS pseudowire terminated on an ES+ card.

  Workaround: There is no workaround.

- CSCta06451

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

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

Workaround: There is no workaround.

- CSCta57455

  Symptoms: Cisco 7600 router processor may crash.

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

  Workaround: There is no workaround.

- CSCta71873

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

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

  Workaround: There is no workaround.

- CSCta73054

  Symptoms: When using passive FTP with NAT VRF, the connection is broken after NAT in the Cisco 7300. The port numbers are not consistent.

  The source port is translated from “X_PORT” to “Y_PORT”, but after NAT to the outside, the port still remains the same. This breaks the passive FTP session.

  Conditions: This issue is observed when using Cisco IOS Releases 12.2(31)SB11, 12.2(31)SB14, 12.2(33)SB3a and 12.2(33)SB5 when using VRF NAT and trying to establish passive FTP connections across the Cisco 7300.

  Workaround: No issues are observed when Cisco IOS Release 12.2(25)S11 is used. The passive FTP session and NAT behave as expected.

- 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.

- CSCta96479

  Symptoms: IPv6 PPPoX session setup rate is low, dropping to about 10 sessions per second.

  Conditions: This symptom is observed under the following conditions:

  1. High number of PPPOX sessions with ipv6 ACLs
  2. IPV6 ACEs use port number
  3. IPV6 ACEs use icmp fields

  Workaround: There is no workaround.

- CSCtb07473

  Symptoms: There is a crash at ipc_print_flow_control_statistics upon issuing the **show ipc session** command.

Conditions: The symptom is observed when the router is booted up upon a redundancy forced switchover after an ISSU software upgrade. During the bring up on the console dump, the **show ipc session rx verbose** command is issued.

Workaround: There is no workaround.

- CSCtb09167

  Symptoms: The following issues can be observed with the PI11 image with a simple setup on both NPE-G1 and NPE-G2:

  1. There is a ~50% degradation on forwarding performance (with service reflect) on NPE-G1 when compared with Cisco IOS Release 12.4T.
  2. When the traffic rate goes higher than the router's capacity, traffic will not recover afterwards, even if the traffic is reduced back to a very low rate.

  Conditions: The symptom is specific to the service reflect feature.

  Workaround: There is no workaround.

- CSCtb13472

  Symptoms: An LDP session flap occurs between PE and P routers. A large number of LDP sessions going down may cause all LDP sessions within the routing context to go down temporarily, and then come back up (i.e.: flap).

  Conditions: This symptom is observed with 100 LDP-targeted sessions between the PEs. When the targeted sessions flap, the link session between PE and P routers also flaps. The symptom is not restricted to just targeted sessions flapping. Any large number of LDP sessions flapping within a routing context could cause all LDP sessions within the routing context to flap. In this example, all the LDP sessions are within the default (non-VRF) routing context.

  Workaround: There is no workaround.

- CSCtb44299

  Symptoms: In certain situations, the standby reloads.

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

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

- CSCtb51922

  Symptoms: Chunk leak of list element when a host-address under a PfR API provider is configured or unconfigured.

  Conditions: This symptom is observed when the following occur:

  1. PfR MC is configured
  2. API provider with a host address is configured
  3. Host address is unconfigured, or the MC process is shut/no shut.

  Workaround: There is no workaround.

- CSCtb60603

  Symptoms: The router crashes and resets when you try to execute the following command: **show run | format** *x* (where x = any keyword).

  Conditions: The symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(24)T. The router needs to have a general route-map configured.

Workaround: Do not execute **show run | format** *x* if there is a general route-map configured in the router.

- CSCtb69796

  Symptoms: The tunnel stitching VC may go down, resulting in traffic loss.

  Conditions: This 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: There is no workaround.

- CSCtb86439

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

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

  Workaround: There is no workaround.

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

- CSCtb88060

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

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

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

- CSCtb89424

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

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

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- CSCtb91412

  Symptoms: An IPv6 EIGRP session may go down if one of the IPv6 addresses configured on the interface is deleted.

  Conditions: This symptom is observed when more than one IPv6 address is configured on the interface, and one of the those addresses is then deleted.

  Workaround: There is no workaround.

- CSCtb92791

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

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

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

- CSCtc00106

  Symptoms: Packets are not routed across PPP over Frame Relay.

Conditions: Occurs during normal operations.

Workaround: There is no workaround.

- CSCtc03750

  Symptoms: The following error message can be seen on an SSO switchover:

  ```
  %RF-3-NOTIF_TID: Notification timer extended for the wrong client
  ```

  In addition, the secondary RP reloads continuously after an RP switchover.

  Conditions: The symptoms are observed when the router has been scaled with 2000 AToM, 1600 TE tunnels, 100 Ethernet over MPLS over GRE (EoMPLSoGRE) sessions, and 100,000 BGP routes.

  Workaround: There is no workaround.

- CSCtc05547

  Symptoms: Ping may fail on a Cisco 3845 integrated services router (ISR) or other low-end router where tunnel does not support turbo path.

  Conditions: This symptom is observed when L2VPN is configured over tunnel.

  Workaround: Do not configure L2VPN over tunnel.

- CSCtc12334

  Symptoms: The device crashes when you issue the **clear ip bgp *** command. This command deletes all BGP neighbor relationships and clears BGP RIB.

  Conditions: The symptom is observed under the following conditions:

  1. Need to have MDT configured.
  2. Need to issue the **clear ip bgp *** command.

  Workaround: There is no workaround.

- CSCtc13344

  Symptoms: Cisco Optimized Edge Routing (OER) experiences a fatal error and is disabled:

  ```
  %OER_MC-0-EMERG: Fatal OER error <> Traceback
   %OER_MC-5-NOTICE: System Disabled
  ```

  Conditions: This symptom is observed when configuring OER to learn the inside prefixes within a network by using the **inside bgp** command.

  Workaround: Disable prefix learning by using the **no inside bgp** command.

- CSCtc15394

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

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

  Workaround: There is no workaround.

- CSCtc16589

  Symptoms: A Cisco router may crash when bringing up PPPoE sessions.

  Conditions: This symptom is observed when bringing up 1000 PPPoE sessions from two ends, one a client router and the other the equipment of a third-party vendor.

  Workaround: There is no workaround.

- CSCtc17058

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

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

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

- CSCtc17311

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

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

  Workaround: There is no workaround.

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

- CSCtc22745

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

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

  Workaround: There is no workaround.

- CSCtc24959

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

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

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

- CSCtc27605

  Symptoms: The **show ip route vrf coke** command has no framed route when applied to “ip-vrf”.

  Conditions: This symptom is observed when a framed-route attribute is downloaded from the AAA server and applied to “ip-vrf”.

  Workaround: Configure VRF in the user profile where the template was used.

- CSCtc32063

  Symptoms: Cisco 7600 router with 12.2SRE software could reload when CFM D1 is configured.

  Conditions: The issue is observed on a Cisco 7600 running Cisco IOS Release 12.2(33)SRE when an ingress LAN card is configured as a MIP with CFM D1.

  Workaround: Use CFM D8 instead of CFM D1.

- CSCtc32375

  Symptoms: A Cisco SAF forwarder may crash when the **show eigrp service-family external-client** command is entered.

  Conditions: This symptom is observed when an external client attempts to register but omits the client-name attribute in the register message. The registration attempt will be rejected, but subsequent attempts to use the **show eigrp service-family external-client** command will crash the Cisco SAF Forwarder.

  Workaround: There is no workaround.

- CSCtc33785

  Symptoms: When a port-channel with MTP BD configuration (scaled to 1000) is removed and reconfigured, ES+ LC and SP crash.

  Conditions: Port-channel with a member link should configured with multiple c-mac bridge-domains.

  Workaround: Remove all EVCs or bridge-domains first, then remove the port-channel.

- CSCtc36588

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

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

  Workaround: Configure the MAC address as follows:

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

- CSCtc37147

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

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

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

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

- CSCtc38796

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

  Conditions: Seen only with RSP720.

  Workaround: There is no workaround.

- CSCtc39809

  Symptoms: Memory leak is seen at EIGRP component.

  Conditions: The symptom is observed when EIGRP encounters an SIA condition.

  Workaround: There is no workaround.

- CSCtc40677

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

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

```
!
ip prefix-list TEST seq 10 permit 0.0.0.0/0 ip prefix-list TEST seq 20 permit
10.0.0.0/8

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

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

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

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

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

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

- CSCtc41760

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

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

  Traceback will vary from code to code.

  Conditions: This symptom occurs when UDLD is configured.

  Workaround: Disable UDLD.

- CSCtc42737

  Symptoms: ES40 line card CPU remains high.

  Conditions: The problem is seen only when you have scaled number of sessions (20,000 sessions) and while bringing up 2,000 sessions and tearing down 2,000 sessions simultaneously at 24 CPS rate.

  Workaround: There is no workaround.

- CSCtc42941

  Symptoms: Standby is not coming up.

  Conditions: When a distribute-list is configured, the ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workarounds:

  1. When a access list is removed, remove corresponding distribute-list configuration as well.
  2. Do not use the same access list name for IPv4 and IPv6.

Further Problem Description:

```
router bgp 100
distribute-list sample in
exit
no ip access-list standard sample
ipv6 access-list sample
permit any any
write mem
```

- CSCtc44589

  Symptoms: Standby not coming up when **snmp-server enable traps** command is configured

  Conditions: The Standby fails to reach Standby HOT when **snmp-server enable traps** is configured.

  Workaround: Do not configure this command.

- CSCtc46174

  Symptom: A Cisco 10000 series router configured for ISG does not limit the number of redirected sessions, which could result in high CPU usage.

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

  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.

- 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.

- CSCtc52149

  Symptoms: SIP200 CPU 1 crash as indicated below.

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

  Conditions: There is no specific trigger to this problem. It happens randomly and recovers on its own.

  Workaround: There is no workaround.

- CSCtc52236

  Symptoms: SIP module crash.

  Conditions: There is no specific trigger to this problem. It happens randomly and recovers on its own.

  Workaround: There is no workaround.

  Further Problem Description: This happens when an IP packet removes padding calculated from ATM control.

- CSCtc52740

  Symptoms: Cisco 7600 ES+ interface will not accept policy map with “random-detect cos-based” statement.

  Conditions: CLI configuration is rejected on main interface of an ES+ line card.

  Workaround: There is no workaround.

- CSCtc54233

  Symptoms: After entering the EXEC command **clear xconnect all**, and then performing a Stateful Switchover (SSO) on the Cisco 7600, packets stop flowing via HDLC, PPP, or Frame Relay over Any Transport over MPLS (AToM) pseudowires.

  Conditions: This symptom has been observed with Cisco IOS Release 12.2SRE.

  Workaround: Enter **clear xconnect all** after switchover.

- CSCtc54257

  Symptoms: PPP fails to establish calls on an AAA dial-out scenario.

  Conditions: This symptom occurs in a dial-out scenario with a TACACS server.

  Workaround: Use a RADIUS server for AAA Dialout.

- CSCtc55937

  Symptoms: In **show spanning-tree mst** output, all links are in forwarding state.

  Conditions: This happens with EVC bridge domain configuration if the ports have EVCs with encapsulation untagged or default configured. Happens only on ESM20 cards.

  Workaround: Enable CFM globally using **ethernet cfm enable**.

- CSCtc57044

  Symptoms: The **mpls propagate-cos** command may not function correctly on a Cisco 7600 router.

  Conditions: This was observed on several Cisco 7600s running Cisco IOS Release 12.2(33)SRC.

  Workaround: Remove and reapply the **mpls propagate-cos** command.

- CSCtc59317

  Symptoms: A crash may occur when TE P2MP tunnels are deleted.

Conditions: The symptom is observed when a large number of TE P2MP tunnels are configured with “fast reroute” and one of the outgoing interfaces is shut so the path to some sub-LSPs is not available. If an attempt is made to delete one or more P2MP tunnels (using the **no interface tunnelX** command) while the TE tries to find a path for the down sub-LSPs, a crash may occur. The issue is seen with Cisco IOS Release 12.2SRE.

Workaround: Do not delete P2MP tunnels in this scenario.

- CSCtc60458

  Symptoms: On a Cisco 7600 router with a large number of VCs and VLANs, traffic stops forwarding traffic for several seconds while standby supervisor is booting.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC4.

  Workaround: There is no workaround.

- CSCtc60463

  Symptoms: The **traceroute mac** <*src_mac*> <*dst_mac*> command can cause a software crash on a Cisco 7600 router when configured with a large number of VLANs.

  Conditions: This occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRC4.

  Workaround: Do not use the **traceroute mac** <*src_mac*> <*dst_mac*> command. Use a specific VLAN ID when using this command.

- CSCtc65227

  Symptoms: Standby unit keeps reloading after forced switch-over.

  Conditions: Occurs in redundancy system when user renames a call-home profile to an empty string using the **rename** command under call-home configuration submode.

  Workaround: Do not rename a call-home profile name to empty string.

- CSCtc67032

  Symptoms: Range is not supported on an ACR interface and, when configured, results in undefined behavior leading to the standby reloading.

  Conditions: The symptom is observed when configuring “range” on an ACR interface.

  Workaround: There is no workaround.

  Further Problem Description: Range is not supported on an ACR interface configured on top of ATM interface. ATM interfaces do support the configuration of range for BBA features but ACR does not, as range is not a requirement for RAN space. So configuring “range” over the ACR interface causes the undefined behavior leading to the standby reloading.

- 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.

- CSCtc71207

  Symptoms: CPU usage goes to 100% with main offending process being “XDR mcast”. In addition, output for **show xdr linecard internal** shows constantly increasing totals for Etherbridge domain MAC security.

  Conditions: Seen in a topology that has numerous bridge-domain c-MAC instances configured on it.

Workaround: In some instances it has been seen that shutting the router's TFTP interface may reduce the CPU usage.

- CSCtc71996

  Symptoms: If "ip flow-export source *any logical interface*" is configured and then if the corresponding logical interface is deleted (but the flow-export configuration remains), the SSO will not work.

  Conditions: The symptom occurs when "ip flow-export source" is already configured with the logical interfaces, followed by the deletion of the logical interface during an SSO.

  Workaround: Use the **ip flow-export source** command to export the flows through any physical interface.

- 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.

- CSCtc75687

  Symptoms: Some commands with large outputs allow the use of ctrl-^ to stop the output before completion. This can cause a crash.

  Conditions: Unknown at this time.

  Workaround: Enter the **no parser command serializer** command.

- CSCtc80800

  Symptoms: The standby unit keeps reloading after a forced switchover.

  Conditions: The symptom is observed if you configure a call-home profile name that includes a quote (").

  Workaround: Do not include a quote among the profile name string.

- CSCtc80850

  Symptoms: Packets are received twice. Packet counters shows twice the number of packets than packets sent.

  Conditions: The symptom is observed with an MTP EVC configuration on UNI interfaces.

  Workaround: There is no workaround.

  Further Problem Description: The issue seems to occur with the script. It cannot be recreated with a manual configuration.

- CSCtc81358

  Symptoms: The Standby RP reloads after an SSO.

  Conditions: The symptom is observed with a scaled L3VPN scenario.

  Workaround: There is no workaround.

- CSCtc81653

  Symptoms: The system crashes if the port-channel is removed while it is serving data traffic.

  Conditions: Port-channel is configured with the member links in it. The traffic is sent through the port-channel. If the port-channel is removed, the system sometimes crashes.

Workaround: There is no workaround.

- CSCtc84960

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

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

  Workaround:

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

  Further Problem Description: P2MP tunnels doesn’t forward the traffic on head end after the reload because of the FPOE programmed Incorrectly. Here we see the traffic hitting the tunnel interface but not the outgoing physical interface. FPOE was not getting populated due to empty port lists.

- 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.

- CSCtc86490

  Symptoms: Error message stating “Can’t install service policy with empty name” is displayed.

  Conditions: When an invalid service policy is pushed from the DBS on to the VC, the error message is thrown and the policy on the VC does not fall to the default.

  Workaround: There is no workaround.

- CSCtc90579

  Symptoms: Router crashes due to memory corruption during MPLS TE auto backup tunnel deletion.

  Conditions: Caused by topology changes triggering backup tunnel deletion and RSVP hello mechanism.

  Workaround: Gloablly, disable RSVP hello and enable BFD hello:

  ```
  Router(config)#no ip rsvp signalling hello
  Router(config)#ip rsvp signalling hello bfd
  Per MPLS TE enabled interface:
  Router(config-if)#no ip rsvp signalling hello
  Router(config-if)#ip rsvp signalling hello bfd
  ```

- 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.

- CSCtc91567

  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.

- 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.

- CSCtc91599

  Symptoms: High CPU is observed when about four percent of PPPoE sessions are churned in a scaled setup, on the ES+.

  Conditions: The symptom is observed with broadband field deployment with PPPoE access.

  Workaround: There is no workaround.

- CSCtd00054

  Symptoms: Link flap/down on PA-MC-T3E3-EC interface.

  Conditions: This symptom is observed when changing encapsulation after reload.

  Workaround: Perform an online insertion and removal (OIR) of the PA.

- CSCtd00070

  Symptoms: If “arp ignore local” is configured under “ip subscriber l2-connected” submode on an interface, ISG will no longer reply to ARPs coming to that interface if the ARP destination IPs are in the same subnet as the ARP source IP, or if the ARP destination IP is not in the subnet of ISG but is routable from the interface where the ARP is received.

  Conditions: The symptom is observed if “arp ignore local” is configured under “ip subscriber l2-connected” submode.

  Workaround: There is no workaround.

Further Problem Description: If this session is in VRF mapping or transfer mode, and the CPE's ARP is for an IP on the access interface that happens to be reachable in the VRF by ISG (e.g.: due to VRF IP spaces overlapping or VRF's default route is set to matching all traffics), the ARP request will receive a reply, even with the above configuration, unless the destination IP is in the same VRF subnet as the VRF's MSI. Note that when the CPE receives ISG's ARP reply in this case and routes the corresponding IP packets to ISG, ISG will route the packet in the VRF space.

- CSCtd00479

  Symptoms: When ISIS is configured for NSF IETF, if the restarting router is a DIS on the LAN, after a switchover the ISIS database and topology could be incorrect. This results in an incorrect routing table.

  Conditions: The symptom is observed when ISIS is configured for NSF IETF and a switchover occurs.

  Workaround: Use NSF CISCO, or disable NSF.

- CSCtd05318

  Symptoms: A watchdog exception crash on "MRIB Transaction" may be observed on a new active RP when an RP switchover is initiated.

  Conditions: The symptom is observed during an RP switchover under a scaled scenario with a router configuration with approximately 1K EBGP peers with 500K unicast routes and 300 mVRFs with 1K mcast routes.

  Workaround: There is no workaround.

- CSCtd09035

  Symptoms: Seeing traffic forwarding drop randomly in L3VPN P2MP testing when doing fast reroute (FRR) test. Tunnels are up, but hardware does not forward traffic.

  Conditions: Occurs with L3VPN P2MP bud node router.

  Workaround: There is no workaround.

- CSCtd11757

  Symptoms: QoS applied on main interface/subinterface is not applied on session traffic on the main interface/subinterface. Also, QoS is not applied to a session following a SPA OIR.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)SRD.

  Workaround: Apply session-specific QoS (control plane policy).

- CSCtd13603

  Symptoms: A Cisco device may crash after the **show cef switching reinject handles** command is entered.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCtd16512

  Symptoms: Web Cache Communications Protocol (WCCP) redirection cannot be configured with a non-default VRF on a subinterface.

  Conditions: This symptom is observed when configuring WCCP redirection with a non-default VRF on a subinterface.

  Workaround: There is no workaround.

- CSCtd18510

  Symptoms: A Cisco router may crash and display a SegV exception error.

  Conditions: This symptom is observed on a Cisco router when OSPF connects the CE and PE routers in an MPLS VPN configuration, and when none of the interfaces are in area 0. This symptom is seen only in Cisco IOS Software versions with the OSPF Local RIB feature.

  Workaround: Enter the **no capability transit** command in the OSPF routing processes.

- CSCtd21969

  Symptoms: The following error message for MFIB sub-block occurs:

  ```
  INTERFACE_API-3-NODESTROYSUBBLOCK
  ```

  Conditions: The symptom is observed when running virtual access interfaces when multicast is enabled.

  Workaround: There is no workaround.

- CSCtd24840

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

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

  Workaround: There is no workaround.

- CSCtd25133

  Symptoms: Router gets into APS channel mismatch state.

  Conditions: Observed with MGX connected as APS peer, when both MGX cards (active and standby) are reloaded simultaneously.

  Workaround: Force APS switchover.

- CSCtd25933

  Symptoms: Active or standby RP crashes on executing the **shut** then **no shut** commands on the interface.

  Conditions: The symptom is observed with the following conditions:

  1. Encapsulation QnQ (or dot1q) is configured and removed on the sub-interface, on a WAN interface (SIP400).
  2. Same VLAN configured as Encapsulation QnQ (or dot1q) on a LAN interface (ES+).
  3. Perform shut/no shut on the ES+ interface.

  Workaround: There is no workaround.

- CSCtd26215

  Symptoms: A Cisco router reports for no apparent reason that an update is malformed or corrupted. When generating an update, the router reports

  ```
  %BGP-4-BGP_OUT_OF_MEMORY
  ```

  and the BGP resets. The update is not malformed and the router is not running out of memory, but BGP falsely believes that there is no more memory available.

  Conditions: This symptom is observed when BGP damping with routemap is configured on a Cisco router running Cisco IOS Release 15.0(1)M, Release 12.2 (33)SRE, Release 12.2(33)SRD3, or Release 12.2(33)SRC5.

  Workaround: Remove the BGP damping routemap.

- CSCtd27247

  Symptoms: The router crashes when doing concurrent VRF add and deletion configurations.

  Conditions: The symptom is observed when a multiple configuration terminal is doing concurrent VRF add and deletion configurations.

  Workaround: Do not do concurrent VRF addition and deletion.

- 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's 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.

- CSCtd40804

  Symptoms: The EVC configuration does not exist on the ES20 line card. The first "show" command (below) shows that the EVC was known to the Route Processor (RP) on the Supervisor Engine, while the second command shows that the EVC did not exist on the ES20 line card in slot 4:

  ```
  #sh ethernet service instance id 3555 interface gi4/0/1
  Identifier Interface State CE-Vlans 3555 GigabitEthernet4/0/1 UP

  #remote command mod 4 sh ethernet service instan id 3555 int gi4/0/1
  EFP ID 3555 on interface GigabitEthernet4/0/1 does not exist
  ```

  Conditions: The symptom is observed after a Supervisor switchover.

  Workaround: There are two workarounds for this issue. Both require that every port on the ES20 be configured prior to a switchover. If this is done, then the problem will not exist after a switchover and new EVCs can be successfully added following the switchover.

  1. Configure at least one service instance under each interface on the ES20. An example is shown below:

     ```
     interface GigabitEthernet1/0/3 service instance 1 ethernet encapsulation dot1q 3
     ```

  2. Configure "ethernet uni id *name*" under each interface on the ES20. An example is shown below:

     ```
     interface GigabitEthernet1/0/5 ethernet uni id gi_1_0_5
     ```

- 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 (>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.

- CSCtd49801

  Symptoms: The "ip sla reaction" configuration resets after restarting the Collector.

  Conditions: The symptom is observed with the following conditions:

  1. A Collector is created for specific device with an Echo operation.
  2. The Collector is stopped and the device is configured follows:

     ```
     ip sla reaction-configuration 167086 react timeout threshold-type xOfy 2 3
     action-type trapOnly
     ```

  3. The Collector is stopped again and the configuration is unexpectedly modified as follows:

     ```
     ip sla reaction-configuration 167086 react timeout threshold-type immediate
     action-type trapOnly
     ```

     (The threshold-type has modified from "xOfy 2 3" to "immediate".)

  4. It is seen with IPM 4.2.

  Workaround: There is no workaround.

- CSCtd54338

  Symptoms: The following output from the command **show ip rtp header-compression**, shows that one channelized serial interface has a large accumulated number of "seconds since line card sent last stats update" compared with another channelized serial interfaces in device with the same platform:

```
GR_SA_CORE_7613R_1#show ip rtp header-compression Serial1/2/0.1/3/1:0
 RTP/UDP/IP header compression statistics:
   Interface Serial1/2/0.1/3/1:0 (compression on, Cisco)
   Distributed fast switched:
   10364 seconds since line card sent last stats update
     Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
              0 dropped, 0 buffer copies, 0 buffer failures
     Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
              0 bytes saved, 0 bytes sent
     Connect: 16 rx slots, 16 tx slots,
              0 misses, 0 collisions, 0 negative cache hits, 0 free contexts
```

  Sometimes there is also a one-way call signaling problem.

  Conditions: The symptom is observed with the following conditions:

  - Cisco IOS Release 12.2(33)SRD3.
  - Platform: Cisco 7613 router.
  - RP: RSP720-3CXL-GE.
  - SIP: Cisco 7600 SIP-200.
  - SPA: SPA-1XCHSTM1/OC3.

  This issue normally begins to show when the count of the channelized subinterface (number of cRTP sessions) is 200 or over.

  Workaround: Disable then enable RTP header-compression on the interface.

  Further Problem Description: The issue can be resolved by using **disable cRTP** and **enable cRTP** on each subinterface (see DDTS CSCso48621). However, sometimes the problem can reoccur in a few days after recovery on the same subinterface.

- CSCtd55219

  Symptoms: Potential traffic loss on NSF switchover. The debugs show:

```
BGP(base): waited 0s for the first peer to establish
```

  With the correct behavior, you should see:

```
BGP(base): will wait 60s for the first peer to establish
```

  Conditions: The symptom is observed with BGP NSF.

  Workaround: There is no workaround.

- CSCtd59174

  Symptoms: PfR MC logs an Exit Mismatch after controlling a traffic class using policy based routing (PBR). At this point, PfR uncontrols the traffic class because it appears that traffic is not flowing over the exit interface that is expected.

  Conditions: This condition is observed under the following conditions:

  - At least one Cisco Catalyst 6000 PfR BR must by configured.

  - Monitor mode must include passive monitoring such as mode monitor both or mode monitor passive.

  Workaround: Apply mode monitor active policy to the traffic classes controlled by PBR. Note, however, that this will prevent these traffic classes from being used for load, range, or cost policies.

- CSCtd66014

  Symptoms: ES+ line card crashes at powerup of a Cisco 7600 router that is running Cisco IOS Release 12.2SRE image if either the Traffic Manager or Frame memories in the ES+ Network processors report a double bit ECC error. The ES+ line card crashinfo will have the following string:

  ```
  %NP_DEV-DFC2-3-ECC_DOUBLE: Double-bit ECC error detected on NP 0, Mem 19,
   SubMem 0x1,SingleErr 1, DoubleErr 1 Count 1 Total 1
  ```

  Conditions: Router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCtd66837

  Symptoms: When the First Search memory in the ES+ Network processor detects a single bit ECC error, it is incorrectly decoded in Cisco IOS as a double bit ECC error. The recovery action for a double bit ECC error is a crash and reload of the line card.

  Conditions: This symptom is seen if the Search memory in any of the ES+ Network processors encounters a single bit ECC error.

  Workaround: There is no workaround. Crash cannot be avoided due to this false alarm.

- CSCtd66918

  Symptoms: Standby Supervisor continually resets during detection of bad hardware in the system.

  Conditions: The symptom is observed when the bad line card is inserted in the slot following the Standby Supervisor slot (e.g.: Standby Supervisor in slot 6 and bad line card in slot 7).

  Workaround: There is no workaround.

- CSCtd70439

  Symptoms: A packet buffer leak may occur when using the Service Reflect feature.

  Conditions: This symptom is observed when an uncoalesced input packet is received by the service reflect VIF in the fast-switching context. The input packet will not be freed after obtaining a new packet buffer and coalescing the input packet into the new buffer.

  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.

- CSCtd72426

  Symptoms: Checkpointing facility on the standby SP is leaking memory buffers. This can lead to a WATERMARK error message.

Conditions: The symptom is observed with the checkpointing facility on the standby SP.

Workaround: There is no workaround.

Further Problem Description: This issue can be checked with the command **show ipc session all verbose** from the standby SP. This output will show more messages requested then messages returned for the client "CHKPT:STANDBY SP" and this difference will grow every day. The **show check client** command from the standby SP will show the buffers held for "REP CHKPT CLIENT" and that this value is increasing over time.

- CSCtd72462

  Symptoms: A Cisco 7600 series router with an RSP720-3C processor may unexpectedly reboot after the **show policy-map interface** command is executed.

  Conditions: The issue is seen when there is a policy map on an interface with the following:

  - No set action.
  - No shared aggregate policer action.
  - No aggregate policer action.
  - uflow policer with "conform action" configured.

  Workaround: There is no workaround.

- CSCtd73256

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

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

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

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

```
Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1
```

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

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```

  Workaround: There is no workaround.

- CSCtd75033

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
<output truncated>
```

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

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

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in “White Paper: Cisco IOS Reference Guide” at the following link:

http://www.cisco.com/warp/public/620/1.html

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

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

* NTP Access Group

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

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

access-list 1 permit 171.70.173.55

!--- Apply ACE to the NTP configuration

ntp access-group peer 1
```

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

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

* Infrastructure Access Control Lists

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

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

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

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

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

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

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

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

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

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

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

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

```
access-list 150 permit ip any any

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

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

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

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

* Control Plane Policing

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

- Filtering untrusted sources to the device.

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

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

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

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 123

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

access-list 150 permit udp any any eq 123

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

```
!--- the CoPP feature

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

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

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

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

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

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

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

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

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

access-list 150 permit udp any any eq 123

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

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

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

policy-map rate-udp-traffic
 class rate-udp-class
```

```
  police 10000 1500 1500 conform-action transmit
        exceed-action drop violate-action drop

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

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

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

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

- CSCtd75248

  Symptoms: With QoS is disabled globally and when the ES20 interface is configured as a trunk, if traffic is sent with a valid COS value, the ES20 re-marks all COS values to “0”.

  Conditions: The symptom is observed when QoS is globally disabled.

  Workaround: Enable QoS globally using **mls qos** and trust the ES20 trunk interface to retain COS values using **mls qos trust cos**.

  Further Problem Description: This issue is not seen in Cisco IOS Release 12.2(33)SRB. It is present in Cisco IOS Release 12.2(33)SRC onwards

- CSCtd77905

  Symptoms: Traffic will not flow properly for the first VRF, if there is a switchover from active to standby. This issue occurs because of a race condition.

  Conditions: The symptom is observed only in the HA setup.

  Workaround: Delete and reconfigure the problematic VRF.

  Further Problem Description: The problem is a timing issue. In the standby Supervisor, the aggregate labels are not getting programmed properly for the first VRF configured in the system.

- CSCtd80007

  Symptoms: The standby routing processor crashes during an SSO when TE auto- tunnel backup is enabled.

  Conditions: The symptom is observed during an SSO only on a new standby RP when TE auto-tunnel backup is in use.

  Workaround: Disable TE auto-tunnel backup.

- CSCtd87264

  Symptoms: DHCP unicast BootP offers can not be propagated back in the incoming interface as the ARP entry is missing. This happens only when the relay function is combined in a VRF and the incoming interface is unnumbered.

  Conditions: The symptom is observed when SRD/SRE Cisco 7600 series router is a DHCP relay/snooping agent. The request must come in a VRF.

  Workaround: Move the relay agent function to the global routing table.

- CSCtd90429

  Symptoms: VPLS traffic occasionally gets blackholed after multiple iterations of mid-point failure or reoptimization.

  Conditions: The symptom is observed when the core-facing interfaces are SIP400.

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

- CSCtd94128

  Symptoms: On ES+ cards, packets in the egress direction do not have the outer tag preserved.

  Conditions: This is seen on a port-mode configuration for an L2TPv3 tunnel where tagged packets are sent from the subscriber. The outer tag is always rewritten to null while the COS bits are preserved.

  Workaround: There is no workaround.

- CSCtd94438

  Symptoms: When the **show memory** *fast* **fragment detail** command is given, it leads to a crash of the Cisco 7600 series router. The console logs show some semaphore lock-related messages, IPC/XDR messages, and RP crash-related messages.

  Conditions: The symptom is observed when BFD is enabled and the **show memory** *fast* **fragment detail** command is given.

  Workaround: Avoid using the **show memory** *fast* **fragment detail** command, or disable BFD from the startup configuration and reload the router.

  Further Problem Description: If BFD is disabled in the startup configuration (i.e.: BFD is not configured when bringing up the router) the crash is not seen.

- CSCtd99244

  Symptoms: ES+ line card crashes reporting double bit ECC error.

  Conditions: This symptom occurs usually in the initial phases of line card bootup, but this has also been reported after a few hours of traffic through the ES+ line card ports.

  Workaround: There is no workaround. The ES+ may not report this error in the second reload. If errors persist, powercycle the chassis, or OIR the ES+.

- CSCtd99248

  Symptoms: There could be occasional double bit ECC errors for the traffic manager and other metadata memories that are reported on the Network processor on the ES+ line card.

  Conditions: This symptom is observed when the router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- 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.

- CSCtd99916

  Symptoms: After a quick activation/deactivation of a BGP neighbor in the VPNv4 address family, the router can have a unexpected reload. Traceback shows:

  ```
  1#9ef25813351d0da79497b4305144eadc :10000000+5A9860 :10000000+5A9BE4
  :10000000+10B9CA0 :10000000+10BEF34 :10000000+421761C :10000000+2AD6FC
  :10000000+2ADA28 :10000000+2FA91C :10000000+2FAF84 :10000000+2E748C

  Exception to IOS Thread: Frame pointer 35233FD8, PC = 1027203C

  ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = BGP Router
  -Traceback= 1#9ef25813351d0da79497b4305144eadc :10000000+27203C :10000000+271DAC
  :10000000+273218 :10000000+2741B8 :10000000+33AE64 :10000000+33B5C4 :10000000+291D2C
  :10000000+2921C8 :10000000+2928AC
  ```

  Conditions: The symptom is observed whenever an old style multicast update is received and it uses the same AF value as that for VPNv4. Cisco IOS Release 12.2(33)XNE has code that detects this behavior, hence the traceback.

  Workaround: Use new-style MDT peering.

- CSCte02087

  Symptoms: With a port-channel on the interface of a ES+, performing a **shut** on the port-channel or adding/removing members of the port-channel causes a CPU hog with the following trace back:

  ```
  %SYS-DFC13-3-CPUHOG: Task is running for (4000)msecs, more than (2000)msecs
  (0/0),process = SCP Hybrid process.
  -Traceback= 0x9272FA8z 0x81B0288z 0x81B36E4z 0x93CC1F4z 0x93CC264z 0x93B69F8z
  0x93A8C0Cz 0x93C928Cz 0x93C9CE8z 0x93C7BC8z 0x914A1D4z 0x913F148z 0x9255EA8z
  0x92501C0z
  ```

  Conditions: The symptom is observed on a Cisco 7600 series router with around 3k subinterfaces configured on a port-channel interface.

  Workaround: There is no workaround.

- CSCte02184

  Symptoms: An L2TPv3 tunnel fails to establish when the access-facing card is an ES+ Combo card.

  Conditions: The symptom is observed when tunnels fail to establish while hardware switching is enabled.

  Workaround: There is no workaround.

- CSCte06443

  Symptoms: The IPv6 configuration shows incorrectly in running configuration. Additionally, the configuration may disappear after a reload:

  ```
  7200-7(config)#int lo 0
  7200-7(config-if)#ipv6 address 2001:0dB8:FFFF::2/128 ----> configured address
  7200-7(config)#^Z
  7200-7#sh run int lo 0 interface Loopback0
  ip address 10.195.95.2 255.255.255.255
  ipv6 address /1698840608 -------> displayed address end
  ```

  after a reload it becomes like this:

  ```
  7200-7#sh run int lo 0
  interface Loopback0
  ip address 10.195.95.2 255.255.255.255
  ```

  Conditions: The symptom is observed only with an “spservice” image of a Cisco IOS SRE Release.

  Workaround: There is no workaround.

- CSCte07666

  Symptoms: A Cisco router may crash when the TCL script without_completion.tcl is run.

  Conditions: This symptom is observed when running the TCL script without_completion.tcl as the script tries to fill in the _cerr_name field with an array that is not sufficiently populated.

  Workaround: There is no workaround.

- CSCte10706

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

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

  Workaround: There is no workaround.

- 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

- CSCte21958

  Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.

  Conditions: This symptom is observed when the following sequence of commands is entered:

  - configure terminal
  - interface Ethernet0/0.1
  - encapsulation dot1Q 400
  - xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test
  - pseudowire-class test
  - encapsulation l2tpv3
  - protocol l2tpv3 test
  - ip local interface Loopback0
  - vpdn enable

  This symptom affects all platforms.

Workaround: Define the pseudowire class using the **pseudowire- class** configuration command before referencing that pseudowire class in an xconnect configuration.

- CSCte28933

  Symptoms: L2TPv3 VLAN-mode reassembled packets get dropped on ES+.

  Conditions: The symptom is observed when “L2TPv3 cookie” is configured and L2TPv3 packets get fragmented in the core or at source.

  Workaround: Configure L2TPv3 without cookies.

- CSCte37192

  Symptoms: Traffic is dropped in the egress by SIP400.

  Conditions: The symptom is observed when BRE is configured, then removed, then reconfigured. Then perform a shut/no shut on the interface where the PVC is present.

  Workaround 1: Perform a shut/no shut on the interface.

  Workaround 2: Perform a SPA OIR.

- CSCte38652

  Symptoms: The standby reloads due to one of the line cards getting powered down with the reason given as: “Failed to configure the linecard”.

  Conditions: The symptom is observed with a fully-loaded setup with all ESM20G cards and a large amount of configuration.

  Workaround: There is no workaround.

- 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.

- CSCte48009

  Symptoms: The NAS-Port and NAS-Port-ID AAA Attributes are not sent in radius messages.

  Conditions: The symptom is observed if the VCI value configured on the interface is larger than 32767.

  Workaround: Use VCI values less than 32767.

- 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.

- CSCte48935

  Symptoms: Following a reload, the ES20 port is unbundled from the port-channel and the following error message is shown:

  Port-channel10 and TenGigabitEthernet9/0/0 have different trust states

  Conditions: The symptom is observed with “mls qos” disabled globally and “mls qos trust” disabled on the ES20 interface.

Workaround: Enable “mls qos” on the router. If “mls qos” is not desired, there is no workaround.

- CSCte50573

  Symptoms: Degraded performance with RLB and T-RLB.

  Conditions: The symptom is observed with the following conditions:

  1. SLB is configured with service radius.
  2. High CPU even at lower rates of 300 TPS.
  3. Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- 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 Cisco IOS Release 12.2(33)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.

- CSCte60000

  Symptoms: Destination prefix is not collected for IP to MPLS packet flow in netflow aggregation cache.

  Conditions: The symptom is observed in a VRF + MPLS setup.

  Workaround: Collect prefix in non-VRF + MPLS setup.

- CSCte66046

  Symptoms: MDT entries are missing in MPLS forwarding table of P router after OSPF flap on edge router.

  Conditions: The symptom is observed on IGP flap in the core.

  Workaround: Flap MLDP on P or PE router.

- CSCte68259

  Symptoms: Random end-to-end traffic failure with an ES+ line card with L2TPv3 termination on one port which is interfacing with EVC BD remotely.

  Conditions: This issue occurs when the ES+ line card is configured with the L2TPv3 feature.

  Workaround: There is no workaround.

- CSCte69014

  Symptoms: Multiple memory leaks are seen when you try to bring up an unauthenticated session:

```
0x11FF95E0       7812      37  AAA Request Data
 0x11FFA020       4692      18  SSS AAA auth req
```

```
0x11CBD48C       1692      18  AAA AUTHEN Username
```

Conditions: The symptom is observed when a TAL authorization failure occurs due to access-reject. When you try to bring the session up again this leak is seen.

The steps are:

1. Configure L2-connected session.
2. Bring up an L2-connected IP session and verify the access-reject event is triggered.
3. Check for these leaks using “show memory” commands.

Workaround: There is no workaround.

- CSCte75406

  Symptoms: A crash can occur if the memory is low during the initialization of the OSPF process.

  Conditions: The symptom is observed if the memory is low during OSPF process initialization.

  Workaround: There is no workaround.

- CSCte77990

  Symptoms: QoS marking does not work.

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

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

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

- CSCte78805

  Symptoms: Free memory is going down because SSS Manager is growing.

  Conditions: The symptom is observed when there is an error configuration on user/service profile.

  Workaround: Correct the configuration error.

- CSCte78958

  Symptoms: “%BGP-3-NEGCOUNTER” can appear during graceful restart.

  Conditions: The symptom is observed with non-NSF graceful restart on branches with the fix for CSCtd99802.

  Workaround: There is no workaround.

- CSCte95228

  Symptoms: The line card 7600-ES+ on a Cisco 7600 series router may reload due to memory corruption.

  Conditions: One of the conditions is cable pull with scaled configurations. This is seen with VPLS configuration only so far. This is a rare situation and seen only once.

  Workaround: Shut the port on which OIR is done.

- CSCte97615

  Symptoms: BFDv6 will not work with ipservices images on a Cisco 7600 series router.

  Conditions: The symptom is observed with normal loading of an ipservices image (as the subsystem itself is missing for BFDv6).

  Workaround: There is no workaround.

- CSCtf02916

  Symptoms: IPv6 multicast traffic is not replicated properly after a shut/no shut.

  Conditions: The symptom is observed when you do a **shut** followed by a **no shut** to a port downstream.

  Workaround: Set replication mode ingress.

- CSCtf12803

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

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

  Workaround: There is no workaround.

- CSCtf15927

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

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

  Workaround: Clear the tunnel manually.

- CSCtf16623

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

  Conditions: The symptom is observed with basic functioning.

  Workaround: There is no workaround.

- CSCtf17273

  Symptoms: A Cisco router crashes during startup when receiving an AS_SET attribute from its peer.

  Conditions: This symptom is observed when the BGP peer sends an AS_PATH or AS4_PATH containing an AS_SET attribute.

  Workaround: There is no workaround.

- CSCtf20182

  Symptoms: Duplicated traffic is received on all sub-LSPs, due to a mid-point packet replication issue.

  Conditions: The symptom is observed on a Cisco 7600 series router as a mid-point, a primary tunnel with FRR protection, and when link failure is recovered.

  Workaround: There is no workaround.

- CSCtf22968

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

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

  Workaround: There is no workaround.

- CSCtf25124

  Symptoms: PIM neighborship is not getting established in an MVPN scenario.

  Conditions: The symptom is observed in an MVPN scenario with MLS switching enabled. The PIM neighbor address is not found.

  Workaround: Disable MLS switching.

- CSCtf27187

  Symptom: Traffic stops after doing SPA OIR.

  Conditions: This symptom is observed only while doing SPA OIR.

  Workaround: Do a SIP OIR; the traffic resumes.

- 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.

- CSCtf47216

  Symptoms: Traffic duplication occurs when the egress line card has both primary and backup path configured.

  Conditions: The symptom is observed on an LSM with TE-FRR on the bud node.

  Workaround: There is no workaround.

- CSCtf50862

  Symptoms: With MAC OOB feature enabled, on the router bootup, in steady state, mac addresses [both core and access side] are flushed out periodically resulting in traffic flooding across all ports

  Conditions: The problem can occur when MAC OOB is enabled by the **mac-address-table synchronize**command.

  If we have EVC-pc on access and VPLS in the core, and traffic flow is assymetric, then, this can result in flooding of the traffic from access to core and core to access

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

- CSCtf56678

  Symptoms: Aggregate policer starts dropping traffic before reaching the configured Committed Information Rate (CIR).

  Conditions: The symptom is observed when the PFC QoS aggregate policer is configured and when the CIR configured is above 1370 Mbs. For example:

```
Policy Map POLICER-IN
    Class class-default
     police cir 1380000000 bc 31250000
       conform-action transmit
       exceed-action drop
```

  Workaround: Configure a value below or equal to cir 1370000000.

- CSCtf75587

  Symptoms: Active RP crashes when ISSU upgrade is initiated (SSO mode) from Cisco IOS Release 12.2(33)SRD3 to Release 12.2(33)SRD4 or latest Cisco IOS Release 12.2(33)SRE (post Release 12.2(33)SRE0a and pre Release 12.2(33)SRE1).

  Conditions: This symptom occurs when the **mls qos** command is configured on the router, and then SSO mode ISSU switchover is initiated.

  Workaround: ISSU upgrade in RPR mode.

- CSCtf78076

  Symptoms: An ISSU from Cisco IOS Release 12.2(33)SRD4 to Cisco IOS Release 12.2(33)SRE1 fails due to a configuration synchronization issue. There will be a secondary reset and it will go to RPR mode.

  Conditions: The symptom is observed with an ISSU SSO.

  Workaround: Use the **redundancy config-sync ignore mismatched-commands** command to ignore the config sync and to proceed with the remaining ISSU process.

Open Caveats—Cisco IOS Release 12.2(33)SRE0a

Cisco IOS Release 12.2(33)SRE0a is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are open in Cisco IOS Release 12.2(33)SRE0a. This section describes only select open caveats.

- CSCtf83092

  Symptoms: Standby resets continuously on ISSU run.

  Conditions: This issue is seen with mpls vc configuration.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE0a

Cisco IOS Release 12.2(33)SRE0a is a rebuild release for Cisco IOS Release 12.2(33)SRE. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRE0a but may be open in previous Cisco IOS releases.

- CSCtd66014

  Symptoms: ES+ line card crashes at powerup of a Cisco 7600 router that is running Cisco IOS 12.2SRE image if either the Traffic Manager or Frame memories in the ES+ Network processors report a double bit ECC error. The ES+ line card crashinfo will have the following string:

  ```
  %NP_DEV-DFC2-3-ECC_DOUBLE: Double-bit ECC error detected on NP 0, Mem 19, SubMem
  0x1,SingleErr 1, DoubleErr 1 Count 1 Total 1
  ```

  Conditions: Router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCtd99244

  Symptoms: ES+ line card crashes reporting double bit ECC error.

  Conditions: This symptom occurs usually in the initial phases of line card bootup, but this has also been reported after a few hours of traffic through the ES+ line card ports.

  Workaround: There is no workaround. The ES+ may not report this error in the second reload. If errors persist, powercycle the chassis, or OIR the ES+.

- CSCtd99248

  Symptoms: There could be occasional double bit ECC errors for the traffic manager and other metadata memories that are reported on the Network processor on the ES+ line card.

  Conditions: This symptom is observed when the router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCte18253

  Symptoms: MFIBv6 is not supported in advipservices images.

  Conditions: This symptom occurs when trying to deploy IPv6 Multicast.

  Workaround: There is no workaround.

  Further Problem Description: IPv6 Multicast subsystems are missing the advipservices images.

Open Caveats—Cisco IOS Release 12.2(33)SRE

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRE. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRD. This section describes only select open caveats.

- CSCeh32251

  Symptoms: A mismatched bandwidth may generate corrupt packets that are not detected in the hardware when CRC-16 is configured on the interfaces. The corrupt packets may cause the CPU usage of the RP to increase to 100 percent, and the corrupt packets may be dropped.

  Conditions: This symptom is observed on a Cisco platform that is configured with a 2-port or 4-port clear channel T3/E3 SPA (SPA-2XT3/E3 or SPA-4XT3/E3) or 4-port channelized T3 (DS0) SPA (SPA-4XCT3/DS0) that is configured for T3 DSU Kentrox mode with a subrate bandwidth above 35,000 when the far-end is also configured for DSU Kentrox mode but with a mismatched bandwidth that is less than 35,000

  Workaround: When you use DSU Kentrox mode, configure CRC-32 on the interfaces and configure the correct bandwidth before you enable the interfaces.

- CSCsj43861

  Symptoms: EzVPN hardware client will not attempt to connect to the same peer or the next peer after QUICK MODE failure during IKE.

  Conditions: This symptom is observed when EzVPN hardware client remains in SS_OPEN state after the failure of QUICK MODE.

  Workaround: Clear the EzVPN session.

- CSCso07705

  Symptoms: Tracebacks seen on Cisco 7200 router.

  Conditions: Occurs when SSH is used to connect to Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) multilink IP address.

  Workaround: There is no workaround.

- CSCsr42769

  Symptoms: When multiple transform set is configured to the crypto map, only the first transform set is configured to it. Remaining transform sets are truncated and not configured to it.

  Conditions: Multiple transform sets have to be configured to the crypto map.

  Workaround: There is no workaround.

- 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.

- CSCta10835

  Symptoms: Ingress IPv6 packet classification not working.

  Conditions: Occurs only on MFR interface on Cisco 7600.

  Workaround: Use sub-interface mode.

- CSCta57455

  Symptoms: Cisco 7600 router processor may crash.

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

  Workaround: There is no workaround.

- CSCta77577

  Symptoms: Traffic stops after a switchover.

  Conditions: Occurs on DMFR on SIP-200 in a high-availability setup, following an online insertion and removal (OIR) and the **redundancy force switchover** command.

  Workaround: Enter **hw-module module** <*no*> **reset** on the new active supervisor.

- CSCtb09080

  Symptoms: A Cisco 7600 RP may crash.

  Conditions: May occur when the following commands are entered in succession:

  * no router bgp [AS]

  * no ipv6 unicast-routing

  Workaround: There is no workaround.

- CSCtb15071

  Symptoms: Traffic is denied even though inbound ACL is configured on EVC on ESM20 to permit the traffic.

  Conditions: Occurs after the inbound ACL is changed from Layer 3 to Layer 4.

Workaround: Reload the device.

- CSCtb15832

  Symptoms: A label swap operation might be wrongly performed and the expected label is not swapped.

  Example:

```
Router#show mpls for label 20
Local Outgoing Prefix Bytes Label Outgoing Next Hop
Label Label or VC or Tunnel Id Switched interface
20 142 10.0.0.1/32 10 Gi1/6
10.0.2.1
103 10.0.0.1/32 20 Gi1/1 10.0.2.5

Router#show mls cef mpls label 20
Codes: + - Push label, - - Pop Label * - Swap Label, E - exp1
Index Local Label Out i/f
Label Op
455 20 184(*),142(+) Gi1/6 , 0000.dead.beef
158(*),103(+) Gi1/1 ,
0000.c0ff.ffee
```

  Where we see the label swap becomes a label imposition.

  Conditions: This has been seen under following conditions:

  1) A Cisco 7600 running Cisco IOS Release 12.2(33)SRB4.

  2) Load balancing of the destination prefix needs to exist.

  Workaround: Clear the route.

- CSCtb25155

  Symptoms: The router may crash.

  Conditions: Configure a PVC range and before hitting exit/end, perform an online insertion and removal (OIR) operation. Exit from the range mode. After the card comes up, try to go into the range configuration mode.

  Workaround: Do not OIR while configuring a new range VCS.

- CSCtb64405

  Symptoms: Bulk-sync failure due to servicing incompatibility while configuring **ip nhrp responder Loopback** and removing the loopback after stateful switchover (SSO).

  Conditions: Observed on a Cisco 7600 router running Cisco IOS Release 12.2(32.8.24)REC186 image.

  Workaround: There is no workaround.

- CSCtb75569

  Symptoms: IP address is not assigned to the client on VPN routing/forwarding (VRF) from the DHCP server.

  Conditions: This happens when we configure **ip dhcp test relay link-selection** *50.0.0.2* and **ip dhcp relay override giaddr link-selection** on the realy1 and relay2 respectively.

  Workaround: There is no workaround.

- CSCtb80765

  Symptoms: Cisco 7200 may crash after an online insertion and removal (OIR) operation.

  Conditions: Occurs when MFR bundle is in SW mode and OIR is performed on CJ-PA.

Workaround: There is no workaround.

- CSCtb80788

  Symptoms: Lost fragments seen on multilink.

  Conditions: Occurs when 12 members are added to a multilink on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCtb82666

  Symptoms: SIP-400 crashes at dev_ds26504_isr.

  Conditions: SIP-400 will crash if connecting BITS port of SPA to a device which has mismatch in framing type configured on local end.

  Workaround: Disconnect the port with a wrong framing type.

- 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.

- CSCtb88060

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

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

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

- CSCtb98274

  Symptoms: Block overrun leading to crash. Issue is seen on the IT-SP-ISG system testbed with RSP720 and SIP-400 line cards. Issue is seen with scale sessions.

  Conditions: The setup was running 24,000 PTA and 12,000 DHCP sessions with end-to-end traffic running.

  Workaround: There is no workaround.

- CSCtc00106

  Symptoms: Packets are not routed across PPP over Frame Relay.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- CSCtc02769

  Symptoms: The router crashes when a policy with fair-queue along with other queuing is attached to the port-channel sub-interfaces.

  Conditions: This happens only with fair-queue + shaping + queue-limit is configured in the following order:

```
policy-map shape-llq-policy
class class-default
shape average 80000 320 320
random-detect
fair-queue
queue-limit 10000 packets
```

!
Workaround: Configure in the following order:

```
policy-map shape-llq-policy
class class-default
fair-queue------------------> configured fair-queue first
random-detect---------------->random-detect next
shape average 80000 320 320-------> shape-average next
queue-limit 10000 packets-------------> queue-limit at last
```

- CSCtc15394

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

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

  Workaround: There is no workaround.

- CSCtc15920

  Symptoms: In EMVPN scenario, high CPU utilization was observed when VPN routing/forwarding (VRF) select was used.

  Conditions: This can be reproduced in any EMVPN scenario using VRF select.

  Workaround: Stop using vrf select and use other means to configure EMVPN.

- CSCtc22090

  Symptoms: Multilink members go down on Cisco 7200 router.

  Conditions: Occurs when members from second controller are added to multilink where first controller members are in the bundle.

  Workaround: There is no workaround.

- CSCtc22745

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

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

  Workaround: There is no workaround.

- CSCtc27236

  Symptoms: MFR members are down.

  Conditions: MFR members are stuck at add-sent when bundle moves from SW to HW.

  Workaround: Perform a online insertion and removal (OIR) on the PA.

- CSCtc27605

  Symptoms: The **show ip route vrf coke** command has no framed route when applied to “ip-vrf”.

  Conditions: It happens when a framed-route attribute is downloaded from the AAA server and applied to “ip-vrf”.

  Workaround: To configure VRF in the user profile where template was used.

- CSCtc28091

  Symptoms: Tracebacks were seen while removing a port-channel.

  Conditions: Occurs when port-channel is configured with “c-mac” bridge domain and port-channel is removed.

  Workaround: Remove the “evcs” first before removing port-channel.

- CSCtc31493

  Symptoms: After executing **no ip vrf** <*vrf*>, the VRF may still be around, thus causing other VRF dependent CLI to be unconfigurable or lead to other unexpected behavior. One known issue is failed bulk sync, thus leading to unsuccessful switchover.

  Conditions: This only affects MVPN setup.

  Workaround: The user must unconfigure all VRF dependent CLI before removing VRF, otherwise it may lead to unsuccessful switchover or even crashes.

- CSCtc32063

  Symptoms: Cisco 7600 router with 12.2SRE software could reload when CFM D1 is configured.

  Conditions: The issue is observed on a Cisco 7600 running Cisco IOS Release 12.2(33)SRE when an ingress LAN card is configured as a MIP with CFM D1.

  Workaround: Use CFM D8 instead of CFM D1.

- CSCtc33785

  Symptoms: When a port-channel with MTP BD configuration (scaled to 1000) is removed and reconfigured, ES+ LC and SP crash.

  Conditions: Port-channel with a member link should configured with multiple c-mac bridge-domains.

  Workaround: Remove all EVCs or bridge-domains first, then remove the port-channel.

- CSCtc36619

  Symptoms: Multicast traffic is not forwarded across a Virtual Private LAN Services (VPLS) pseudowire.

  Conditions: Occurs when ES20+ line card connects n-PE to CPE device. Problem occurs when bridge-domain VLAN is configured as L2 and IGMP snooping is enabled. For example:

  ```
  interface Vlan100
  description VPLS
  no ip address
  xconnect vfi HVPLS
  ```

  Workaround: Disable IGMP snooping on the bridge-domain VLAN, or configure a routed pseudowire.

- CSCtc38796

  Symptoms: In some instances, when the Cisco 7600/RSP720/RP crashed and the core dump is configured to be created using FTP and RCP, the core dump recreation fails to complete.

  Conditions: This symptom is observed in an MPLS VPN large topology network.

  Workaround: There is no workaround.

- CSCtc40111

  Symptoms: When a large number of service groups are configured with multiple EVCs in them, the following anomaly can be observed. On doing online insertion and removal (OIR), some of the service groups (Layer 2 nodes) are configured in TMC which instead of in TMB. Before and after OIR output differs as below

  Before OIR

  ```
  *************
  Evee-dfc4#sh platform hardware qos np 0 queue resources np tm level groups entity
  ---------------------------------------------
  0 0 L4 4096/6 32768/16 0 0 L3 256/4 4096/6 0 0 L2 16/1 256/1 0 0 L1 32/1 32/1
  ---------------------------------------------
  ```

```
0 1 L4 4096/4081 32768/11732 0 1 L3 256/256 4096/4081 0 1 L2 8/1 256/256 0 1 L1 32/1
32/1 -------------------------------------------
0 2 L4 4096/3 32768/5 0 2 L3 256/2 4096/3 0 2 L2 8/1 256/2 0 2 L1 32/1 32/1
```

After OIR

```
*************
Evee-dfc4#sh platform hardware qos np 0 queue resources np tm level groups entity
-------------------------------------------
0 0 L4 4096/6 32768/16 0 0 L3 256/4 4096/6 0 0 L2 16/1 256/1 0 0 L1 32/1 32/1
-------------------------------------------
0 1 L4 4096/1043 32768/2996 0 1 L3 256/67 4096/1043 0 1 L2 8/1 256/67 0 1 L1 32/1 32/1
-------------------------------------------
0 2 L4 4096/3041 32768/8741 0 2 L3 256/191 4096/3041 <<<<<<<<<<<<<<<<<<<<<<<<< 0 2 L2
8/1 256/191 <<<<<<<<<<<<<<<<<<<<<<<<< 0 2 L1 32/1 32/1
```

Conditions: This happens with Ten Gigabit Ethernet interface and a large number of service groups and EVCs.

Workaround: One option is to keep scale below 250. Aside from that there is no workaround.

- CSCtc42108

  Symptoms: Pseudowires remain down when resetting the module after SSO.

  Conditions: Occurs when module needs to be reset after SSO.

  Workaround: There is no workaround.

- CSCtc42696

  Symptoms: Spurious memory access is seen while executing the command **show memory dead** after stateful switchover (SSO).

  Conditions: MPLS needs to be configured.

  Workaround: There is no workaround.

- CSCtc42737

  Symptoms: ES40 line card CPU remains high.

  Conditions: The problem is seen only when you have scaled number of sessions (20,000 sessions) and while bringing up 2,000 sessions and tearing down 2,000 sessions simultaneously at 24 CPS rate.

  Workaround: There is no workaround.

- CSCtc42941

  Symptoms: Standby is not coming up.

  Conditions: When a distribute-list is configured, the ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workarounds:

  1. When a access list is removed, remove corresponding distribute-list configuration as well.
  2. Do not use the same access list name for IPv4 and IPv6.

  Further Problem Description:

```
router bgp 100
distribute-list sample in
exit
no ip access-list standard sample
ipv6 access-list sample
permit any any
```

```
write mem
```

- CSCtc43042

  Symptoms: WS-X6704-10GE module running c6lc2-sp-m.122-33.SRC4 code may crash due to memory corruption.

  Conditions: MPLS-TE Fast Reroute (FRR) should be enabled.

  Workaround: There is no workaround.

- CSCtc44589

  Symptoms: Standby not coming up when **snmp-server enable traps** command is configured

  Conditions: The Standby fails to reach Standby HOT when **snmp-server enable traps** is configured.

  Workaround: Do not configure this command.

- CSCtc44620

  Symptoms: EoMPLS VC on TE tunnel does not comes up after switchover.

  Conditions: Occurs after a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCtc44749

  Symptoms: Bulk sync failure and high-availability router goes to RPR mode from SSO mode.

  Conditions: Occurs when MVPN with MDT data is configured along with access-list option. If the access-list is removed and recreated with different type of ACL. In this condition if a forced switchover happens there will be a sync failure

  Workaround: Remove the MDT data configuration and reload the router.

- CSCtc45500

  Symptoms: The pseudowire goes down when reapplying xconnect under a sub-interface.

  Conditions: This happens when reapplying the xconnect to sub-interface which already has xconnect configured.

  Workaround: There is no workaround.

- CSCtc47677

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

  Conditions: Occurs when **ip multicast vrf** <*vrf1*> **rpf select** <*vrf2*> command is configured. Later if the *vrf2* is deleted and a forced switchover is done, 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.

- CSCtc48628

  Symptoms: BGP Sessions are taking longer to come up in scale scenario.

  Conditions: Occurs after reloading the router.

  Workaround: There is no workaround.

- CSCtc49228

  Symptoms: Memory leak of AAA cursor.

  Conditions: Install interface configuration using AAA on PPPoE session (such as lcp: interface-config).

Workaround: There is no workaround.

- CSCtc52149

  Symptoms: SIP200 CPU 1 crash as indicated below.

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

  Conditions: There is no specific trigger to this problem. It happens randomly and recovers on its own.

  Workaround: There is no workaround.

- CSCtc52631

  Symptoms: In some instances, a Cisco 7600/SP crashed when all the VRFs in MPLS L2/L3 network are unconfigured.

  Conditions: This symptom is observed in MPLS L2/L3 VPN scaled network when all the VRFs are unconfigured.

  Workaround: There is no workaround.

- CSCtc52740

  Symptoms: Cisco 7600 ES+ interface will not accept policy map with “random-detect cos-based” statement.

  Conditions: CLI configuration is rejected on main interface of an ES+ line card.

  Workaround: There is no workaround.

- CSCtc54233

  Symptoms: After entering the EXEC command **clear xconnect all**, and then performing a Stateful Switchover (SSO) on the Cisco 7600, packets stop flowing via HDLC over Any Transport over MPLS (AToM) pseudowires.

  Conditions: This symptom has been observed with Cisco IOS Release 12.2SRE.

  Workaround: Enter **clear xconnect all** after switchover.

- CSCtc55937

  Symptoms: In **show spanning-tree mst** output, all links are in forwarding state.

  Conditions: This happens with EVC bridge domain configuration if the ports have EVCs with encapsulation untagged or default configured. Happens only on ESM20 cards.

  Workaround: Enable CFM globally using **ethernet cfm enable**.

- 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.

- CSCtc57044

  Symptoms: The **mpls propagate-cos** command may not function correctly on a Cisco 7600 router.

  Conditions: This was observed on several Cisco 7600s running Cisco IOS Release 12.2(33)SRC.

  Workaround: Remove and reapply the **mpls propagate-cos** command.

- CSCtc57092

  Symptoms: In a HA router, standby keeps on rebooting during switchover.

  Conditions: This is seen when we configure RIP with a standard access-list in offset-list, followed by deleting the access-list and creating an IPv6 access-list with the same name.

  Workaround: Avoid creating IPv6 access-list with the same name of an IPv4 named access-list.

- CSCtc58898

  Symptoms: In MPLS VPN scenario, if it happens that default route known via RIP in VRF is looping, route might stay in RIB.

  Conditions: Issue observed in Cisco IOS Release 12.2(33)SRC4 and 12.2(33)SRC5.

  Workaround: Clear VRF routing table of with the **clear ip route vrf** <*name*> ***** command.

- CSCtc60458

  Symptoms: On a Cisco 7600 router with a large number of VCs and VLANs, traffic stops forwarding traffic for several seconds while standby supervisor is booting.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC4.

  Workaround: There is no workaround.

- CSCtc60463

  Symptoms: The **traceroute mac** <*src_mac*> <*dst_mac*> command can cause a software crash on a Cisco 7600 router when configured with a large number of VLANs.

  Conditions: This occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRC4.

  Workaround: Do not use the **traceroute mac** <*src_mac*> <*dst_mac*> command. Use a specific VLAN ID when using this command.

- CSCtc61430

  Symptoms: If PVC Discover is configured, PVCs may not be discovered and some other VCs may disappear from interface.

  Conditions: Occurs after a crash or online insertion and removal (OIR) operation.

  Workaround: There is no workaround.

- CSCtc64520

  Symptoms: Router reloads due to watchdog timer expiration.

  Conditions: Occurs on a Cisco 7301 running Cisco IOS Release 12.2(33)SRC4 image with Bidirectional Forwarding Detection (BFD) configured.

  Workaround: There is no workaround.

- CSCtc65227

  Symptoms: Standby unit keeps reloading after forced switch-over.

  Conditions: Occurs in redundancy system when user renames a call-home profile to an empty string using the **rename** command under call-home configuration submode.

  Workaround: Do not rename a call-home profile name to empty string.

- CSCtc65612

  Symptoms: Some BGP prefixes are not advertised to their relevant BGP peers until a soft clear is done.

Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB6 and configured for MPLS VPN.

Workaround: There is no workaround.

- CSCtc66490

  Symptoms: Per-user ACL is not getting synced with standby.

  Conditions: Occurs during normal operations. No specific trigger.

  Workaround: There is no workaround.

- CSCtc67380

  Symptoms: After bringing up a port-channel that has been in err-disabled state, traffic stopped flowing in one VLAN.

  Conditions: This has been observed on Cisco 7600 with ES20 module running Cisco IOS Release 12.2(33)SRC4.

  Workaround: This issue can be solved by shut/no shut of the affected Vlan interface.

- CSCtc67432

  Symptoms: Multicast traffic is not forwarded after LACP switchover.

  Conditions: For some port combinations on same line card or on different line cards in a port-channel case, multicast traffic does not flow after LACP switchover.

  Workaround: Enter the **clear ip mroute** <*option*> *command.*

- CSCtc71207

  Symptoms: CPU usage goes to 100% with main offending process being “XDR mcast”. In addition, output for **show xdr linecard internal** shows constantly increasing totals for Etherbridge domain MAC security.

  Conditions: Seen in a topology that has numerous bridge-domain c-MAC instances configured on it.

  Workaround: In some instances it has been seen that shutting the router’s TFTP interface may reduce the CPU usage.

- CSCtc75338

  Symptoms: Traceback is seen when ISSU commit version is performed.

  Conditions: Issue is seen with default configuration and under no traffic conditions.

  Workaround: There is no workaround. Occurs only with ISSU.

- CSCtc75687

  Symptoms: Some commands with large outputs allow the use of ctrl-^ to stop the output before completion. This can cause a crash.

  Conditions: Unknown at this time.

  Workaround: Enter the **no parser command serializer** command.

- CSCtc78951

  Symptoms: If a port channel is enabled with standalone-disable and some non-default native VLAN, and if any peer bundled port is unbundled from the port channel, then the respective local port goes into “s” state as per the design. But when the peer port is bundled again, the local port does not recover from “s” state to “P” state.

  Conditions: Port-channel standalone-disable and a non-default native VLAN need to be configured on the port-channel. The problem only happens if one of the port is put in suspended state.

Workaround: A **shutdown**, **no shutdown** is required to get the port bundled into the port-channel.

- CSCtc81653

  Symptoms: The system crashes if the port-channel is removed while it is serving data traffic.

  Conditions: Port-channel is configured with the member links in it. The traffic is sent through the port-channel. If the port-channel is removed, the system sometimes crashes.

  Workaround: There is no workaround.

- CSCtc81717

  Symptoms: Layer 2 protocols on MTP EVC do not get forwarded as data.

  Conditions: Occurs when the **l2protocol forward** command is configured.

  Workaround: There is no workaround.

- CSCtc83544

  Symptoms: LDP release messages were seen multiple times on a Cisco 7600 P3 router running Cisco IOS Release 12.2(33)SRD.

  P3#

  ```
  *Oct 19 04:00:29: %TIB-5-WDRAWTAG: 10.9.155.0/24, tag 18656; Withdrawn tag record has
  timed out.
  *Oct 19 04:00:30: %TIB-5-RELTAG: 10.9.155.0/255.255.255.0, peer 192.168.2.4:0; tag
  18656; Unexpected LDP label release; specified label not in TIB
  ```

  Conditions: At that time router was consuming 396,000 routes in CEF table, which was consuming 95% of memory.

  Workaround: There is no workaround.

- CSCtc84659

  Symptoms: In a HA router during switch-over, standby keeps on rebooting.

  Conditions: This issue happens when we configure a NULL route-map for redistribution under router IS-IS.

  Workaround: Use a valid route-map name.

- CSCtc84960

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

  Conditions: The problem is seen in LSM P2MP setup where egress line card is different from ingress line card.

  Workaround: The problem can be prevented by configuring **tunnel mpls traffic-eng fast-reroute** on the P2MP tunnel interface.

  If the problem is still noticed, then it can be fixed by one of following steps.

  1) Programming the FPOE table by using **test fpoe index** <*index*> **value** <*value*>.

  2) Resetting ingress line card.

- CSCtc86490

  Symptoms: Error message stating “Can’t install service policy with empty name” is displayed.

  Conditions: When an invalid service policy is pushed from the DBS on to the VC, the error message is thrown and the policy on the VC does not fall to the default.

  Workaround: There is no workaround.

- CSCtc87700

  Symptoms: A Cisco 7600 router may fail to process ingress Link Integrity Protocol messages on MFR serial link members, which will disallow Multilink Frame Relay interfaces from enabling.

  Conditions: Occurs on a Cisco 7600 router with SUP-720-3BXL and OSM CHOC12, and running Cisco IOS Release 12.2(33)SRC and 12.2(33)SRD. This issue happens when MFR serial members are configured on CHOC12 OSM but may also occur on other line cards.

  Workaround: There is no workaround.

- CSCtc88534

  Symptoms: After upgrade, device has its T1 link go UP/Down after a period of normalcy.

  Conditions: Occurs on a Cisco 7609 with a channelized SPA-4XCT3/DS0 on a SIP-200 and running Cisco IOS Release 12.2(33)SRD3.

  Workaround: Problem is resolved with a flap of the service-policy on the T1, but issue will reoccur.

- CSCtc89094

  Symptoms: A Cisco 7600 HA router changes its state from SSO to RPR after a forced switchover with maximum timer configured under ODR.

  Conditions: Timer basic is configure to maximum value 4294966. After saving the configuration followed by a forced switchover, the router moves to RPR state.

  Workaround: There is no workaround.

- CSCtc90579

  Symptoms: Router crashes due to memory corruption during MPLS TE auto backup tunnel deletion.

  Conditions: Caused by topology changes triggering backup tunnel deletion and RSVP hello mechanism.

  Workaround: Gloablly, disable RSVP hello and enable BFD hello:

  ```
  Router(config)#no ip rsvp signalling hello
  Router(config)#ip rsvp signalling hello bfd
  Per MPLS TE enabled interface:
  Router(config-if)#no ip rsvp signalling hello
  Router(config-if)#ip rsvp signalling hello bfd
  ```

- 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.

- CSCtc92342

  Symptoms: ES+/Combo card crashes when we remove member links of EVC port-channel.

  Conditions: This issue is seen only with scaled configuration with 4,000 EVCs configured on the port-channel and HQoS policy-map is applied on each EVC. This issue is very inconsistent and is not seen with 1,000 EVCs on Port-channel and HQoS policy-map applied on it.

  Workaround: There is no workaround.

- CSCtc96446

  Symptoms: Crash due to bus error seen with spurious memory access.

  ```
  %ALIGN-1-FATAL: Illegal access to a low address<TIME> IST <DATE> addr=0x<LOW MEMORY
  ADDRESS>, pc=0x<STACK VALUE>, ra=0x<MEMORY ADDRESS>, sp=0x<STACK POINTER>
  <TIME> IST <DATE>: TLB (store) exception, CPU signal 10, PC = 0x<STACK VALUE>
  ```

  Conditions: Normal conditions.

  Workaround: There is no workaround.

- CSCtd00054

  Symptoms: Link flap/down of PA-MC-T3E3-EC interface.

  Conditions: Occurs when changing encapsulation after reload.

  Workaround: Perform a online insertion and removal (OIR) of the PA.

- CSCtd05287

  Symptoms: Very low rate of packet inputs compared to the rate of packet outputs.

  Conditions: Occurred on a 7600-SIP-400 with a sub-module of SPA-4XOC3-ATM.

  Workaround: Reset the entire 7600-SIP-400 module to clear the issue.

- CSCtd08797

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

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

  Workaround: Flap the interface.

- CSCtd09035

  Symptoms: Seeing traffic forwarding drop randomly in L3VPN P2MP testing when doing fast reroute (FRR) test. Tunnels are up, but hardware does not forward traffic.

  Conditions: Occurs with L3VPN P2MP bud node router.

  Workaround: There is no workaround.

- 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.

See the MDT SAFI document:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCtd21590

  Symptoms: RP crashed after executing **no import ipv4 unicast map filter**.

  Conditions: BGP import events debugging is on with **do debug ip bgp import event**.

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

- CSCtd25133

  Symptoms: Router gets into APS channel mismatch state.

  Conditions: Observed with MGX connected as APS peer, when both MGX cards (active and standby) are reloaded simultaneously.

  Workaround: Force APS switchover.

- CSCtd26400

  Symptoms: There is a risk to introduce inconsistency between hardware routing table (MLS CEF) and software table (IP CEF) in some VRFs. Some interfaces in affected VRF may also be seen as part of other VRFs.

  Conditions: Occurs when modifying route-map sequence of a route-map applied to an interface with PBR VRF select.

  Workaround: Enter the **clear ip route vrf xxx *** command. Or you can perform a shut/no shut on the affected subinterfaces.

- CSCtd28578

  Symptoms: There are MPLS TE tunnels from PE1/2 to P2 and from PE3/4 to P1 using load-sharing. Issue started once second multilink was configured between P routers. PE routers started to observe inconsistencies between MLS CEF and routing tables. Bogus MLS entries are created.

  Conditions: This was found under the normal conditions on a Cisco 7600 router with SUP32 with PFC2 and MSFC2a. This router is PE and running Traffic Engineering tunnels to the core with load sharing configured. Two PPP multilinks are used in the core.

  Workaround: Enter the **clear ip route** command to temporarily resolve the issue.

- CSCtn68668

  Symptoms: The following symptoms are observed:

  1. The STATUS LED on the line card faceplate is amber.
  2. The **remote command module** *module* **show platform hardware environment temperature** command reports high line card inlet temperature:

```
Router#remote command mod 1 show plat hard env temp

        ------------------------------------------------------------
              Temperature and Threshold Table
        ------------------------------------------------------------
         Sensor          Minor          Major          Current
           ID          Threshold      Threshold      Temperature
        ------------------------------------------------------------
        BB Outlet 0       60             75             47
        BB Inlet 0        50             65             27
        BB Outlet 1       75             85             54
```

```
BB Inlet 1        50            65            32
PE Outlet         60            75            53
PE Inlet          50            65            34
LC Outlet         60            75            49
LC Inlet          50            65            50   <<<<<<<<
```

Conditions: This issue is specific to the following Cisco 7600 ES+ combo cards:

- 76-ES+XC-20G3C
- 76-ES+XC-20G3CXL
- 76-ES+XC-40G3C
- 76-ES+XC-40G3CXL

Line card inlet sensor is inappropriately positioned in a place where temperatures are higher than on the inlet point.

Workaround: There is no workaround.

Further Problem Description: There are no problems with the functioning of the board. Only the external communication is affected. “BB Inlet 1” shows the actual inlet temperature. It can be used for reliable measurement of line card inlet temperature.

Resolved Caveats—Cisco IOS Release 12.2(33)SRE

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRE. The caveats listed in this section are open in Cisco IOS Release 12.2(33)SRD.

- CSCee36959

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

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

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

  Workaround: There is no workaround.

- CSCeg49153

  Symptoms: It may take a long time for the IPSec router to detect that the CA server is down while trying to reach it for CRL retrieval.

  Conditions: The symptom is observed on a LAN-to-LAN IPSec tunnel between two routers, where one router is configured for CRL checking.

  Workaround: The situation may be slightly improved by lowering the “tcp synwait” value, for example: ip tcp synwait-time 5.

- CSCeg59484

  Symptoms: Entering the **debug ipv6 ospf lsa-generation** may crash the router if LSA with max-age is generated.

  Conditions: Occurs after **clear ospfv3 proc** along with **debug ospfv3 lsa-gen** enabled.

  Workaround: Do not use this **debug** command.

- CSCeg87070

  Symptoms: A Cisco 10000 crashes at igmp-process:

  ```
  Cisco IOS Software, 10000 Software (C10K2-P11-M), Version 12.3(7)XI2b,
  ```

```
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 08-Jan-05 16:25 by <software engineer>

ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios-
rommon 112], DEVELOPMENT
SOFTWARE

r-pa068 uptime is 19 hours, 58 minutes
System returned to ROM by RPR switchover at 19:03:47 MET Mon Jan 24 2005
System restarted at 19:07:22 MET Mon Jan 24 2005
System image file is "disk0:c10k2-p11-mz.123-7.XI2b"
```

Conditions: This symptom is observed during 7xi2b monitoring.

Workaround: There is no workaround.

- CSCeh24147

  Symptoms: The implementation of IPv6 scope support in the Bootstrap Router (BSR) mechanism may cause interoperability problems.

  Conditions: This symptom occurs because the specification of IPv6 scope support in the BSR mechanism has changed.

  Workaround: Do not use IPv6 scope support in the BSR mechanism.

- CSCeh71577

  Symptoms: A Cisco 7200 series does not load an image and generates a traceback.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(1), that is configured with an NPE, and that has the L3 cache disabled. The symptom may also occur in other releases.

  Workaround: Enable the L3 cache by entering the **no l3 cache disable** command.

- CSCej18051

  Symptoms: Terminal window PPP clients may fail with Cisco Access servers.

  Conditions: This symptom has been observed on Cisco AS5400 gateways and Cisco AS5800 servers.

  Workaround: There is no workaround.

- CSCej20707

  Symptoms: The CPU usage may be high, and an IGP (OSPF or IS-IS) adjacency may drop when PIM sparse mode (PIM-SM) stress traffic is being processed.

  Conditions: This symptom is observed on a Cisco router that connects to a receiver and that has 60,000 (s,G) join messages. The symptom occurs when you enter the **show ip mroute count** command or when there is an abrupt increase in multicast groups.

  Workaround: Do not enter the **show ip mroute count** command. Rather, enter the **show ip mroute count terse** command. Increase multicast groups gradually to avoid high CPU usage. In addition, the following actions may also help to alleviate the symptoms:

  - Enter the **ip pim register-rate-limit** command on the first hop.

  - Enter the **ip pim fast-register-stop** on the PIM-RP.

  - Disable RP rate-limiting commands on the PIM-RP and first hop.

- CSCej33698

  Symptoms: A router that is running Cisco IOS software may mistakenly fail a CRC check on files in NVRAM.

  Conditions: This symptom has been observed with large files, such as large startup configurations.

  Workaround: There is no workaround.

- CSCek26595

  Symptoms: After configuring Multicast and applying the **crypto map** command, traffic can't go through from the second Ethernet interface to the same group. However, traffic goes through fine from the first Serial interface.

  Conditions: The symptom has been observed in Cisco IOS interim Release 12.4 (5.13)T2.

  Workaround: There is no workaround.

- CSCek32744

  Symptoms: The vlan-id is not propagated in the NAS Port ID field when the PPPoE over VLAN call is up.

  Conditions: The symptom is observed when using both configurations (main interface and sub-interface) for PPPoE over VLAN. The NAS Port ID value shows correctly while using the sub-interface configuration but incorrectly when using the main interface. The main interface used for PPPoE over VLAN is shown below:

```
interface Ethernet1/0
 no ip address
 vlan-id dot1q 4
  pppoe enable group global
  exit-vlan-config
```

  The expected NAS Port ID is 1/0/0/4 but 1/0/0/0 is received.

  Workaround: There is no workaround.

  Further Problem Description: This will impact AAA as this information should be updated by PPP to AAA.

- CSCek55668

  Symptoms: Border Gateway Protocol (BGP) next hop may fail after BGP neighbor send-label is configured.

  Conditions: Occurs when Carrier support carrier(CSC) is used. If the EBGP session to one site goes down and up the PE doesn¬¥t send the transport label information to the other site¬¥s. It sends only the route with an imp-null label and so the CSC-CE has the route without a label in his cef-table.

  This condition has been observed in routers running Cisco IOS Release 12.4(6)T4, 12.2(31)SB11, and 12.2(33)SRC1.

  Workaround: Applying a route-map to the bgp neighbour with assigns a soo community to the prefix prevents this problem to occur.

- CSCek63963

  Symptoms: Router crashes with a traceback decode showing a divide by 0 error.

  Conditions: Occurs when a rate-based event is configured for a counter that has a value of 0, such as the following scenario:

  1. The customer must be using a Cisco IOS Embedded Event Manager (EEM) rate-based Interface Event Detector (either applet or Tcl script). Rate-based means use of the **rate** keyword in the event specification statement.

2. The rate calculation is attempted after the counters are cleared and before any samples have been taken.

Workaround: There is no workaround.

- CSCsa55482

  Symptoms: A duplicate PIM register encapsulation tunnels may be created for a static rendezvous point.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv6 multicast when you configure a static rendezvous point after having disabled an embedded rendezvous point.

  Workaround: Configure the static rendezvous points while the embedded rendezvous point is enabled and then disable the embedded rendezvous point.

- CSCsb27969

  Symptoms: The IPv6 PIM register encapsulation tunnel does not come up after a switchover. The PIM Register mechanism does not work for sources directly connected to the router.

  Conditions: This symptom has only been observed when the **ipv6 pim register-source** global configuration command is configured.

  Workaround: After switchover, unconfigure and re-configure the **ipv6 pim register-source** command.

- CSCsb64662

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are dropped.

  Condition 1: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S.

  Workaround 1: There is no workaround.

  Symptom 2: Multicast packets that traverse a Frame Relay virtual circuit (VC) bundle are process-switched.

  Condition 2: This symptom is observed with Cisco IOS Release 12.3.

  Workaround 2: There is no workaround.

- CSCsc07793

  Symptoms: The standby supervisor in SSO mode system reloads.

  Conditions: Setting stpxMSTInstanceEditVlansMap to a VLAN causes standby causes supervisor in SSO mode to reload.

  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.

- 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.

- CSCse60667

  Symptoms: Core dump occurs.

  Conditions: When running command **show ip cef with feature lfd summary**.

  Workaround: Do not use this command.

- CSCsg49395

  Symptoms: The following BIT-OUTOFRANGE error message and traceback information may be displayed:

  ```
  1d21h: %BIT-SP-4-OUTOFRANGE: bit 127 is not in the expected range of 128 to 2175
  -Traceback= 40D8A8B0 40D8ADFC 40512B4C 407A8118 40CC5838 404B5978 404B5C84term m
  ```

  Conditions: Occurs on a Cisco Catalyst 6500 if an SNMP walker utility sends bridge port number 0 to the switch.

  Workaround: Configure the SNMP walker utility to get MIB objects starting from bridge port number 1.

- CSCsg62638

  Symptoms: Scan of a router when a DNS server is enabled can cause high CPU usage of the DNS process itself. Overall performance of the device can deteriorate to some extent.

  Conditions: This symptom has been observed on a router when a DNS server is enabled when running Cisco IOS software from Cisco IOS interim Release 12.4 (11.1)T up to but not including Cisco IOS interim Release 12.4(13.08)T.

  Workaround: The only way to rectify this situation is to reboot the device.

- CSCsh11993

  Symptoms: When a Demilitarized Zone (DMZ) port is configured on a router, autoinstall does not function.

  Condition: This symptom is observed on a Cisco 830 series that runs Cisco IOS Release 12.4 or Release 12.4T when you use Fast Ethernet (FE) port 0, port 1, port 2, or port 3 instead of port 4 that is linked to the Ethernet 2 interface that is used as the DMZ port. The Ethernet 2 interface receives the IP address via DHCP, but because FE port 4 is in the down/down state, autoinstall does not function.

  The following is an example of the configuration:

  ```
  AUTOINSTALL: Ethernet2 is assigned <ip add 1> AUTOINSTALL: Obtain tftp server address
  (opt 150) <ip add 2>
  ! interface Ethernet0 no ip address shutdown ! interface Ethernet2 ip address dhcp end
  ```

  When the symptom occurs, the output of the **show ip interface brief** shows the following:

  ```
  Interface IP-Address OK? Method Status Protocol FastEthernet1 unassigned YES unset
  down down FastEthernet2 unassigned YES unset up up FastEthernet3 unassigned YES unset
  down down FastEthernet4 unassigned YES unset down down Ethernet0 unassigned YES unset
  administratively down down Ethernet2 <ip add 1> YES DHCP down down
  ```

Workaround: Use FE port 4 that is linked to the Ethernet 2 interface and that is used as the DMZ port.

- 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.

- CSCsh39329

  Symptoms: A Cisco c7206VXR NPE-G2 router with SA-VAM2+ card may cause router crash. After a period of time in operation, depending on the Cisco IOS version, the error message can be seen multiple times before crashing.

  ```
  -Process= "Crypto Support", ipl= 4, pid= 154 -Traceback= 0x1408008 0xAE28 0x33387C
  0x33544C 0x1A882D8 0x1A87DF8 0x2CCF9BC 0x2DD6900 0x782670
  ```

  Conditions: There is no specific trigger for this. It happens randomly.

  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.

- 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.

- CSCsi68963

  Symptoms: A Cisco 7200P router crashes while removing an IPv6 Protocol Independent Multicast (PIM) bootstrap router (BSR) candidate from the configuration.

  Conditions: This symptom is observed when the IPv6 PIM BSR candidate is unconfigured.

  Workaround: There is no workaround.

  Further Problem Description: After RP information is learned on all of the routers, delete the ACL first and then the BSR candidate.

- CSCsi69186

  Symptoms: Interface is reported by Optimized Edge Routing (OER) as being an invalid interface for sending an active probe.

  Conditions: Occurs on an Optimized Edge Routing (OER) border router with an external interface defined as a tunnel interface (mGRE).

  Workaround: There is no workaround.

- CSCsi89769

  Symptoms: Router experiences memory leak.

  Conditions: Occurs when the router is a group domain of interpretation (GDOI) member and encrypts bulk rate multicast traffic. If the user enters the **clear crypto sa** command to delete all of the IPsec SAs, the memory leak occurs.

  Workaround: Either avoid using multicast fast switch or do not manually clear bulk GDOI SAs.

- CSCsj64230

  Symptoms: When a bidir PIM, with no directly connected receivers, router has to change its RPF interface to the RP, multicast traffic could be lost for up to 60 seconds.

  Conditions: This symptom occurs if the connection to the first RP is lost and the middle router changes its RPF for its bidir upstream interface. The middle router then restarts the election process on all DF interfaces, and purges the interface point in the leaf router out its OI @L. That interface will only get repopulated upon a periodic state refresh from the leaf router because the leaf router does not have an RPF change and therefore has no reason to send a triggered Join.

  Workaround: There is no workaround.

- CSCsk07875

  Symptoms: MPLS LDP autoconfig functionality is broken in OSPF.

  Conditions: This symptom is observed in the following two scenarios:

  – When adding all areas via the **mpls ldp autoconfig** command and removing a specific area via the **no mpls ldp auto area X** command, LDP is disabled.

  – If you disable LDP autoconfig completely and enable the **mpls ldp autoconfig** command for all OSPF areas, LDP does not come up until you enable the specific area X via the **mpls ldp autoconfig area X** command.

  Workaround: Enable the specific area with the following command:

  mpls ldp autoconfig area X

- CSCsk25878

  Symptoms: An alignment error may occur.

  Conditions: This symptom is observed when using the v9 export protocol with Flexible Netflow.

  Workaround: There is no workaround.

- CSCsk29013

  Symptoms: IGMP groups in the VRF not rejoined after executing **cle ip mr vrf**.

  Conditions: This symtom observed on Cisco 7200 and 7600 platforms in Cisco IOS Release 12.2(32.8.11)SX96 and above.

  Workaround: There is no workaround.

- CSCsk30146

  Symptoms: A router may reload when you unconfigure a sub-interface or loopback interface.

  Conditions: This symptom is observed when IGMP is enabled in the interface which is being deleted and a multicast group is joined to the interface using **ip igmp join-group** *group address* command.

  Workaround: The problem can be avoided when you delete a sub-interface or loopback interface after unconfiguring **ip igmp join-group** *group address* command from interface configuration mode and IGMP is disabled on the interface.

- CSCsk32872

  Symptoms: Router might crash if masklen and prefix have not been set and passed to CEF.

  Conditions: Caused by the **debug cef table**.

  Workaround: There is no workaround.

- CSCsk34641

  Symptoms: A router may exception while registering a corrupt eToken.

  Conditions: This symptom is observed only when a particular corrupt eToken is inserted. This symptom has been observed only on a single eToken.

  Workaround: Format the eToken.

- CSCsk34715

  Symptoms: Router crashes when the **no ip nat outside** command is removed while traffic is being processed.

  Conditions: Occurs on a Cisco 7200 router that uses ACL as source.

  Workaround: There is no workaround.

- CSCsk49073

  Symptoms: Router may crash due to bus error.

  Conditions: Occurs when MVPN is configured.

  Workaround: There is no workaround.

- CSCsk55012

  Symptoms: The standby supervisor might crash when portDuplex is set from “full” to “full” for an interface whose speed is configured as “auto”.

  Condition: It might occur when the interface speed is “auto” value.

  Workaround: Do not set portDuplex object from “full” to “full” via SNMP when the interface speed has “auto” configured on the interface.

- CSCsk77282

  Symptoms: A Cisco IOS router may no longer be able to show the configuration or do other file operations because all of the file descriptors are in use by files opened by the Embedded Event Manager (EEM) Remote Procedure Call (RPC) Event Detector (ED) policies.

  Conditions: This symptom is observed when a significant number of EEM RPC policies are executed. Each time a new EEM RPC session is started and then closed, a single file descriptor is left open.

  Workaround: The only way to recover is to reload the Cisco IOS device.

  Further Problem Description: The output of **show file descriptors** command can show you which file descriptors are open. Ones left open by EEM RPC will show a path of tmpsys:eem_rpc_n, where n is some integer. For example:

```
Router# show file descriptors
File Descriptors:
FD Position Open PID Path 0 0 0002 137 tmpsys:eem_rpc_1 1 0 0002 118 tmpsys:eem_rpc_0
2 0 0002 137 tmpsys:eem_rpc_1 3 0 0002 118 tmpsys:eem_rpc_0
```

- CSCsk84780

  Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

  Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase "cloned from: AAA, AAA, ..." (that is, multiple instances of AAA) as identification.

  Workaround: There is no workaround.

  Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

  – Increase the hello timers for L2TP and for the receive windows.
  – Configure the timers under the virtual template.
  – Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
  – Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- CSCsk87526

  Symptoms: The following traceback is seen:

  `%IPV6-3-INTERNAL: Internal error, Protocol <protocol>, decrement of zero ref count`

  Conditions: The traceback may be seen when the following conditions are met:

  – Two or more instances of the same IPv6 routing protocol are configured. For example, two instances of OSPFv3 are configured.
  – A particular route is first learned by one instance of the protocol, then by the second instance at a better metric.
  – The IPv6 routing table is cleared with the **clear ipv6 route *";** command or the first instance of the routing protocol is shut down.

  Workaround: There is no workaround.

- CSCsl09904

  Symptoms: The Bootstrap Router message (BSM), with RP information and holdtime of zero, creates a group-mapping state when the RP information does not exist.

  Conditions: The symptoms are observed in internal negative testing in an IPv6 multicast environment. Trigger is when a packet with an RP holdtime of zero is sent.

  Workaround: There is no workaround.

- CSCsl20701

  Symptoms: A Cisco IOS router that is configured to run Embedded Event Manager (EEM) Remote Procedure Call (RPC) policies may leak memory when those policies are run.

  Conditions: This only occurs when EEM RPC is configured and an EEM RPC TCL policy is executed.

  Workaround: There is no workaround.

- CSCsl33632

  Symptoms: Router crashes when VRF is unconfigured.

  Conditions: Router crashes when **no ip vrf** is executed. This is a platform independent issue. This issue is seen while using a script. Manually this issue is not seen.

  Workaround: There is no workaround.

- CSCsl46683

  Symptoms: Tracebacks may be observed while rebooting the device.

  Conditions: The symptoms are observed when there are no other SNMP CLI and SNMP-server manager is the first CLI to be configured.

  Workaround: There is no workaround.

- CSCsl51495

  Symptoms: A memory leak may be observed on the standby node.

  Conditions: The symptom is observed only when broadcast accounting is configured in the standby node. The memory leak is verified by using the **show processes memory | i AAA ACCT** command.

  Workaround: There is no workaround.

- CSCsl57993

  Symptoms: Router crashes when **show oer master traffic-class** command is executed.

  Conditions: It only happens when the one of the traffic-class being displayed has the **mode monitor active** configured.

  Workaround: Use the older version of the CLI. The older version is **show oer master prefix** or **show oer master appl**.

- CSCsl72702

  Symptoms: When running MPLS with SSO on a Cisco 6500 or 7600 platform, a VLAN allocation error may be seen.

  ```
  "SP-STDBY: pm_get_standby_vlan:Cannot allocate VLAN"
  ```

  Conditions: This is seen when MPLS is enabled along with SSO HA.

  Workaround: There is no workaround.

- CSCsm00496

  Symptoms: When v6 RP mappings with the same group range but with different mode (for example, bidir and sparse) are advertised to a bootstrap router (BSR), only one of the mappings is installed by the BSR.

  Conditions: When multiple IPv6 RP mappings with the same group range (for example, bidir and sparse) as shown below:

  - ipv6 pim bsr candidate rp 30::1:1:3 group-list acc_grp1
  - ipv6 pim bsr candidate rp 30::1:1:3 group-list acc_grp1 bidir

  The router installs only one of the mappings. The bidir mapping is installed in the above example.

  Workaround: There is no workaround.

- CSCsm02687

  Symptoms: When a multicast packet is fast switched and the output interface is an MGRE tunnel, the router crashes if there is no CEF adjacency established for the tunnel.

Conditions:

1. When a multicast packet is fast switched to an MGRE tunnel output interface, the packet is switched by CEF. If CEF has not established an adjacency for the MGRE tunnel, the router will crash.
2. The crash can also happen if we do have CEF adjacency for the tunnel (CEF only maintains unicast adjacency) but we do not have the configuration of **ip pim nbma** in tunnel. In this case when we receive a Join we are adding midb->nexthop as group address if **ip pim nbma** is not configured so CEF does not have adjacency, and this will lead to a crash.

NOTE: It is mandatory to configure **ip pim nbma** in DMVPN . If it is not configured, when packet comes to Fast switching, CEF will find adjacency based on next hop which is not the correct input for adjacency.

Workaround: Disable fast switching on MGRE tunnel interfaces.

- CSCsm04843

  Symptoms: PXF crashes seen with TCAM parity errors.

  Conditions: These crashes will happen when: 1. The parity error happens at an invalid entry. 2. Multiple parity errors happen within a very short time.

  Workaround: There is no workaround.

- CSCsm16355

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive ISG PPPoA call bringup.

  Conditions: The symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsm20461

  Symptoms: In an IPv6-over-IPv4 MGRE tunnel, disabling IPv6 Cisco Express Forwarding (CEF) without disabling IPv4 CEF results in dropped packets after decryption. Enabling **debug crypto engine packet** on the router helps verify the packet drops after decryption.

  Conditions: The bug is seen if IPv6 CEF is disabled but IPv4 CEF enabled and when tunnel protection is enabled on the MGRE interface.

  Workaround: If IPv6 CEF is disabled, disable IPv4 CEF also.

- CSCsm26466

  Symptoms: The active route processor displays the message %MCASTRED-3-BULKACKTIME and the standby route processor will timeout and reload during a bulk sync.

  Conditions: Seen on an ASR-1000 configured for multicast With a medium/large scale config (thousands of VLANs). On reload the standby will sync correctly.

  Workaround: Reducing the size of config will limit the risk of a timeout.

- CSCsm32130

  Symptoms: Router crashes while performing simultaneous operation in vc-class.

  Conditions: Occurs on a Cisco 7200 running an internal version of Cisco IOS Release 12.4T. This may happen when the router is accessed from multiple terminals simultaneously, configuring the **vc-class atm** *WORD* command.

  Workaround: Avoid simultaneous operation from multiple Telnet sessions on this configuration.

- CSCsm62215

  Symptoms: A Cisco router may reload unexpectedly when the DMVPN tunnel is bounced.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(11)T2. The information points to an SW issue when upon bouncing the DMVPN GRE tunnel the NHRP is automatically cleared which triggers the bus error crash.

  Workaround: Clear the DMVPN session only using the following command (note: the static must be used to clear the individual session or all will be cleared): **clear dmvpn session [peer {nbma | tunnel** *ip- address*] [**interface tunnel** *number*] [**vrf** *vrf- name*] [**static**].

- CSCsm73364

  Symptoms: The router will crash if the routing instance has been removed and an instance-specific command is issued (e.g. shutdown, maxpaths, split horizon etc).

  Conditions: The symptom is observed when removing an instance from either console or VTY while another console or VTY is still in router mode.

  Workaround: Exit and re-enter router mode before issuing any instance- specific commands.

- CSCsm82264

  Symptoms: When standby boots up, deadlock could happen, causing the standby to crash. Also can happen when the call-home process is restarted on active, causing the active supervisor to crash.

  Conditions: This problem depends on timing. Occurs after configuration changes could alter bootup timing.

  Workaround: There is no workaround.

- CSCsm82551

  Symptoms: You may see ASR1000-WATCHDOG: Process = IP Background followed by Traceback message during system bootup.

  Conditions: This happens when L2VPN is configured. It may be likely to occur when many interfaces are configured.

  Workaround: There is no workaround.

- CSCsm97014

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

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

  Workaround: There is no workaround.

- CSCsm98756

  Symptoms: CPU utilization peaks at 99% for a sustained period when issuing **show run | inc ipv6 route**.

  Conditions: With a large scale configuration (thousands of VLANs), performing **show run | inc ipv6 route** causes CPU utilization to peak at 99% and various control plane functions such as SBC call setup may not function as expected.

  Workaround: Redirect the **show run** command output to a file for post-processing.

- CSCso07520

  Symptoms: In a high availability/stateful switchover (SSO) environment, when a switchover occurs, an established OSPFv3/BFD peer will flap.

Conditions: The environment in which this issue can be reproduced is one of an route processor (RP) SSO state along with the configuration of at least one OSPFv3 BFD client. A series of one or more RP/SSO switchovers will cause a BFD peer/link flap.

Workaround: The only workaround at this point is to not execute or trigger an RP/SSO switchover with any established OSPFv3 BFD peers.

- CSCso18683

  Symptoms: On a catalyst 6500, mac entries might not get programmed correctly because the request to program the entries is stuck in a queue which is blocked by a purge request.

  Conditions: The exact conditions are unknown but it has been seen on one particular router consistently. It might happen when a purge request is issued.

  Workaround: There is no workaround

- CSCso45508

  Symptoms: Fragmented multicast rekeys and pings are not acknowledged by a multicast receiver.

  Conditions: Occurs when fragmented multicast packets are received on a multicast receiver interface with crypto map attached.

  Workaround: There is no workaround.

- CSCso47363

  Symptoms: A Cisco router may crash when the **no bba-group pppoe** *word* command is issued from the VTY.

  Conditions: This symptom is observed on a Cisco router when the **bba- group pppoe** *word* command is issued from the console and removed from VTY using the **no bba-group pppoe** *word* command. In this mode, when giving the command service profile “abcd refresh 2” in the console, the router will crash.

  Workaround. There is no workaround.

  Further Problem Description: The issue impacts device operations. This is a corner case issue, seen in an unusual sequence of testing. This issue is not seen on Cisco IOS Release 12.4(21).

- CSCso51749

  Symptoms: QoS works fine with unicast packets over a GRE tunnel, but it does not work for multicast over GRE tunnels.

  Conditions:

  1. Apply a simple policing policy on a GRE tunnel.
  2. Build an mroute table entry.
  3. Send multicast traffic switched over the tunnel.
  4. Verify the police functionality.

  Workaround: There is no workaround.

- CSCso99283

  Symptoms: The RP crashes when using Cisco IOS Release 12.2(33)SRC.

  Conditions: The symptom is observed when using the command **show ipc port**.

  Workaround: There is no workaround.

- CSCsq09377

  Symptoms: The ESR-HH-1GE card on a Cisco 10000 router may crash with the following message:

  ```
  "%PXF_NICKEL-2-IB_ERR_SPR: IB Stuck Pause Request Error in slot X/Y"
  ```

  Conditions: The crash is seen on a Cisco 10000 platform that is running Cisco IOS Release 12.2(31)SBX. Previous Cisco IOS versions are potentially affected. Some known conditions that trigger this error are:

  1. Continuously flapping the interface using **shut** and **no shut** of the ESR-HH-1GE interface.
  2. Changing the MTU size (it is seen only on ATM based cards).
  3. Continuously setting and resetting the negotiation using the **negotiation auto** and **no negotiation auto** commands on ESR-HH-1GE interface.
  4. Most of the customer issues that trigger this error are not yet known.

  Workaround: There is no workaround.

  Further Problem Description: The “IB_ERR_SPR” indicates that the egress data path of the LC is stuck, and the only way to recover the path is to reset the LC. In most of the conditions explained above, the LC was only stuck for few seconds, and in those cases, the LC was unnecessarily reset. In this fix the IB_ERR_SPR handling is improved to avoid such LC resets.

- CSCsq13554

  Symptoms: Router crashes when the **clear ip nhrp group** command is used.

  Conditions: Conditions are unknown at this time.

  Workaround: Do not use this command.

- CSCsq20928

  Symptoms: In certain scenarios the IPv6 neighbor discovery and CEF entries get out of sync and as a result traffic for IPv6 cannot be forwarded.

  Conditions: One known condition is to apply a service policy that classifies IPv6 packets.

  Workaround: There is no workaround.

- CSCsq31602

  Symptoms: DBS enabled VCs are not syncing to standby RP. This issue is reproducible even with a single VC when the router is reloaded.

  Conditions: This symptom is observed on a Cisco 10000 series router that is a HA setup with SSO mode configured.

  Workaround: Resetting the standby will bring the VCs up.

  Further Problem Description: This will effect the synchronization of PPP sessions to standby.

- CSCsq40088

  Symptoms: A Cisco 3845 router may crash when unconfiguring IPv6 nodes.

  Condition: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4T. The traceback is produced after configuring the **no ipv6 unicast-routing** command.

  Workaround: There is no workaround.

- CSCsq40659

  Symptoms: A client may not get a prefix when it has two relay agents on two interfaces of a single DHCP relay agent, with one of them being an unnumbered interface.

  Conditions: The symptom is seen on a router that is running Cisco IOS Release 12.4T.

Workaround: There is no workaround.

- CSCsq45502

  Symptoms: Serials that are part of MLPPP/MFR remain in a down state. This issue can also happen for serial interfaces with PPP, FR and HDLC encap.

  Conditions: This symptom is observed when T1/E1 controllers remain down. Trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCsq45836

  Symptoms: Dynamic Multipoint VPN (DMVPN) shortcut tunnels may fail to get established on a DMVPN spoke running a phase 3 setup.

  Conditions: Occurs in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround. However, data traffic would not be affected since the packets would take the spoke-hub-spoke path.

- CSCsq49768

  Symptoms: MAC L2TP clients failed to setup tunnel after L2TP network server (LNS) upgraded to Cisco IOS Release 12.4(19.18)T3.

  Conditions: Occurs when Mac OS X 10.4 and Mac OS X 10.5 clients attempt to connect to a LNS running Cisco IOS Release 12.4(19.18)T3. image loaded.

  Workaround: There is no workaround.

- CSCsq51826

  Symptoms: Router crashes when Flexible NetFlow for IPv6 is received and IPv6 fragmented packets are received.

  Conditions: Flexible Netflow for IPv6 must be configured and fragemented IPv6 packets must be received.

  Workaround: Deconfigure IPv6 Flexible NetFlow.

- CSCsq70588

  Symptoms: A router's memory 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.

- CSCsq75661

  Symptoms: An ATM interface that is configured with a large number of PVCs may exhibit PVC provisioning problems after repeated interface flaps. The VCC count on the ATM interface would increase by a random number once after each flap.

  Conditions: This symptom is observed on a dual PRE2 system that is running Cisco IOS Release 12.2(31)SB12 code and operating in SSO mode.

  Workaround: Router reload or PRE cutover.

- CSCsq88391

  Symptoms: Standby device configured for stateful switchover (SSO) continuously reloads.

  Conditions: The reload occurs as soon as the standby and primary devices are loaded with stateful switchover (SSO) configuration.

Workaround: There is no workaround.

- CSCsq91258

  Symptoms: L2 entries are deleted and reinstalled periodically and needlessly even when L3 entry is associated with it.

  The expected behavior is that with L3 multicast routing enabled, a L3 MSC GCE is mirrored to L2 MCAST GCE and the L2 entry is never cleared even when IGMP leaves are received or when source stops sending traffic. This is because the entry is associated with L3 entry, and L3 entry clearing process would take care of this removal of L2 multicast GCE/entry as well.

  Conditions: When L3 multicast routing is configured and source-only entries are deleted.

  Workaround: There is no workaround.

- CSCsq92063

  Symptoms: Router may crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a flow record that includes layer 4 fields and the flow monitor is applied to IPv6 traffic, and the traffic that FNF is monitoring has a payload length that does not allow us to reach the tranport header in the IPv6 packet.

  Workaround: Configure Flexible NetFlow with a record that does not have any layer 4 (transport) fields.

- CSCsq99299

  Symptoms: Router crashes during traceback generation with a bus error.

  Conditions: When CPUHOG occurs, traceback is generated. In some cases, it may lead to crash due to uninitialized internal data.

  Workaround: There is no workaround.

- 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.

- CSCsr05431

  Symptoms: There is a traffic drop after an SSO.

  Conditions: The symptom is observed with high scaling, lots of VRFs, and a core with no load sharing. It is seen with two VRFs that are overloaded and slow due to the shared link.

  Workaround: There is no workaround.

  Further Problem Description: Use the graceful restart timer to increase the time that it takes the the initial and subsequent peers to come up, before doing bestpath calculations.

- CSCsr09208

  Symptoms: A memory allocation error shows (cause: memory fragmentation) when there is plenty of memory available.

Conditions: The symptoms are observed when configuring a large number of ACLs. The memory fragmentation issue is gone after removing the ACLs.

Workaround: There is no workaround.

- CSCsr15478

  Symptoms: An input wedge is observed on an interface, when multicast traffic is flowing.

  Conditions: The symptom is observed in a DMVPN hub-spoke scenario with a point-to-multipoint (P2MP) GRE tunnel having tunnel protection configuration. When multicast traffic flows from hub to spoke through these tunnel interfaces, the incoming interface of the hub is getting wedged and even the ping to peer stops working.

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

- CSCsr16147

  Symptoms: Session is not getting disconnected when the locally configured timers expire.

  Conditions: Occurs while testing an internal build of Cisco IOS Release 12.4(22)T on the Cisco 7200.

  Workaround: There is no workaround.

- CSCsr21842

  Symptoms: On a Cisco 7200 series router that has a crypto map protecting GRE tunnel traffic, putting an inbound ACL to drop the decrypted, GRE- decapsulated IP traffic may not work. The traffic is not dropped as expected and there is no hit count on ACL/ACE (although permit ACE still works properly and receives hit counts).

  Conditions: The symptoms are observed with the following conditions:

  1. On a Cisco 7200 series router with K9 images.
  2. Where a crypto map is applied on a physical interface protecting GRE tunneling traffic (47 host2host)
  3. When “deny inbound ACL” is configured on the tunnel interface to drop the cleartext (the traffic will not be dropped as expected).
  4. It occurs with certain configuration sequences, such as configure tunnel and crypto map. (If you bring up IPSec SA, then apply inbound ACL to the tunnel interface, then save the configuration at the start-up configuration and boot from there, the issue may not show up.)
  5. This only affects inbound ACLs. Outbound ACLs are not affected

  Workaround: Use an inbound crypto map ACL (ipsec-dACL) instead of a inbound ACL on tunnel in this senario. Inbound crypto map ACL sees the decrypted GRE packets, and it can drop the traffic properly. For example:

  ```
  router#sh cry map Crypto Map "testtag" 10 ipsec-isakmp Peer = 10.0.0.8 Extended IP
  access list 101 access-list 101 permit gre host 10.0.0.9 host 10.0.0.8 Extended IP
  access check IN list imacl access-list imacl permit ahp any any access-list imacl
  permit esp any any access-list imacl deny gre any any access-list imacl permit ip any
  any Current peer: 10.0.0.8 Security association lifetime: 4608000 kilobytes/3600
  seconds PFS (Y/N): N Transform sets={ proposal1: { ah-sha-hmac } , { esp-3des
  esp-sha-hmac } , } Interfaces using crypto map testtag: GigabitEthernet0/1
  ```

  Alternate workaround: Turn off CEF switching and use process switching.

- CSCsr23454

  Symptoms: A device reloads with a bus error and may display the following message:

  ```
  CMD: ’ aggregate-address 224.0.0.0 224.0.0.0 attribute-map GCI-aggregations
  suppress-map Suppress-ESNAK’ Address Error (load or instruction fetch) exception, CPU
  signal 10, PC = 0x60CDD444
  ```

  Conditions: The symptoms are observed on a device configured with Border Gateway Protocol (BGP).

  Workaround: There is no workaround.

- CSCsr39340

  Symptoms: Packets may be dropped.

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

  Workaround: There is no workaround.

- CSCsr40997

  Symptoms: When a router interface is shut, the prefix attached to the interface is not advertised with infinite metric out the other interfaces.

  Conditions: Occurs when route is configured for RIP for IPv6 (RIPng)

  Workaround: There is no workaround.

- CSCsr44967

  Symptoms: When registering a multi-event Tool Command Language (TCL) policy in the Embedded Event Manager (EEM), the registration will fail with the following error message:

  ```
  %HA_EM-6-FMPD_EEM_LOG_MSG: Register event failed: Only correlate and attribute
  statements are allowed within trigger
  ```

  Conditions: The symptom is observed on all multi-event TCL policies in EEM 2.4 when the trigger block contains a closing brace that is by itself on a line. For example:

  ```
  ::cisco::eem::trigger { ::cisco::eem::correlate event e1 or event e2 or event e3 or
  event e4 ::cisco::eem::attribute tag e1 occurs 1 ::cisco::eem::attribute tag e2 occurs
  1 ::cisco::eem::attribute tag e3 occurs 1 ::cisco::eem::attribute tag e4 occurs 1 }
  ```

  Workaround: Add a space to the beginning of the line with the closing brace of the trigger block:

  ```
  ::cisco::eem::trigger { ::cisco::eem::correlate event e1 or event e2 or event e3 or
  event e4 ::cisco::eem::attribute tag e1 occurs 1 ::cisco::eem::attribute tag e2 occurs
  1 ::cisco::eem::attribute tag e3 occurs 1 ::cisco::eem::attribute tag e4 occurs 1 }
  ```

  Further Problem Description: This will not impact customer network and traffic.

- CSCsr46367

  Symptoms: When registering an Embedded Event Manager (EEM) Tool Command Language (TCL) policy that has multi-event correlation for just track objects, the EEM system may get into an inconsistent state where a previously registered TCL policy will not be triggered, unregistered, or reregistered. This is seen when the following error is printed while registering the problematic policy: Embedded Event Manager configuration: failed to register the event spec for policy all_track.tcl: requested function is not supported

  Conditions: The symptom occurs only if the event manager server returns an error while trying to register an event. In this case the error is "function is not supported" because a multi-event TCL policy must have at least one event in the correlation statement.

  Workaround: Do not try to register a policy that is unsupported.

- CSCsr49376

  Symptoms: Device Reloads after EIGRP adjacency changes.

Conditions: Occurs on a Cisco Catalyst 3560 running Cisco IOS Release 12.2(44)SE. This has been observed on several other devices also. At this stage, the root cause has not been found.

Workaround: There is no workaround.

- CSCsr57815

  Symptoms: Unable to attach a VC class to ATM sub-interface after unconfiguring **mpls experimental 1**.

  Conditions: The symptom occurs with a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCsr61532

  Symptoms: Router may experience dropped packets.

  Conditions: Occurs when passive probing is configured with mode select-exit best. A prefix is rotated through all exits for holddown time to get passive performance on all exits. In doing so, if a link is already overloaded, putting prefix on the overloaded link can cause the performance to further deteriorate.

  Workaround: There is no workaround.

- CSCsr62545

  Symptoms/Conditions: RPM-XF cards 9(active) and 11(standby) are in redundancy. When we reset the active card, we see that secondary card 11 comes up as active but primary card 9, instead of coming up as standby, is continuously rebooting, resulting in many crashinfo files being generated.

  Workaround: There is no workaround.

- CSCsr68212

  Symptoms: MVRF name may get truncated if the VRF name is too long.

  Conditions:VRF name itself can be as long as VRF_MAX_NAME (32). When its length is 32, MVRF name mvrf_string will be truncated.

  Workaround: Use VRF name less than 32.

- CSCsr72674

  Symptoms: With MPLS over GRE enabled. There is a possibility where the RP could encounter a software exception resulting in a crash.

  Conditions: With MPLS VPN enable over a tunnel (GRE in this case), and that the tunnel is configured to be associated with a user-configured VRF.

  Workaround: There is no workaround.

- CSCsr82152

  Symptoms: With rsp720-10G in a S-chassis or 7604 chassis, sometimes on switchover, the traffic stops through sip400 or traffic loss is greater than 800Msec.

  Conditions: rsp720-10G in a S-chassis or 7604 chassis and sip400/sip200 as line card.

  Workaround: No proper workaround. SIP400 module soft reset might help if traffic is stuck.

  Further Problem Description:

- CSCsr85093

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

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

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

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

- 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.

- CSCsr94563

  Symptoms: When registering an Embedded Event Manager (EEM) policy in a scheduler class that has no threads allocated to it, EEM will produce the following error message:

  ```
  %HA_EM-4-FMPD_NO_SCHED_THREAD: No threads are configured to service event class
  ```

  When attempting to unregister the policy, EEM may produce the following error and the policy will not be unregistered:

  ```
  EEM configuration: failed to unregister the event spec for policy policyname: unknown
  event ID
  ```

  In addition, a triggered event will not actually run once this problem is experienced.

  Conditions: This symptom is observed in images with the fix for CSCsr46367 and support for different scheduling classes in the EEM server.

  Workaround: First allocate some threads to the class, and then configure the policy in that class.

  Further Problem Description: This problem affects both Tcl-based policies and applets.

- CSCsr96084

  Symptoms: A router crashes with the following error:

  ```
  %SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000
  ```

  Conditions: The symptom is seen on routers that are running Dynamic Multipoint VPN (DMVPN) when a routing loop occurs while an NHRP resolution request is received by the router. If the routing loop leads to a tunnel recursion (where the route to the tunnel endpoint address points out of the tunnel itself) the crash may be seen.

  Workaround: Use PBR for locally-generated traffic to force the GRE packet out of the physical interface which prevents the lookup that can lead to the recursion. For example (note: the interfaces and IPs will need to be changed to the appropriate values):

  ```
  interface Tunnel97 ... tunnel source POS6/0 ...
  interface POS6/0 ip address 10.2.0.1 255.255.255.252
  ip local policy route-map Force-GRE
  ip access-list extended Force-GRE permit gre host 10.2.0.1 any
  route-map Force-GRE permit 10 match ip address Force-GRE set interface POS6/0
  ```

- CSCsr98707

  Symptoms: When the main ATM interface MTU has an explicit non-default value (something other than 4470), then the subinterfaces may not save (shown with the **show run** command) the explicit MTU configuration of the default (4470) even though the command is expected.

  Conditions: The symptoms are observed only for the ATM MTU value 4470. This unexpected behavior is not seen for any other value (less than or more than 4470 within allowed ATM MTU values).

Workaround: Upon reload, manually (explicitly) configure MTU 4470. You can configure an IP MTU under the ATM interface instead of an ATM MTU.

- CSCsr99022

  Symptoms: Remove interface virtual-template, then reconfigure it IOS failed to create virtual-template interface

  Conditions: Remove interface virtual-template

  Workaround: Do not remove virtual-template interface

- CSCsu10261

  Symptoms: ISSU downgrade does not always work.

  Conditions: Will see the following messages:

  ```
  %RF-5-RF_RELOAD: Peer reload. Reason: RF Client BFD RF Client(146) notification
  timeout %REDUNDANCY-4-RELOADING_STANDBY: Reloading the Standby RP %RF-3-NOTIF_TMO:
  Notification timer Expired for RF Client: BFD RF Client(146)
  ```

  Workaround: There is no workaround.

- CSCsu20376

  Symptoms: When a user configures the **exception flash all disk1:core1** command, the resulting coredump pathname becomes "disk1:core1:ram1-7206-2-coreiomem.Z". The presence of the ":" following core1 is bogus since ":" is a reserved character used to delimit device and partitions. And "core1" is not a valid partition identifier.

  A reasonable interpretation of "core1" would be as an existing subdirectory, not as the first 5 characters of a core file name.

  Conditions: Occurs when user configures the **exception flash all disk1:core1** command.

  Workaround: Copy the core dump to "disk1:" instead of "disk1:core1". Use "exception flash all disk1:".

- CSCsu25016

  Symptoms: The **pppoe-client** command is not accepted on ATM interfaces. Cisco IOS software will report "% Unrecognized command" when an attempt is made to configure it.

  Conditions: This symptom is observed when an attempt is made to configure the **pppoe-client** command.

  Workaround: Use **pppoe_client** as the command prefix followed by the normal pppoe-client configuration items.

- 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.

- CSCsu45342

  Symptoms: CCM enums for client types have diverged between mcp_dev and other branches

  Conditions: ISSU from MCP and other related brances

  Workaround: There is no workaround.

- CSCsu59900

  Symptoms: Standby RP crashes.

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

  Workaround: There is no workaround.

- CSCsu62175

  Symptoms: Error message with a traceback is observed while configuring IPSec authentication/encryption for an IPv6 Open Shortest Path First (OSPF) process with no router-id.

  Conditions: The error message is issued when authentication or encryption is configured for an OSPFv3 process that has not been able to obtain a router-id.

  Workaround: Provide a loopback or other "up" interface with an IPv4 address, or use the **router-id** command to establish the OSPFv3 router-id before configuring OSPFv3 authentication or encryption.

- CSCsu62356

  Symptoms: Under certain conditions the RIP for IPv6 (RIPng) “Last Gasp” message (all metrics infinite) does not get sent.

  Conditions: This is seen under high load or on routers with large numbers of interfaces.

  Workaround: There is no workaround but routes will eventually time out.

- CSCsu68245

  Symptoms: A router may crash.

  Conditions: The symptoms are observed when traffic is flowing and if the interface is **shut** then **no shut**.

  Workaround: There is no workaround.

- CSCsu78975

  Symptoms: Crash seen @adj_switch_ipv4_generic_les on a Cisco 3800 router.

  Conditions: This symptom is observed upon issuing the command **no ip route 10.2.82.0 255.255.255.0 vlan1**.

  Workaround: There is no workaround.

- CSCsu79988

  Symptoms: Before this BGP aspath memory optimization, the memory consumption for aspath has increased. With this memory optimization, the memory consumption for aspath has reduced.

  Workaround: There is no workaround.

- CSCsu90369

  Symptoms: Messages similar to the following are seen on switchover:

  ```
  %ISSU-SP-3-NOT_FIND_MSG_SES: Can not find message session(0) to transform msg from
  receive side %XDR-SP-6-ISSUBADRCVTFM: Failed to rcv_transform message - slot RP (28),
  reason: ISSU_RC_MSG_SESSION_NOT_REGISTERED
  ```

Conditions: The messages may be displayed during switchover from an active RP to a standby RP. The likelihood of appearance of the messages is dependent on the timing of the switchover and the configuration in use.

Workaround: There is no workaround.

- CSCsv15931

  Symptoms: Crash is seen when L2TP HA is configured with tunnel and session teardown scenario.

  Conditions: When tunnels are cleared with **clear vpdn tunnel** comand when the tunnel/session are being established.

  Workaround: There is no workaround.

- 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.

- CSCsv23797

  Symptoms: ASR Router goes down.

  Conditions: Occurs when when kron policy is configured and SCP is used.

  Workaround: Use regular SCP.

- CSCsv25088

  Symptoms: When the IMA group statement under the atm3/0 T1 interface is removed, the other T1s will still remain up in the IMA group, but the PVC will become inactive. This symptom happens only when the ATM Bandwidth Dynamic statement is under the atm1/ima main interface. When removing the IMA group under atm3/1 without the ATM Bandwidth Dynamic statement under the atm3/ima0 interface, the PVC stays up on line.

  Condition: This problem is seen in the Cisco 7206vxr with a npe-g1 or npe-400 with the 8-port PA IMA card PA-A3-8T1IMA. The problem is not see in Cisco IOS Release 12.3(28)M, but the problem is seen in Cisco IOS Release 12.4(6)T11 and 12.4(15)T6/T7 and also in Cisco IOS Release 12.4(20)T and 12.4(21)M.

  Workaround: Re-add ima-group 0 back under the atm3/1 interface and then shut down the atm3/1 interface.

  Further Problem Description: Steps to recreate the issue:

```
configure terminal
int atm3/1
no ima-group 0 < take out
int atm3/2
ima-group 0
int atm3/3
ima-group 0

atm3/ima0
atm bandwidth dynamic

atm3/ima0.1
ip address x.x.x.x
pvc 1/101
vbr-nrt 4500 4500
```

  The **show atm vc** will show the PVC as inactive.

- CSCsv36306

  Symptoms: If **show bfd neighbor** is issued on a router while BFD sessions on peer are flapping, it makes the router crash.

  Conditions: When there is just one BFD session between peers with just one client and sessions begin to flap.

  Workaround: There is no workaround.

- CSCsv43385

  Symptoms: Connectivity from a Dynamic Multipoint VPN (DMVPN) hub router to spokes may be lost due to a invalid Cisco Express Forwarding (CEF) adjacency.

  If tunnel protection is configured on the hub, the traffic from hub to spokes will get dropped on the tunnel interface and the **show interface tunnelx** command will show the "Total output drops" counter incrementing.

  This is intermittent and the problem will generally appear right after a reload of the router. It may not happen after some reloads of the router.

  Conditions: Seen only on Cisco IOS Release 12.4(20)T and 12.4(22)T

  Workaround #1: Disable/enable the tunnel mode: interface Tunnel30 no tunnel mode gre multipoint tunnel mode gre multipoint

  Workaround #2: Remove the tunnel configuration and re-add it: no interface Tunnel30 interface Tunnel30 ip address 192.168.50.1 255.255.255.0 ip nhrp authentication cisco ip nhrp map multicast dynamic ip nhrp network-id 111 ip nhrp holdtime 900 tunnel source FastEthernet0/0 tunnel mode gre multipoint

- CSCsv46240

  Symptoms: A flow exporter that is configured for v9 may export corrupt data.

  Conditions: This symptom occurs under the following configuration sequence:

  - Create a flow exporter, but do not set any values within the exporter.
  - Create a flow monitor, and apply the exporter to it.
  - Apply the flow monitor to an interface.
  - Configure the destination of the exporter.

  Workaround: Configure the destination of the exporter before applying it to any flow monitors. Alternatively, remove the flow monitor from all interfaces and reapply it, which causes correct export packets to be sent.

- CSCsv60775

  Symptoms: EoMPLSoGRE Tunnel on a Cisco 1805 fails to forward packets after the the tunnel is established.

  Conditions: Approximately the first 200 packets are forwarded, but then the router stops forwarding packets across the tunnel.

  Workaround: There is no workaround.

- CSCsv61816

  Symptoms: Issue in ISDN call setup.

  Conditions: This symptom is observed on a Cisco router when making a isdn test call.

  Workaround. There is no workaround.

- CSCsv62004

  Symptoms: With IPbase image, standby reloads on configuring **vrf definition** or if the running configuration includes 6VPE configurations **route-target**, **rd** commands.

  Conditions: This occurs on ipbase images which do not support 6VPE configurations. If the user tries to restore a configuration that includes VRF commands, the standby reloads continuously. If the user tries to configure **vrf definition** with ipbase image also, the problem will be seen.

  Workaround: Remove the VRF configuration in the boxes that run IPbase images and the boxes come up fine.

- CSCsv66215

  Symptoms: Problem with IPv6 when deactivating and then reactivating VPN routing/forwarding (VRF).

  One symptom is a message "Can’t activate address-family ‘ipv6’ "

  Another aspect is a reference to tableid 10000000 that is reserved and should not apply to VRF.

  Conditions: Occurs when using VRFs. The problem only occurs if IPv6 routing is used and then fully removed. When IPv6 is removed from the system, the IPv6 RIB goes away. One way of reactivating the IPv6 RIB is indirectly to create some VRFs. In that case, it is possible that the tableid 10000000 be allocated to a VRF, in which case the problem occurs.

  Workaround: The path that leads to the problem consists in allocating the IPv6 RIB indirectly via VRFs installation. The problem only occurs at reactivations. There are thus a few ways to workaround:

  – Reboot the router.

  – Configure **ipv6 unicast router** or IPv6 on interfaces before entering VRF configuration.

- CSCsv73721

  Symptoms: The following tracebacks appeared on the active RP console during router boot up:

  ```
  000131: *Nov 12 16:16:43.075 EST: %ISSU-3-FAILED_TO_ALLOC_UNDER_ENDPOINT: Can not
  allocate transport id(131072) control block.
  -Traceback= 1#04182c093c3bf3fa21a9ef089770e5a6 :10000000+5179E0 :10000000+518294
  :10000000+515F3C :10000000+200F5DC :10000000+200E5C4 :10000000+1F78A0C 000132: *Nov 12
  16:16:43.077 EST: %ISSU-3-ERP_CLIENT: For context ID 131072, Current context for ERP
  isn’t available
  -Traceback= 1#04182c093c3bf3fa21a9ef089770e5a6 :10000000+5179E0 :10000000+518294
  :10000000+515F3C :10000000+200E898 :10000000+1F78A0C 000133: *Nov 12 16:16:43.078 EST:
  %IPC-3-ISSU_ERROR: ISSU register peer failed failed with error code 0 for seat 20000
  -Traceback= 1#04182c093c3bf3fa21a9ef089770e5a6 :10000000+5179E0 :10000000+518294
  :10000000+515F3C :10000000+1F78D5C
  ```

  Conditions: The symptom will show up at boot up if the box has more than 10 ISSU endpoints. ISSU aware RP, SP, linecards all count as endpoints.

  Workaround: There is no workaround.

- CSCsv76105

  Symptoms: Standby supervisor crashes during bootup.

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

  The crash occurs if the following commands are configured:

  ```
  snmp mib notification-log globalsize 10000
  snmp mib notification-log globalageout 120
  snmp mib notification-log default
  ```

  Workaround: Remove the above commands from the configuration.

- CSCsv76862

  Symptoms: A Cisco router running a version of code that contains the Embedded Event Manager (EEM) version 3.0 or EEM version 3.1 may:

  - Allow a policy in the user policy directory to be registered as a system run-type policy.
  - Allow a policy to be registered where the user specifies a type of system but the policy is registered as a run-type user policy.
  - Require the user to specify a type of user when registering a policy to override a system policy.
  - Prevent a policy that was registered with a type of user specified in the policy registration command to be unregistered using the no form of the policy registration command.
  - Not generate a configuration command when a default option to Mandatory policy is changed so the change can not be saved to the startup-config.
  - Not generate a configuration command when a user policy is being used to override a system Mandatory policy so the user policy will need to be re-registered after every bootup.
  - Leak memory when a Mandatory policy is registered and unregistered and an error occurs.

  Conditions: These occur in Cisco IOS and Cisco IOS software modularity versions that contain EEM version 3.0 and EEM version 3.1. EEM versions 2.4 and earlier are not affected. Users can check what version of EEM is in their image by using the **show event manager version** command that was introduced in EEM version 2.4.

  Workaround: There is no workaround.

  Further Problem Description: The EEM command to register a policy is:

  event manager policy *filename.tcl*

  This command has an option to specify a type of either *system* or a type of *user*. This option is designed to allow the user to specify which directory is searched when looking for the policy to register. If the user specifies a type of system, the system policy directory (hardcoded in the image) is searched for apolicy with the filename specified. If the user specifies a type of user, only the user policy directory (which must be configured with the **event manager directory user policy** *device:directory* command) is searched. If the user does not specify a type, first the user policy directory is searched and if no policy is found then the system policy directory is searched - this allows the user to override a system policy with a user policy and not have to specify a type of user.

  The concept of which directories are searched when registering a policy is different from the concept of which run-type the policy is registered with. The run-type specifies the privilege level that the policy will execute with. System policies have full privileges. User policies are limited to the privileges of Safe-Tcl with a few exceptions that are covered in the EEM documentation. The run-type of the policy is determined by the following rules:

  - If a policy is in the system policy directory at the time it is being registered, that policy will be registered with a run-type of system.
  - If a policy is in the user policy directory at the time it is being registered and it does not contain a valid Cisco digital signature it will be registered with a run-type of user. Exception: If the policy is in the user policy directory at the time it is being registered and it contains a valid Cisco digital signature it will be promoted to a run-type of system.

  The problems described in this bug occur because of an implementation that jumbled these two concepts together.

- CSCsv77932

  Symptoms: Router crashes.

  Conditions: Occurs while configuring serial interface for insufficient MTU.

Workaround: There is no workaround.

- CSCsv80230

  Symptoms: The standby RP in a Cisco 7600 series and some of its linecards may crash numerous times upon booting.

  Conditions: Seen in a Cisco 7600 with dual RPs.

  Workaround: There is no workaround.

- CSCsv81635

  Symptoms: When traffic engineering (TE) and fast reroute (FRR) are configured between a stitching router and provider edge (PE), Virtual Circuit Connection Verification (VCCV) ping fails.

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Disable TE and FRR.

- CSCsv83645

  Symptoms: With 1600 pseudowires configured on Cisco 7600 as S-PE, when online insertion and removal (OIR) is performed on core interface, some of the pseudowires do not come up.

  Conditions: The OIR of core interface creates this condition.

  Workaround: There is no workaround.

- CSCsv84557

  Symptoms: Acct-Session-Id not getting created when unique-ident configured Conditions: Acct-Session-Id not getting created when radius-server unique-ident is configured in NAS Workaround: No workaround

- CSCsw14433

  Symptoms: On UBR10K platform, during PRE runversion of the ISSU upgrade process, the IPC connection between RP and cable line cards may take additional 1 sec to come up.

  Conditions: Happens during PRE runversion.

  Workaround: There is no workaround.

  Further Problem Description:The problem is due to a race condition during IPC issu negotiation. When the PRE finishes ISSU negotiation, it sends the port registry response to the peer cable line card. The race condition happens when the response is received by the line card before the line card has declared ISSU negotiation is done. The response will be dropped, and resent in 1 second, causing the 1 second additional delay.

- 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.

- CSCsw17553

  Symptoms: Catalyst 6500 always sends authentications to a known down ACS server. The **show aaa server** output also shows the ACS server up even with its LAN port shutdown. Therefore in a failover, the use of the secondary ACS server is delayed. The down ACS primary server appears to never be declared as down.

Conditions: Two ACS servers in a primary and backup scenario. When the primary is actively DOWN the Catalyst 6500 always tries to send authentications to it and should declare it as down and use the secondary ACS server. RADIUS messages are even showing up that the primary ACS server is available/connected even with no LAN connection.

Workaround: There is no workaround.

- CSCsw18733

  Symptoms: Cisco 7200 router is crashing while unconfiguring crypto IPSec tunnel with easyvpn client configurations.

  Conditions: Crypto IPSec tunnel configured and then unconfigured.

  Workaround: There is no workaround.

  Further Problem Description: CIsco 7200 crashes while unconfiguring a virtual-template of type tunnel.

- CSCsw19819

  Symptoms: A crash is seen when **show atm pvc <>** command is excuted for a PVC where a VC class is attched with **oam-pvc manage auto-detect**.

  Conditions: This issue is seen when a multipoint sub-interface is configured as point-to-point sub-interface, which throws the error message as expected. After repeated tries upon the **show atm pvc** router crashed.

  Workaround: Do not configure multipoint subinterface as a point to point subinterface.

- CSCsw22106

  Symptoms: Device reloads after EIGRP adjacency changes.

  Conditions: Occurs on a Cisco Catalyst 3560 running Cisco IOS Release 12.2(44)SE. This has been observed on several other devices also. At this stage, the root cause has not been found.

  Workaround: There is no workaround.

- CSCsw24779

  Symptoms: A Cisco 7200 series router emits tracebacks.

  Conditions: The symptom is observed when a service policy with netflow sampler is attached to a PVC.

  Workaround: There is no workaround.

- CSCsw45691

  Symptoms: The atmPreviouslyFailedPVclTimeStamp returns a non-zero value when the VC is brought DOWN for the first time.

  Conditions: This issue is seen on router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- 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.

- CSCsw49297

  Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

  Conditions: This symptom may occur during periods of bursty traffic.

  Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

  ```
  interface Multilink1 ppp multilink queue depth qos 3
  ```

- 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.

- CSCsw69621

  Symptoms: A BR goes down on the learning cycle.

  Conditions: The symptoms are observed when the inside BGP is learning configured:

  ```
  conf t oer master learn no throughput no delay inside bgp
  ```

  Workaround: Configure as follows:

  ```
  conf t oer master learn throughput inside bgp
  ```

- CSCsw75233

  Symptoms: ASR crashes in process "L2TP mgmt daemon" with the following error message:

  ```
  %L2TUN-3-ILLEGAL: Failed to insert into socket DB %L2TP-3-ILLEGAL:
  B0D0B0D:_____:0000CF2C: ERROR: Unable to associate L2TP session with socket handle
  ```

  Conditions: Observed in a ASR1002 when the platform functions as an L2TP Network Service (LNS)

  Workaround: There is no workaround.

- CSCsw78426

  Symptoms: Router crashed after entering the **show atm pvc <>/<>** command.

  Conditions: The issue is seen after configuring Layer 2 transport PVC.

  Workaround: There is no workaround.

- CSCsw87906

  Symptoms: Router crashed due to bgp update while flapping BGP peers at remote side.

  Conditions: Happens specifically on ASR platform.

  The setup is an MVPN configuration with 100PEs and 1Unique MVRF per PE with 100 MVPN group and 1 MVPN source in each VRF. OSPF, iBGP, LDP, PIM SM is used in provides side and PIM SSM in customer side and ASR (PE) is configured as RP.

  Workaround: There is no workaround.

- CSCsw90492

  Symptoms: WRED counters disappear after doing online insertion and removal (OIR) with DLFI over ATM.

  Conditions: Configure DLFI over ATM and attach policy to VT with WRED. Perform a OIR, a WRED will disappear.

  Workaround: Remove policy from VT and attach it

- CSCsw90599

  Symptoms: Unable to remove the grandchild policy from the child policy of a three-level policy.

  Condition: The symptom is observed with a router that is loaded with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsw95793

  Symptoms: When 3000 VCs with PW redundancy are configured in the system, some of the VCs may stay in the DOWN state after the system reload.

  Conditions: It is seen with 3000 VCs on a RP2.

  Workaround: Shut/no shut on the interface can clear the issue.

- CSCsw98231

  Symptoms: RF progression halts at "in progress to standby cold-bulk" on the standby RP during ISSU runversion.

  Conditions: Should only be seen on dual RP/SP platforms during ISSU. Is also affected by timing of start of the CEF sync to the standby SP, so it doesn't happen for many sotware versions/configurations.

  Workaround: Use an alternative upgrade method.

- CSCsw98399

  Symptoms: During the SSO, packet loss is more than expected

  Conditions: AToM VC is UP , before SSO traffic was flowing fine, during SSO, for a few seconds, there was packet outage which again resumed. The outage was more than expected.

  Workaround: There is no workaround.

- CSCsx10140

  Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

  The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitely state what to do if such invalid data is received, so the Cisco implemention of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

  RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

  "To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment

types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message."

The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

(1) For more information please visit:

http://www.merit.edu/mail.archives/nanog/msg14345.html

- CSCsx11266

  Symptoms: With discovered PVCs, stand-by crashes after SSO.

  Conditions: PVCs are discoverd in the main-interface. In one of the VCs, service-policies are attached to mark the CLP. Packets were marked fine through the VCs, but after SSO the new active crashes. ILMI discovered PVC's from the switch are created as PVC-D in both active and standby. But, this PVC-D is not being updated properly on stand-by properly in internal data structure.

  1. PVCs are discoverd in 7600-1
  2. Policy-map is attached to one of the PVC, where atm map is created
  3. trafic is sent from IXIA . 4) Do SSO, the new active crashes

  Workaround: There is no workaround.

- CSCsx15038

  Symptoms: NVgen issue occurs with **violate-action** commands under policy-map class.

  Conditions: When we configure **violate-action** commands with "police cir" and "exceed" under policy-map class, it is not reflected under **show run** output.

  Workaround: Do not configure as a whole with policy cir and eceed command. configure as individual commands.

- CSCsx17881

  Symptoms: Show run command displays "Configuration buffer full message" message

  Conditions: Show run command displays "Configuration buffer full message" message

  Workaround: There is no workaround.

- CSCsx18860

  Symptoms: Traffic does not pass.

  Conditions: The symptom is observed with a Cisco VPN Acceleration Module 2+ (VAM2+) originating traffic and with process switching.

  Workaround: There is no workaround.

- CSCsx30903

  Symptoms: CLI help is not usable in global configuration mode.

  Conditions: The symptom occurs with **cns config notify diff** configured in the router.

  Workaround: There is no workaround.

- CSCsx31996

  Symptoms: When a RP switchover was performed, the booting standby RP was reset with a message of "AAA HA failure" and a few tracebacks thrown out.

  Conditions: Tracebacks occur , when RP s/o is performed.

Workaround: There is no workaround.

- CSCsx32049

  Symptoms: Traceback is observed and the system may reboot, depending on the platform.

  Conditions: The symptom is observed when the ESM filter is configured and contains an ios_config statement.

  Workaround: Remove ios_config statements from ESM filter.

- CSCsx32416

  Symptoms: A session may go down one or more times before stabilizing in the up state.

  Conditions: This symptom is observed when a BFD session is first coming up and the network is suffering from congestion.

  Workaround: There is no workaround.

- CSCsx43644

  Symptoms: Policy-name remains unchanged after renaming.

  Conditions: The symptom is observed only with an ATM interface.

  Workaround: There is no workaround.

- CSCsx47069

  Symptoms: Ping replies have wrong source address.

  Conditions: Occurs after switchover.

  Workaround: There is no workaround.

- CSCsx47260

  Symptoms: Unable to delete the IPv6 DHCP pool.

  Conditions: The symptom is observed after creating an IPv6 DHCP pool with a null string.

  Workaround: Do not create the IPv6 DHCP pool with a null string.

- 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.

- CSCsx52339

  Symptoms: AToM VC does not come up on flapping the interface with SSO.

  Conditions: It happend when **mpls label range** is configured.

  Workaround: There is no workaround.

- CSCsx53733

  Symptoms: BGP session getting flapped while doing ISSU runversion

  Conditions: Configure the router with BGP, do loadversion, proceed with runversion and BGP session flapped here.

  Workaround: There is no workaround.

- CSCsx54861

  Symptoms: Gigaword Accounting attributes not sent in the accounting record.

Conditions: Observed when the sessions input or output traffic goes beyond 2^32 bytes.

Workaround: There is no workaround.

- CSCsx55240

  Symptoms: Router crash seen at **html_config_command**.

  Conditions: This issue is observed on a Cisco 7200 router running Cisco IOS Release 12.4(24.2)T.

  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 router must be configured with one or more VRFs and must have the BGP VPN address family enabled. The problem may be triggered by the deletion of a VRF from the router config 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: To avoid the issue the user can 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 config 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.

- CSCsx58009

  Symptoms: SAMI PPC crashes due to a SegV exception at the L2TP process.

  Conditions: The symptom is observed under the following conditions:

  1. L2TP communication down keeps more than 180 seconds between LAC and LNS.
  2. Crash will occur where the communication down happens after about 17 seconds from receiving the last L2TP hello.

  Workaround: Avoid sending L2TP hello at L2TP shutting down process by L2TP shutdown timer expiration. (For example, use **l2tp tunnel timeout no-session 0**. The command will teardown the session immediately when there is no session.)

- 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.

- CSCsx72853

  Symptoms: Multi-hop PPPoE relay is not working.

Conditions: The symptom is seen with Cisco ASR routers loaded with Cisco IOS Release 12.2XNC and configured with multi-hop PPPoE relay.

Workaround: There is no workaround.

- CSCsx74883

  Symptoms: Router crashes while deleting VRFs when many VRFs are configured and **no router bgp** is immediately followed by **no ip vrf** for all configured VRFs.

  Conditions: Usually seen when many VRFs are configured. VRF deletion of all VRFs must immediately follow removal of the BGP router.

  Workaround: Allow **no router bgp** to complete before issuing the **no ip vrf** commands, or allow the deletion of all VRFs to complete before issuing **no router bgp**.

- CSCsx75623

  Symptoms: Tracebacks are seen when **create on-demand** is configured on a VC class and when an OIR is performed on the ATM interface.

  Conditions: This symptom occurs only if an OIR is performed when the configurations are made.

  Workaround: There is no workaround.

- CSCsx75866

  Symptoms: Use of eigrp STUB feature in a <U>STUB Site</U> could result in routing loops, This issue relates to a network configuration we have not previously supported, therefore your customer should not be affected.

  Workaround: There is no workaround. I your customer wishes to use this feature, then please move to an image with this fix

- 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.

- CSCsx81468

  Symptoms: ISIS neighborship may not get established if we use SIP-400 in core with local switching.

  Conditions: SIP-400 as core.

  Workaround: There is no workaround.

- CSCsx99015

  Symptoms: Modular Cisco IOS router may experience unexpected restart of process iprouting.iosproc if it is configured with two OSPF processes, one of processes redistributes another OSPF process and cost of interface covered by OSPF process being redistributed changes (either via configuration or dynamically on multilink/multichannel interfaces).

  Conditions: Problem is specific to modular Cisco IOS. Problem is specific to the case of redistribution from OSPF into OSPF.

  Workaround: Process restart will have no impact on transit packet forwarding if all routing processes were enabled with NSF.

- CSCsy03374

  Symptoms: The following message may be displayed when using software compression over PPP Multilink:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 1740 bytes failed from 0x2140A734, alignment
  128 Pool: I/O Free: 38080 Cause: Memory fragmentation Alternate Pool: None Free: 0
  Cause: No Alternate pool -Process= "PPP Compress Input", ipl= 0, pid= 178, -Traceback=
  0x23060470 0x214014DC 0x21401BFC 0x21402AD0 0x21407798 0x21F398B8 0x21F376B8
  0x230CB274 0x230CB3D8
  ```

  Conditions: The symptom is observed when the input traffic rate is extremely high. It does not occur over low speed links (for example: ISDN B channels).

  Workaround: Disable software compression.

- CSCsy03781

  Symptoms: Router crashes when detach/ attach a HQF at Fr map-class

  Conditions: Seen with FRF.12 config.

  Workaround: There is no workaround.

- CSCsy07709

  Symptoms: A Catalyst 6500 VSS switch may create the below log message upon failover of supervisors.

  ```
  %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A (if_number 158).
  -Traceback= <snip>
  ```

  Conditions: Occurs when running Cisco IOS Release 12.2(33)SXI.

  Workaround: There is no workaround.

- CSCsy08048

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

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

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

- CSCsy10893

  Symptoms: A router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  Conditions: The symptom is observed when issuing the **show buffers leak** command. It occurs only with certain patterns and scale of traffic and does not occur all the time.

  Workaround: There is no workaround.

- CSCsy15150

  Symptoms: Traceback shows up when **default interface** command is entered.

  Conditions: When ION image is running, and when ISIS is configured on the interface that is to be made to default.

  Workaround: Remove ISIS first with **no ip router isis** command before **default interface** command is entered on the interface.

- CSCsy17342

  Symptoms: A Cisco 2800 series router may reload when configuring and unconfiguring **cns config notify diff interval**.

  Conditions: The symptom is observed when configuring and unconfiguring **cns config notify diff interval** along with a **call-router h323-annexg** configuration.

  Workaround: There is no workaround.

- CSCsy17832

  Symptoms: On an RP SSO, tunnels/sessions were lost.

  Conditions: Bring up L2TP tunnels/sessions Perform an RP SSO.

  Workaround: There is no workaround.

- CSCsy17893

  Symptoms: Ping to a tunnel's own address does not work on an IPIP tunnel.

  Conditions: The symptom is observed when there are other tunnels in existence or forwarding traffic on the router, especially those using different types, such as IPv6-related.

  Workaround: There is no workaround.

- 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.

- CSCsy20891

  Symptoms: The standby reloads.

  Conditions: The symptom is observed with the command **no snmp trap link-status** which is being accepted under the virtual-template even though **no virtual-template snmp** is present in the global configuration mode. After switchover **no virtual-template snmp** is missing on the standby, and the standby reloads when doing the second switchover.

  Workaround: There is no workaround.

- CSCsy32146

  Symptoms: Through-the-box traffic is dropped on the router (when the egress path is from the clear-text side to the encrypted side).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T and with L2TP over IPSec with a front door VRF.

  Workaround: Disable **ip route-cache** and **ip route-cache cef** on the clear-text interface (where the clear-text traffic comes from).

- CSCsy39545

  Symptoms: Tunnel-link-stop record is missing at LAC when clearing the session with **clear pppoe all**.

  Conditions: With **vpdn session accounting network** configured at LAC and when clearing the session with **clear pppoe all** Tunnel-link-stop record is missing at LAC.

  Workaround:

  1. Use default accounting method list for Tunnel link:

```
conf t no aaa accounting network tlss start-stop group radius aaa accounting network
default start-stop group radius
no vpdn session accounting network tlss vpdn session accounting network default end
```

2. Configure session accounting to use named accounting method list:

Configure accounting for both session and tunnel link.

```
conf t interface Virtual-Template1 ppp accounting tlss end
```

- 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.

- CSCsy45414

  Symptoms: OSPFv3 sessions flap due to dead timer expiring.

  Conditions: The devices are directly connected and are using subinterfaces on gig ports. The issue seems to be present after a reload on the box. The interface running ospfv3 does not join ff02::5 group.

  Workaround: Shut/no-shut of the interface or a reload of the box fixes the issue. Removing and adding the OSPFv3 config on the interface will resolve the issue temporarily.

- CSCsy46543

  Symptoms: The WS-X4503+ supervisor reboots/reloads.

  Conditions: This happens only when the **default interface** command is issued to the Cisco IOS HTTP server. The WS-X4503+ is the only supervisor affected. This occurs only when two WS-X4503+ supervisors are installed in a redundant configuration.

  Workaround: Use the CLI to issue the **default interface** command on WS-X4503+ supervisors are installed in a redundant configuration.

  Further Problem Description: The Cisco Network Assistant application communicates with network devices using HTTP or HTTPS. It sends the **default interface** command before applying a SmartPorts macro.

- CSCsy54068

  Symptoms: HQF policer policy with exceed action does not attach. Or, when execute exceed action is in an attached parent policy, policy is removed from the interface.

  Conditions: This symptom is seen in a two level, two rate, two color policy.

  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.

- CSCsy61259

  Symptoms: The router crashes or hangs.

Conditions: The symptom is observed when executing the **show filesystem** command on any file system or when there is pending write to the filesystem that has earlier resulted in an error.

Workaround: There is no workaround.

- 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: Router crahses when removing the vpn service from the PVC.

  Conditions: This symptom is observed on a Cisco router running IOS 12.2(33.01.23)MCP04 .

  Workaround. Do not enable VPN service for PTA service.

- CSCsy62643

  Symptoms: Duplicate packets are sent for all traffic routed to a third-party vendor NLB server running in IGMP mode.

  Conditions: The symptom is observed when PIM is enabled on the NLB server VLAN.

  Workaround:

  1. Use non-IGMP NLB modes (unicast or multicast with static MACs).
  2. Use IGMP snooping querier instead of PIM on NLB SVIs.
  3. If PIM is required on the NLB VLAN interfaces: apply inbound access-list to all PIM router interfaces in NLB VLAN permitting IP traffic to the local physical/virtual IPs and denying traffic with destination of local NLB subnet.

- CSCsy62813

  Symptoms: A multilink bundle which is under heavy packet load may cause the router to reload.

  Conditions: The symptom is observed when an interface, which has just joined a multilink bundle, receives packets at a rate faster than the router can process them.

  Workaround: There is no workaround.

- CSCsy69883

  Symptoms: ATM sub-interface goes down on flapping the primary pseudowire path.

  Conditions: This is seen if Cisco ASR PE is connected to a Cisco 7200 CE router;working fine between two ASRs.

  Workaround: There is no workaround.

- CSCsy70524

  Symptoms: A router crashes upon deleting range PVCs with PPPoE sessions and with bandwidth configured through DBS.

  Conditions: The symptom is observed when deleting the range PVCs with PPPoE sessions.

  Workaround: There is no workaround.

- CSCsy75718

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

  Conditions: The issue appears to be Day 1, reported on a Cisco 7200/NPE-400 and 7200/NPE-G2 that is running Cisco IOS Release 12.4T, 12.4M, or 12.2SB.

  Workaround:

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

  Further Problem Description: The issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire when the PPP user's virtual access interface changes.

  Note: Use case fixed via CSCsy39667:

  1A. PPP session with userid "jerry", VAI 100, and va_swidb "X" goes down.

  1B. New PPP session with userid "jerry", VAI 100, and va_swidb "Y" is negotiated within 5 seconds of 1A.

  Fix Overview: DHCP looks for match on PPP userid and VAI number (not va_swidb) to reclaim DHCP Lease.

  Use-case still requiring a fix:

  2A. PPP session with userid "jerry" and VAI 100 goes down.

  2B. New PPP session with userid "jerry" and VAI 200 is negotiated within 5 seconds of 2A.

- CSCsy76404

  Symptoms: A Catalyst 6500 Series Switch running Modular IOS release 12.2(33)SXI may fail to correctly free memory from the CEF background process, eventually leading to an unexpected reload.

  Conditions: System runs Modular IOS release 12.2(33)SXI. CEF table consistency-check is configured.

  Workaround: Disable the CEF table consistency-check (**no cef table consistency-check ipv4**)

  Further Problem Description: **show memory detailed ios-base allocating-process totals** shows "CEF background process" continually increasing in memory usage.

- CSCsy77842

  Symptoms: The router will display some traceback message.

  Conditions: When the modular IOS image is running, and when ISIS is configured on subinterface, and when ISIS is removed on router level with **no router isis** command.

  Workaround: Remove ISIS at the interface level before removing ISIS at router level.

- CSCsy78382

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

Conditions: If traffic is non IOS control packets this could cause a IOSD crash.

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.

- CSCsy89729

  Symptoms: VCs under VP are recreated continously.

  Conditions: VP is configured under main IMA interface with PCR as some value. Also there is a PVC on a IMA sub-interface. When we shut the sub-interface and then try to change PCR of VP or change it to “no-f4-mgmt” the VCs are recreated continously

  Workaround: Do no shut of the sub-interface and then shut/no sh of the IMA interface. It should work.

- CSCsy90482

  Symptoms: Router reloads when running IPSec.

  Conditions: The symptom is observed when packets decrypted by IPSec are process switched.

  Workaround: There is no workaround.

- CSCsy91226

  Symptoms: IP IRDP packets from CE get stuck in the interface input queue.

  Conditions: The symptom is observed with IP interworking in Ethernet over MPLS over GRE (EoMPLSoGRE) and keepalive enabled on the GRE tunnel. The packets get stuck in the interface input queue of the Xconnect interface.

  Workaround: There is no workaround.

- CSCsy96184

  Symptoms: can result in dup packets on segment when mcast topo changes in multi-vendor environment. The **debug ip pim** command will show PIM(0): Received v2 Assert on Vlan1 from 192.168.1.1 PIM(0): Invalid host address 0.0.0.0

  Conditions: When another router sends PIM assert with source address 0.0.0.0 and RPT bit set, PIM will reject it as an invalid source. Only happens when forwarding on shared tree as this is the only time per RFC 4601 when assert with source address 0.0.0.0 is valid.

  Workaround: Ensure that PIM switches over to source tree(ie. do not use "ip pim spt-threshold infinity") or use pim mode w/o shared tree such as SSM.

- 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.

- CSCsz07103

  Symptoms: Router crash@nvgen_action on configuring 500 IPSec tunnels and **write memory**.

  Conditions: Configuring 500 IPSec tunnels and **write memory**. Might be a scalability issue.

  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.

- CSCsz13123

  Symptoms: Frame-relay DLCI is not released from interface in a certain configuration sequence.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS 12.4T images.

  Workaround: There is no workaround.

- CSCsz16022

  Symptoms: A Cisco 7200 series router may crash with LFIoLL+QoS configurations.

  Conditions: The symptom is observed when the slot for MCT3/MCTE1 is powerdown.

  Workaround: Remove the QoS configurations from the multilink.

- CSCsz16386

  Symptoms: Router will reboot and also causes traceback output.

  Conditions: This happens when running check syntax mode. In syntax mode, when a user enters the event manager applet submode and execute the **no event manager applet** *xxx* two times, this will cause the reboot. "xxx" is the applet name specified when the user enters the submode.

  Workaround: Do not run the **no event manager applet** *xxx* command in check syntax mode.

- CSCsz16580

  Symptoms: Active RP's 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 , Show command load.

  Workaround: During the Bootup case, workaround is to delay the Standby RP bringup using EEM or other methods untill all the DHCP users address are assigned and SBC Signalling Pinholes are established.

- CSCsz22249

  Symptoms: The following traceback and error message are displayed:

  ```
  %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE) (0x0) 172.24.0.0/16, state
  7, event 0->1, nh_type 1 flags 4 - Process= "RIP Router", ipl= 0, pid= 336 -Traceback=
  407FFAA4 407FFFE8 40D97228 40D981F4 40D99FCC 40D9A110 40D94EF0 40D963A4 41107300
  41107AB4 4110A67C 4110CF04
  ```

  Conditions: This symptom is observed when RIP is configured on a Cisco 10000 series router with PRE4 and is running Cisco IOS Release 12.2(34)SB2. The RIP holddown timer is set to “0”. The GigE or Sonet controller on the Cisco 10000 series router that has RIP enabled is shut down.

  Workaround: There is no workaround.

- CSCsz23951

  Symptoms: NSAP address family cannot be configured.

  Conditions: The symptom is observed with the initial configuration.

  Workaround: There is no workaround.

- CSCsz24554

  Symptoms: The standby router reloads continuously.

  Conditions: In highly scaled environments the Checkpointing Facility may get permanently stuck to FLOW_OFF if the Standby Unit reloads when FLOW_OFF is asserted.

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

  Further Problem Description: Execute the following command at the active router console CLI and determine if the flow control state is set to OFF:

  show checkpoint stat

- CSCsz24818

  Symptoms: Router crashes when trying to initiate a telnet client using an IPv6 address.

  Conditions: The symptom is observed when **ip telnet source interface** is configured to point to an interface that has an IPv6 address configured on it. It does not matter which interface it is: gig0 or any other interface.

  Workaround: Remove the **ip telnet source interface** configuration.

- CSCsz25686

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

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

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

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

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

  Workaround: There is no workaround.

- CSCsz28231

  Symptoms: Unable to attach a policy when a 100% bandwidth is assigned to that policy. The policy configures with bandwidth percent and priority percent. After changing the total percentage to 90% on that policy, it is attached on the interface. If you change that policy to 100%, it is still attached on the same interface.

Conditions: The symptom is observed only when “class-default” is configured with “priority percent”. (It is not seen if “class-default” is configured by “bandwidth percent”.)

Workaround: Configure the priority percent in the class-default so that total percentage is 90%. You can now attach the policy to the target successfully. Change the priority percent in the class-default so that total percentage is back to 100%.

- 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.

- 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.

- CSCsz42939

  Symptoms: IOS crashes when Router has multiple interfaces configured with SPA-4XCT3/DS0/ SPA-2XCT3/DS0 SPA.

  Conditions: Configure multiple channel groups on SPA-4XCT3/DS0 SPA and performing a soft/hard OIR SPA would crash the Router and the Router reloads.

  Workaround: There is no workaround.

- CSCsz47622

  Symptoms: Tracebacks can be seen at default_ip_raw_enqueue function on a Nat box configured for multicasting using Vif interface.

  Conditions: The above symptom is seen on a router loaded with Cisco IOS interim Release 12.4(24.6)T8 ios release.

  Workaround: No workaround.

- CSCsz47914

  Symptoms: Pings from LAN to LNS are not successful after the PPTP session establishment

  Conditions: This is observered while testing when clear vpdn counters tunnel pptp is configured for Cisco IOS interim Release 12.4(24.6)T8.

  Workaround: There is no workaround.

- CSCsz55618

  Symptoms: Memory leak in “SSS Manager” when churning CoA messages to turn off/on a parameterized QoS service.

  Conditions: ASR1000 as PTA terminating PPPoEoQinQ sessions

  Workaround: There is no workaround.

- CSCsz55834

  Symptoms: GLBP may provide BIA MAC instead of Virtual MAC for mobile users.

  Conditions: The symptom is observed when IP Mobility and GLBP are configured.

  Workaround: There is no workaround.

- CSCsz56169

  Symptoms: A software-forced crash occurs after a **show user** command is performed.

  Conditions: The crash occurs after the user performs a **show user** command and then presses the key for next page. It is observed on a Cisco 3845 that is running Cisco IOS Release 12.4(21a).

  Workaround: Do not perform a **show user** command.

- CSCsz56382

  Symptoms: The Tunnel0 interface used on a DMVPN hub is reporting “Tunnel0 is reset, line protocol is down” or no traffic is passing through this interface anymore.

  The IKE and IPSec SAs may still be up, but only the decaps counters will be seen increasing, not the encaps counters.

  Conditions: This symptom is observed on Cisco 2821 routers that are running Cisco IOS Releases 12.4(9)T7 or 12.4(15)T9. Other platforms and releases may be affected.

  Workaround: Shutdown Tunnel0 and create interface Tunnel1 with the same configuration instead, if you cannot reload the router.

  Otherwise reloading the router will resolve the issue. Do not configure another identical Tunnel interface in this case or you will run into CSCsl87438. If you reload the router at a later time, be sure to remove the duplicate Tunnel interface prior to the reboot.

- CSCsz63606

  Symptoms: Ping fails when NAT outside is enabled on UUT.

  Conditions: The symptom is observed only with NAT outside (static, dynamic or overload).

  Workaround: There is no workaround.

- CSCsz63721

  Symptoms: CPU utilization goes to 90% or above when PfR is configured with a large number of policy using fastmode and forced target.

  Conditions: The problem is limited to a large number of forced target (greater than 500) and fastmode with probe frequency of 2-5 seconds. CPU usage progressively gets worse with the increase in number.

Workaround: Use longest-match targets instead of forced targets. Forced targets are configured under oer-map, and longest-match targets are configured under OER master. Forced targets are required only if the target does not belong to the destination subnet of the traffic-class being optimized.

- CSCsz69301

  Symptoms: Some LDP sessions go down after reloading the Router with EoMPLSoGRE Sessions

  Conditions: Issue is seen with ~30 EoMPLSoGRE sessions or above with traffic running. Some of the LDP sessions go down after reloading the Router

  Workaround: There is no workaround.

- CSCsz71654

  Symptoms: Accounting records do not show the correct username.

  Conditions: The symptom is observed when account-logon (authentication) happens after failed Transparent Auto-Logon (TAL).

  Workaround: There is no workaround.

- CSCsz72142

  Symptoms: Memory corruption is hypothetically possible.

  Conditions: The memory corruption might be seen after issuing: **clear ip bgp ... soft** on a BGP session which includes a connector attribute.

  Workaround: There is no workaround.

  Further Problem Description: This problem was found by automated analysis tools, and has not been showing to have any real-world impact.

- CSCsz74362

  Symptoms: The router crashes when you try to attach a service policy with a policer to an interface.

  Conditions: The symptom is observed when the service policy has a policer defined in it and when you try to attach that service policy to an interface.

  Workaround: There is no workaround.

- CSCsz75221

  Symptoms: Crash when cdp is running on the interfaces.

  Conditions: None. This is a rare issue.

  Workaround: Disable cdp using **no cdp run** global configuation command.

- CSCsz77311

  Symptoms: Crash occurs in mfib_db_table_is_downloadable().

  This bug may be seen when the following config command is issued: **no ipv6 multicast-routing**.

  Conditions: This is a platform-independent bug and has been spotted on the Cisco ASR1k and the Cisco CAT6000.

  Workaround: There is no workaround.

- CSCsz78864

  Symptoms: When testing the HTTP PAI ENH feature to check whether PAI can handle the different password scenarios (given below) with and without AAA authentication, the test cases fail and show the error “Authentication to Privilege level 15 failed”.

Conditions: The symptom is observed under the following different password scenarios:

1. EnableBlank_WithAAA: Test to verify that PAI can handle empty password values and use AAA enable password authentication.
2. EnableSecret_WithAAA: Ensure that PAI can handle password encryption and substitution. Use enable password authentication.
3. EnablePass_NoAAA: Verify that PAI can handle password encryption and substitution.
4. EnableSecret_NoAAA: Verify that PAI can handle password encryption and substitution.
5. SpaceEmbedded_Password: Ensure that PAI can handle a space in the password.

Workaround: There is no workaround.

- CSCsz84906

  Symptoms: The ISIS redistribution RIB has a stale route that is not removed after the original ISIS route is deleted when an interface is shut down. This can cause wrong ISIS database information and wrong routing information in the routing table.

  Conditions: This symptom is observed when the router is an L1L2 router and the old ISIS route to be deleted after interface shutdown has a backup route from other routing protocols. If the **ip routing protocol purge interface** command is configured, the issue will not happen.

  Workaround: Either configure the **ip routing protocol purge interface** command or enter the **clear isis *** command, which may resolve the problem temporarily.

- CSCsz88850

  Symptoms: Active RP's CPU% spikes by MLD process/PIM process after reload or switchover or interface state flapping.

  Conditions: This MLD CPU Spike is seen right after the Bootup when Active RP is Synching with Standby RP. The PIM CPU Spike is seen when the interface state is changing. But again this two problem can be seen randomly.

  Workaround: There is no workaround.

- CSCsz89107

  Symptoms: CPU utilization is high when there is a scaled configuration of more than 1000 interfaces and 100-pps traffic is being sent on UUT along with BGP and multicast traffic.

  Conditions: This symptom is observed when several sessions are active and generating traffic.

  Workaround: There is no workaround.

- CSCta04391

  Symptoms: Router with dynamic NAT for unicast and multicast traffic crashes after deleting **ip nat inside source list**.

  Conditions: Router crashes when there is unicast and multicast traffic and only when unicast and multicast traffic uses the same NAT rule.

  Workaround: Use separate NAT rule for unicast and multicast traffic.

- CSCta08194

  Symptoms: The router crashes when running a certain test case that reprovisions an AToM tunnel multiple times.

  Conditions: The crash happens while reprovisioning an AToM tunnel with AAL5 encapsulation.

  Workaround: There is no workaround.

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

- CSCta08772

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

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

  Workaround: There is no workaround.

- CSCta10075

  Symptoms: An incorrect logic in doing increment comparisons for counters, such as interface resets will cause EEM policy to be triggered. That is, if there are any numbers in the interface resets counter and a “clear counters” is performed on the next EEM poll interval the command executes, which is not correct.

  Conditions: This is seen in the latest Cisco IOS Relase 12.4(24)T. Most of the newer Cisco IOS Release 12.4T images are also affected.

  Workaround: There is no workaround.

- CSCta10402

  Symptoms: Continuous packet send by BFD causing CPU hog.

  Conditions: BFD enabled in router.

  Workaround: Disable BFD.

- CSCta10764

  Symptoms: The SBC SIP application is not VRF address aware.

  Conditions: The symptom is observed when using an overlapping local IP address.

  Workaround: Use a non-overlapping local IP address.

- CSCta14505

  Symptoms: For pim sparse mode groups, no s,g would form in the network. This leads to traffic failures.

  Conditions: Pim sm be configured in the network and traffic is being sent for the pim sm groups.

  Workaround: Shut the upstream interface, remove the ip address, configure it again and do a no shut on the interface.

- 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.

- CSCta22221

  Symptoms: Frame relay client triggers reload of standby router.

  Conditions:Occurs if lot of frame relay related configuration is present.

  Workaround: There is no workaround.

- CSCta27331

  Symptoms: HSRP authentication applied to secondary addresses fails, generating the following syslog message:

  %HSRP-4-BADAUTH: Bad authentication from 172.16.123.2, group 2, remote state Active

  Conditions: The symptom is observed with HSRP authentication applied to secondary addresses. (HSRP authentication applied to primary addresses are unaffected.) It is seen with Cisco IOS Release 12.4(24)T and 12.2(33)SXI.

  Workaround: Disable authentication on HSRP groups configured with secondary addresses.

- CSCta30292

  Symptoms: HIGH CPU after MR APS switchover resulting in OSPF link flaps.

  Conditions: Above symptom seen in Cisco routers with IOS image version 12.2(34)SB after APS switchover.

  Workaround: There is no workaround.

- CSCta30439

  Symptoms:G1 and G2 routers may crash.

  Conditions: When MLP is configured on CJ-PA and OIR is done.

  Workaround: There is no workaround.

- CSCta34812

  Symptoms: The offered rate and bandwidth allocated for all the user classes are the same, although different percentages are configured. The output rate failed to guarantee its minimum bandwidth setting.

  Conditions: The data rate for QoS bandwidth is not meeting its minimum requirement.

  Workaround: There is no workaround.

- CSCta36860

  Symptoms: The ISG will have dangling sessions if multiple CoA messages comes in while the ISG is making a CoA request.

  Conditions: This occurs when ISG makes a CoA request but never receives a response. During that time, another CoA message comes in to disconnect the session. The session will never be disconnected.

  Workaround: Clear the sessions manually.

- CSCta37429

  Symptoms:The user configures multi-word string in the client-ID of ANCP neighbor configuration on ATM pvc using quotation marks. But, the quotation marks are not displayed in the client-ID. Hence, the ANCP configuration on the pvc disappears after router reboot.

  Conditions: Configure a multi-word string in the client-ID of ANCP neighbor name.

  Workaround: There is no workaround.

- CSCta37724

  Symptoms: Modified QoS params are not reflected to atm vc in platform.

  Conditions: If interface is shut and any VC QoS param is modified which triggers VC modification.

  Workaround: Do not modify VC params in interface shut mode.

- CSCta41064

  Symptoms: Console hangs with “system accounting” configured.

  Conditions: The symptom is observed when “console login authentication” is configured with “AAA server group (Radius/Tacacs+)” and when the server is not reachable.

  Workaround:

  1. Configure local authentication: either local, line, or enable.
  2. Wait until the system start timeout occurs.

- CSCta53511

  Following are the symptoms of the issue.

  1. ECC Erros

     1.1 %ECC-3-SBE_HARD: Single bit *hard* error detected

     1.2 %ECC-3-SBE_LIMIT: Single bit error detected and corrected

     1.3 %ECC-SP-STDBY-3-SYNDROME_SBE_LIMIT: 8-bit Syndrome for the for the detected Single-bit error. 1.4 %C7600_MEM_ECC-2-MBE: Multiple bit error detected.
  2. Card stuck before ROMMON prompt during re-boot
  3. Crash while copying IOS images through TFTP to bootdisk.
  4. Crashes due to memory corruption
  5. TLB exception: ** Data TLB Error Exception ***

  Conditions: There is no exact trigger but it could be seen with system booting, copying image from disk/tftp to disk, traffic etc.

  Workaround: Upgrade ROMMON to SRD5 for RSP720 and SRD6 ROMMON for RSP720+10G.

- CSCta55561

  Symptoms: Per-vrf dampening is not supported.

  Conditions: This symptom occurs during normal code flow.

  Workaround: There is no workaround.

- CSCta59045

  Symptoms: If a user configures 32K dual stack sessions on a PTA device(Cisco ASR 1000) with another Cisco ASR 1000 as client using the **test pppoe** command, the client crashes with a Cisco IOS crash when 14K sessions come up on the PTA.

  Conditions:Client crashes with **test pppoe** command while trying to bring up 16K dual stack sessions on a PTA device. Both PPPoE client and PTA are Cisco ASR 1000 routers.

  Workaround:There is no workaround.

- CSCta60119

  Symptoms: Prefixes may be unresolved or dropped if “non recursive accounting” is enabled.

  Conditions: The prerequisites for this symptom to occur are:

  1. Non recursive accounting is enabled (that is, **ip cef accounting non-recursive** is present in the configuration).
  2. A recursive prefix (e.g.: BGP learned) is recursing over another prefix which is also recursive.
  3. The second recursive prefix has multiple recursive paths, e.g.: multiple iBGP paths with **maximum-paths ibgp 2**.

4. None of the recursive prefixes are MPLS labeled.

Workaround:

1. Remove **ip cef accounting non-recursive**.
2. Disable iBGP multipath by configuring **maximum-paths ibgp 1**.

- CSCta67945

  Symptoms: SNMP get for a single request ifInOctets or ifOutOctets, one request/second, shows counters increasing.

  SNMP get two OIDs at the same time (ifInOctets and ifOutOctets or sysUptime, ...) shows counters increasing only every 5 seconds.

  Conditions: This symptom is observed on a Cisco 7300 router that is running Cisco IOS Release 12.2(31)SB14.

  Workaround: There is no workaround.

- CSCta69118

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

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

  Workaround: There is no workaround.

- CSCta69720

  Symptoms: RP is observed to reload after 24hrs

  Conditions: When 10k Sessions out of 23k sessions are flapped for 24hrs, RP is observed to reload and switchover is observed.

  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.

- 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.

- CSCta92029

  Symptoms: MSDP SA is not received on an MSDP peer.

  Conditions: The symptom is observed when the first hop router is also the RP.

  Workaround: There is no workaround.

- CSCta93223

  Symptoms:

  1. On configuring an invalid reg expression like the one below under ip extcommunity-list and sh run the router crashes.

2. On configuring an invalid reg expression like the one below and then in the same extcommunity-list configure another reg expression the router crashes immediately.

Conditions: When an invalid reg expression like the one in the enclosures ")(*)(*&*&^*&^&^%&^%".

Workaround: There is no workaround.

- CSCta95359

  Symptoms: The **write memory** command used in parallel on two VTY sessions erases the standby NVRAM.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)SB, when performing parallel **write memory** commands on two different VTY sessions.

  Workaround: Configure “nvbypass”.

- CSCta98565

  Symptoms: IOSD crashes when establishing PPPoE sessions with invalid configurations.

  Conditions: The symptom is observed under the following conditions:

  1. A Cisco ASR 1006 router used as a PPPoE server.
  2. The configuration “sessions per-vlan throttle” is applied to a physical interface.
  3. A PPPoE session is attempted on the interface.

  Workaround: Remove “sessions per-vlan throttle” from the physical interface.

- CSCtb01505

  Symptoms: Router crashes with ospf_build_net_lsa.

  Conditions: While unconfiguring ospf configurations, router crashes.

  Workaround: There is no workaround.

- CSCtb01970

  Symptoms: Sometimes etherchannel member-link “UP” convergence time takes about 1sec.

  Conditions: PAgP is used.

  Workaround: There is no workaround.

- CSCtb05927

  Symptoms: Fragmented L2TP packets may be dropped when switched from an L2TP tunnel. The debug IP error will show the following:

  IP-6-L2MCASTDROP: Layer 2 Multicast packet detected and dropped

  Conditions: The symptom is observed when there is a Gigabitethernet/Ethernet link between PE routers.

  Workaround: There is no workaround.

- CSCtb09281

  Symptoms: High CPU utilization on LFD main process during SSO.

  Conditions: When having nearly 4k of VCs, High CPU utilization on LFD main process during SSO.

  Workaround: There is no workaround.

- CSCtb13015

  Symptoms: Configure a vpn profile(template) cisco-avpair=”template:ip-addr=10.10.10.10 255.255.255.255”.

Bring up a PPPOE seeion from Client to LNS,call comes up and the virtual-access2.1 on the LNS fails to gets the template IP address 10.10.10.10.

Conditions: When running per vrf aaa script on Pi11r version image , configured vpn profile(template) cisco-avpair="template:ip-addr=10.10.10.10 255.255.255.255". has not applied to the virtual-access on the LNS.

Workaround: There is no workaround.

- CSCtb13846

  Symptoms: Configure policy-map to have small bandwidth attach this service-policy onto MFR interface which is in UP state, next shut down the MFR interface and modify the policy to take more bandwidth in the service-policy then standby resets.

  Conditions: Configure policy-map to have small bandwidth attach this service-policy onto MFR interface which is in UP state, next shut down the MFR interface and modify the policy to take more bandwidth in the service-policy then standby resets.

  Workaround: Configure less bandwidth in the service-policy then the crash will not happen.

- CSCtb18207

  Symptoms: A router crashes.

  Conditions: The symptom is observed when configuring IPSec using the VTI and attaching the service policy to the tunnel interface, while enabling the physical interface and where the tunnel source in the tunnel interface is given as IP address of the physical interface. It is observed when the router is loaded with the c7200-adventerprisek9-mz.124-24.6.PI11r image.

  Workaround: Use the physical interface instead of using the VTI for IPSec.

- CSCtb18408

  Symptoms: In Ascend IP Pool Management, the IP address is not allocated from the default pool during IPCP negotiation, if the pool is not defined explicitly for that client.

  Conditions: The symptom is observed after the routers try to establish one PPPoE session, and one local pool is configured on NAS. When the client makes a call the IP address is not allocated from the default local pool on NAS.

  Workaround: Define the pools explicitly and do not let the IP address be negotiated from any local default pool.

- CSCtb36384

  Symptoms: Memory corruption.

  Conditions: The symptom is observed with an unaligned IP packet in an interrupted switch path.

  Workaround: There is no workaround.

- CSCtb36637

  Symptoms: The registering flag gets set on Mroute entry. Register-Stop is not received from the RP.

  Conditions: The symptom is observed when sending the data packets before the RP address interface comes up in RP. It is observed on a Cisco 7200 series router that is running the 12.4(24.6)PI11r image.

  Workaround: There is no workaround.

- CSCtb37673

  Symptoms: Using a break action within a programmatic Embedded Event Manager applet causes the policy to exit.

Conditions: The symptom is observed when a break action is executed within a loop. For example:

```
action 001 foreach line $output "\n"
action 002 if $line eq ""
action 003 break
action 004 end
action 005 puts "Made it here"
```

After the break is executed, the policy aborts. The “Made it here” string is not printed.

Workaround: If possible, use “if ... goto” statements to get out of the loop without calling break. For example:

```
action 001 foreach line $output "\n"
action 002 if $line eq "" goto 004
action 003 end
action 004 puts "Made it here"
```

- CSCtb40985

  Symptoms: The memory occupied by the IP SLAs Sync Pro may gradually increase.

  Conditions: The issue occurs when ICMP path jitter operation is configured on the router with invalid source address. Platform is sup720-3B with 12.2(33)SXI1 image.

  Workaround: Configure the SLA operation with right source address.

- CSCtb41458

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

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

  Workaround: There is no workaround.

- CSCtb46556

  Symptoms: With a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2, the NPE-G2 sometimes crashes when executing the command **clear int range multilink 1 10** and the NPE-G1 gives spurious access for the same command.

  Conditions: The symptoms are observed with a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2 and when 14 multilinks are configured with two members each. Pagents are sending bi-directional traffic.

  Workaround: Do not perform commands across all interfaces using interface range. Perform the commands one-by-one, manually.

- CSCtb51993

  Symptoms: A router crashes upon bringing up PPPoE sessions.

  Conditions: The symptom is observed when AAA proposes a pool name but the pool is not defined on the NAS as well as the radius.

  Workaround: Define the pool on the NAS or as a dynamic pool on the radius.

- CSCtb57180

  Symptoms: Router may crash with a Software forced crash.

  Conditions: Under certain conditions multiple parallel execution of the <cmd>show user</cmd> command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet and SSH.

For more information on restricting traffic to VTYs, please consult:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_configuration_example09186a0080204528.shtml

The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

For devices acting as a terminal server, to apply the access class to reverse telnet ports, the access-list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

- CSCtb65151

  Symptoms: A device might crash with a bus error and the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: The symptom is observed on a device that is running Cisco IOS Release 12.4(24)T1. Other releases may be affected (those running with the Common Classification Engine). The condition seems to be temporary and after a while it goes away.

  Workaround: There is no workaround.

- CSCtb69063

  Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

  config# username <name of 64 characters> priv <0-15> password 0 <password>

  Conditions: The symptom is observed if the user name is exactly 64 characters.

  Workaround: Configure a user name of less than 63 characters.

  Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the "changed by user" field prints unwanted characters.

- CSCtb69796

  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: There is no workaround.

- CSCtb69859

  Symptoms: Router crash with traceback 0x40A0D7E8 0x40A0C870 0x409D4DC4 0x4098E0AC 0x42655B74 0x40E3CE4C 0x40E3D634 0x40E3DAB8 0x40974B78 0x40974B5C.

  Conditions: This symptom occurs while configuring ip dhcp pool TAL_DHCP_vrf_pool.

  Workaround: There is no workaround.

- CSCtb70578

  Symptoms: with L2pt and SPAN configuration in the same router the following error message might be displayed on 7609.

  ```
  %SPANTREE-SP-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on
  GigabitEthernet1/2 VLAN5. *Sep 1 15:56:08.175: %SPANTREE-SP-2-BLOCK_PVID_LOCAL:
  Blocking GigabitEthernet1/2 on MST0. Inconsistent local vlan.
  ```

  Conditions: 1) RSPAN is configured on the 7609 2) STP BPDUs are being tunneled up to the 7609 via L2PT 3) L2PT is configured locally on the 7609

  With these three conditions present in the network then it is possible to see the problem.

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

  ```
  mac access-list extended block_l2tp_dmac
  deny any host 0100.0ccd.cdd0 Ðß L2PT destination mac
  permit any any
  vlan access-map block_l2tp 10
  match mac address block_l2tp_dmac
  action forward
  vlan filter block_l2tp vlan-list 5 Ðß insert rspan vlan. In this case it is 5
  ```

- CSCtb70584

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

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

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

- CSCtb71610

  Symptoms: When the router boots up, traffic won't flow for some of the EoMPLS VCs.

  Conditions: When the router has more than 400 SCEoMPLS VC.

  Workaround: Shutting and unshutting the core facing interface is the workaround for this issue.

- CSCtb73967

  Symptoms: Using the command **default dest-ipaddr** for udp-echo, udp-jitter, and tcp-connect causes a device to crash.

  Conditions: The symptom is observed with the command **default dest-ipaddr**.

  Workaround: Do not use the command **default dest-ipaddr**. This sets the address to 0.0.0.0, which is not valid.

- CSCtb75294

  Symptoms: A router crashes upon bringing up PPP sessions.

  Conditions: The symptom is observed if IP pools are configured.

  Workaround: There is no workaround.

- CSCtb83353

  Symptoms: After a RP switchover, the new active RP logs traceback many times, and all sessions/tunnels are torn down.

Conditions: LNS is configured with 16000 sessions/8000 tunnels (2 sessions per tunel), all sessions with Model D2 QoS. After a RP switchover, the new active RP logs traceback many times, and all sessions/tunnels are torn down.

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.

- CSCtc00593

  Symptoms: A C10K is experiencing nested crashes due to a corrupted program counter.

  Conditions: This is seen on a C10K running 12.2(33)SB7 during normal operation.

  Workaround: There is no workaround.

- CSCtc23374

  Symptoms: The router produces the message: %SYS-6-STACKLOW: Stack for process BGP Router running low, 0/9000 and reloads

  Conditions: The message and reload are seen only when: 1. BGP is configured 2. BGP has learned about multiple networks 3. The command **clear ip bgp** is issued. It is best-documented with the command **clear ip bgp * soft** but could potentially be generated in response to more limited clear commands, or in response to the removal of BGP-related configuration.

  This problem is only seen in images where CSCsz72142 is integrated.

  Workaround: There is no workaround.

- CSCtc24864

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

  Conditions: This symptoms is observed on a L2 QnQ tunnel port. By default on L2 QnQ tunnel port, cdp is disabled. However cdp can enabled on QnQ port through cli command. After enabling the CDP on a QnQ port, a subsequent link down and link up (shut and no shut) of this QnQ port, results in disabling the CDP which is the default behavior.

  Workaround: The work around to this problem is to configure the CDP (CDP enable)again after link up.

- CSCtc39894

  Symptoms: ES+ Linecard crashes on removing the channel-group configuration from the member-link which is in shut state.

  Conditions: Customer would see this issue whenever the one of the member-link is down and the configurations are changed.

  Workaround: Do "no shut" on the member-link before removing the channel-group configuation.

- CSCtc61025

  Symptoms: For VPLS Autodiscovered pseudowires using FEC129, the label release message is not understood by peer in Inter-Op tests with Alcatel-Lucent. This is because Cisco box is sending label release message in the format <AGI,LAII,RAII> whereas it should be <AGI,RAII,LAII>.

  Conditions: Delete the VFI or shut the attachment circuit to cause the label withdraw message to sent and correspondingly the peer will send label release message.

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

- CSCuk44399

  Symptoms: IP Header Compression (IPHC) may not function for IP multicast packets.

  Conditions: This symptom is observed when IPHC is enabled for IP multicast routing.

  Workaround: There is no workaround.

- CSCum47620

  Symptom: SRE PIM routers running the SRE code do not start the PIM register process for multicast traffic coming from indirectly connected sources. This can affect customers who upgraded to SRE from SRD as some services may stop working due to this change.

  Conditions: This symptom occurs in SRE + PIM SM with multicast coming from indirectly connected neighbors.

  Workaround: Use "ip pim dense-mode proxy-register".