Caveats

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

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

This section consists of the following subsections:

Resolved Caveats—Cisco IOS Release 15.0(1)M10

Cisco IOS Release 15.0(1)M10 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M10 but may be open in previous Cisco IOS releases.

- CSCeb27716

  Symptoms: Spurious memory access at vp_fastsend() may be seen in a Cisco 5800 access server under stress. This may not be service affecting.

  Conditions: This is seen during a stress test of 12 hours with bi-directional traffic setup.

  Workaround: There is no workaround.

- 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.

- CSCtc87162

  Symptoms: Incorrect ceAssetMfgAssyNumber and ceAssetMfgAssyRevision in a Cisco 3900 series router.

  Conditions: The symptom is observed with a Cisco 3900 series router.

  Workaround: There is no workaround.

  Further Problem Description:

  IFR: 3925

```
ceAssetOrderablePartNumber.1 = CISCO3925-CHASSIS
ceAssetOrderablePartNumber.3 = C3900-SPE200/K9
ceAssetOrderablePartNumber.11 = SM-NM-ADPTR <<<<<<<< There is no entry for
"SM-NM-ADPTR" in <CmdBold>show diag<noCmdBold> output. The SM adapter is in
slot 1. but, <CmdBold>show diag<noCmdBold> does not have information about slot 1.

ceAssetMfgAssyNumber.1 = 800-33414-01 <<<<<<< As per <CmdBold>show
diag<noCmdBold> output, the Assy Number for CISCO3925-CHASSIS is 800-31577-01
ceAssetMfgAssyNumber.3 = 800-33414-01
ceAssetMfgAssyNumber.11 = 800-30005-01
```

  IFR: 3945

```
ceAssetOrderablePartNumber.1 = CISCO3945-CHASSIS
ceAssetOrderablePartNumber.3 = C3900-SPE250/K9
ceAssetOrderablePartNumber.11 = SM-NM ADPTR
ceAssetOrderablePartNumber.14 = SM-NM-ADPTR  <<<<<<<<<< Only the SM adapter
which contains the cards are populated in <CmdBold>show diag<noCmdBold> with
adapter and card details. The adapters which doesn't have any cards are not
```

```
displayed in <CmdBold>show diag<noCmdBold>. But, the <CmdBold>show
diag<noCmdBold> has entry for all.

ceAssetOrderablePartNumber.16 = NM-1T3/E3=
ceAssetOrderablePartNumber.19 = SM-NM-ADPTR

ceAssetMfgAssyNumber.1 = 800-33013-01 <<<<<<< As per <CmdBold>show
diag<noCmdBold> output, the Assy Number for CISCO3945-CHASSIS is 800-31577-01
ceAssetMfgAssyNumber.3 = 800-33013-01
ceAssetMfgAssyNumber.11 = 800-30005-01
ceAssetMfgAssyNumber.14 = 800-30005-01
ceAssetMfgAssyNumber.16 = 800-19180-02
ceAssetMfgAssyNumber.19 = 800-30005-01

ceAssetMfgAssyRevision.1 = 08 <<<<< Should be A0
ceAssetMfgAssyRevision.3 = 08
ceAssetMfgAssyRevision.11 = 06  <<<<<<<<<<< Board revision is displayed for
SM-NM-Adapter, but <CmdBold>show diag<noCmdBold> does not have slot 1 information.
ceAssetMfgAssyRevision.14 =
ceAssetMfgAssyRevision.16 = A0
ceAssetMfgAssyRevision.19 =
```

- CSCtl99174

  Cisco IOS Software contains a memory leak vulnerability that could be triggered through the processing of malformed Session Initiation Protocol (SIP) messages. Exploitation of this vulnerability could cause an interruption of services. Only devices that are configured for SIP inspection are affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that must run SIP inspection.

  This advisory is available at the following link:

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

- CSCto60258

  Symptoms: Voice call may fail with MGCP controlled FXS port.

  Conditions: Adding both commands **mgcp default-package fxr-package** and **mgcp fax t38 inhibit** under MGCP may cause voice call to fail.

  Workaround: Disable one of the commands under MGCP configuration.

- CSCtz35999

  The Cisco IOS Software Protocol Translation (PT) feature contains a vulnerability 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 available.

  This advisory is available at the following link:

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

  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

Resolved Caveats—Cisco IOS Release 15.0(1)M9

Cisco IOS Release 15.0(1)M9 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M9 but may be open in previous Cisco IOS releases.

- CSCtf49537

  Symptoms: During the bulk-sync, Standby does not reload when a configuration command with parser return code error is seen on Standby. The user will not notice if a PRC error occurred.

  Conditions: This symptom is observed when the PRC error result status is not sent back from Standby to Active properly.

  Workaround: After the system reaches the SSO state, issue the following exec command via the Active console to check if PRC error occurred.

  ```
  router# show redundancy config-sync failures prc
  ```

- CSCtg59328

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCth20872

  Symptoms: The following error message is seen accompanied by a reset of the Fast Ethernet:

  ```
  %C870_FE-3-TXERR: FastEthernet0: Fatal transmit error. Restarting...
  ```

  Conditions: The symptom is observed on a Cisco 877 router that is running Cisco IOS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCti41891

  Symptoms: When 812 tunnels are configured, Standby starts rebooting.

  Conditions: This symptom is observed with scalability.

  Workaround: There is no workaround.

- CSCtj48387

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

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

  Workaround: There is no workaround.

- CSCtj59117

  Symptoms: The following error message is seen and the router freezes and crashes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```
  A reload is required to recover.

  Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.

  Workaround: Remove CEF.

- 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.

- CSCtq91063

  Symptoms: A Cisco router may unexpectedly reload due to bus error or generate a spurious access.

  Conditions: The issue occurs due to the F/S particle pool running out of free particles and the next packet failing to successfully obtain a particle. The F/S pool is used for fragmentation, so this will only occur when there is a large amount of fragmentation occurring. It has only been seen when there is a “ip mtu 1500” configured on a tunnel interface where the physical mtu is 1500 forcing packets to be fragmented on the physical interface rather than on the tunnel interface.

  Workarounds:

  1. Remove “ip mtu 1500” from the tunnel interface; or
  2. Configure “service disable-ip-fast-frag”; or
  3. Reduce hold queue sizes such that the total size of the queues for all active interfaces in the system does not exceed 512.

- CSCtq92650

  Symptoms: DMVPN tunnel is not selecting the right source interface.

Conditions: The symptom is observed when multi-link frame relay creates more than one sub-interface with the same name.

Workaround: There is no workaround.

Further Problem Description: This bug resolves the issue reported in CSCth08338 for Cisco IOS Release 15.1M.

- CSCtr26373

  Symptoms: Interface bounces and, after coming back up, hangs and does not pass traffic. The rx ring is stuck and it may be observed that all packets coming into the interface are counted as “input errors”.

  Conditions: This has been observed on onboard GE interfaces of Cisco 39xx and Cisco 2951 routers. It may be seen at random times and has thus far been observed to happen after an interface bounce. The interface will still show “up/up” in the **show interface** output.

  Workaround: Bounce the interface again to restore service.

- CSCtr86328

  Symptoms: A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.

  Conditions: Cisco IOS device configured for clientless SSL VPN.

  Workaround: There is no workaround.

  Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

  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 6.8/6.5:

  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:U/RC:C

  CVE ID CVE-2012-1344 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

- CSCtr87070

  Symptoms: Enable login failed with error “% Error in authentication”.

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCtt23358

  Symptoms: RP reset @ __be_tunnel_protection_remove_idb_for_connection in flexVPN scale setup.

  Conditions: The symptom is observed with a shut/no shut on a flex tunnel and then executing the command **clear crypto session**.

  Workaround: There is no workaround.

- CSCtt94391

  Symptoms: A Cisco wireless router may unexpectedly reboot due to a bus error with the following error leading up to the crash:

```
ASSERTION FAILED: file ''../dot11t/t_if_dot11_hal_ath.c'', line XXXX
```

Conditions: This issue relates to the wireless on the router. This crash can be seen on the following platforms: Cisco 870W, 1800W, UC500W, and 2800 and 3800 routers with HWIC-AP. The crash is only seen when an iPhone 4S is connected to the router. The crash has most commonly been triggered by running a video call application on the phone, but there may be other triggers. Other than the wireless configuration and other generic configurations needed to provide connectivity to the router, no other specific configuration is needed to see the crash.

Workaround: No workaround on the router. However, this issue is not seen with an iPhone 4s running iOS 5.1. The issue is only seen on iOS 5.0.

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 6.1/5.8:

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

CVE ID CVE-2012-1327 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

- CSCtu16433

  Symptoms: A Cisco router may reload due to a bus error. It appears to reload just after registration:

  ```
  %GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for group <snip> using
  address <snip>
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = <snip>
  ```

  Conditions: The symptom is observed using GET VPN on Cisco IOS Release 12.4T, 15.0, or 15.1. 15.2 is not affected.

  Workaround: There is no workaround.

- CSCtw45480

  Symptoms: Inbound GRE encapsulated traffic is dropped with the "Unknown-l4 sessions drop log" message on the router with ZBFW.

  Conditions: This symptom is observed when router self zone policies are applied and the GRE tunnel is in an intermediate zone between the inside and outside zones.

  Workaround: Remove the self zone policies.

- CSCtw55976

  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.

  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-20120926-ios-ips

- CSCtw84664

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

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

This advisory is available at the following link:

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

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK but no traffic is going out over the tunnel.

  Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

  For example, the IVRF routing table should show:

  ```
  S 10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```
  but instead it shows:

  ```
  S 10.0.0.0 [1/0] via 192.168.0.1
  ```
  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

  Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

  Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

  Workaround: Configure a static route to the remote network. For example:

  ```
  ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
  ```
  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtx14000

  Symptoms: Router crashes while clearing VTY lines that are idle.

  Conditions: The symptom is observed when clearing the VTY lines that are idle and do not time out.

  Workaround: There is no workaround.

- CSCtx66804

  Symptoms: The configuration “ppp lcp delay 0” does not work and a router does not initiate CONFREQ.

  Conditions: The symptom is observed with the following conditions:

  - “ppp lcp delay 0” is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.

  Workaround: Set delay timer without 0.

- CSCtx72953

  Symptoms: During normal operation, traffic is lost on the HWIC-4ESW and some VLAN information is missing. In the logs you see:

  ```
  esw_mrvl_vlan_port_remove : Unable to find entry for VLAN(xxx) dbnum(xxx)
  ```
  and/or:

```
esw_mrvl_vlan_port_untagged : Unable to find entry for VLAN(1)
```
Conditions: The symptom is observed with Cisco IOS Release 15.1(4)M3.

Workaround: Delete/recreate lost VLAN (except VLAN 1).

- CSCtx86674

  Symptoms: ATM VPI/VCI does not come up after upgrading to Cisco IOS Release 15.1(4)M4.

  Conditions: This symptom is observed when upgrading to Cisco IOS Release 15.1(4)M4, which was an engineering build given for addressing CSCtx09973.

  Workaround: ATM port shut/no shut resolves the issue. However, it refers to about 5000+ nodes here or "config dsl-group 0 pairs 0" instead of dsl-group auto under controller SHDSL.

- CSCtx92802

  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

  Conditions: The symptom is observed under the following conditions:

  – Cisco IOS Release 15.0(1)M7 on a Cisco 1841.

  – VRF enabled.

  – CEF enabled.

  – VPN tunnel.

  Workaround: Disable VFR or CEF.

- CSCty04692

  Symptoms: Intermittently, calls placed to a Cisco Meetingplace server would provide the re-order tone to the caller. This symptom may not be restricted to the Meetingplace application server alone.

  Conditions: The call needs to engage/disengage/engage the IOS XCODER (HW transcoder) in quick succession due to a mismatched codec.

  Workaround: There is no workaround.

  Further Problem Description: Running Cisco IOS debug command **debug voip xcodemsp error** and **debug voip xcodemsp error** will print an error message like the following:

  ```
  sym_xapp_calleg_setup_req: MSPSPI setup request failed for sess
  ```
- CSCty14375

  Symptoms: There is a false temperature alarm on a Cisco 2911 in a production environment:

  ```
  %ENVMON-1-WARN_HDD_HIGH_TEMP: Critical Warning: sensor temperature (65535 C) exceeds
  40 C. System is experiencing excessive ambient temperatures and/or airflow blockage.
  SM-SRE-700-K9 hard disk drive may become unusable if continuously operated at this
  temperature. Please resolve system cooling to prevent system damage.
  ```
  Conditions: This has been seen on a Cisco 2900 router that is running Cisco IOS Release 15.1(4)M, when air intake temperature goes below 0C.

  Workaround: There is no workaround.

- CSCty33945

  Symptoms: When a SIP gateway tears down video and later sets it up again after a midcall invite for the same call, it reuses the same source RTP port as before. Unfortunately, it does not check if this RTP port is in use for a different call, and therefore crosstalk can occur.

  ```
  4310820: Feb 27 17:56:08.910: //3017060/BF76175BB294/SIP/Media/sipSPIAddStream:
  Reusing old src_port(16384)
  ```
  Conditions: This symptom is observed when a SIP gateway tears down video and later sets it up again after a midcall invite for the same call.

Workaround: There is no workaround.

- 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.

- CSCty35840

  Symptoms: Distinctive ring feature is not working with SIP phones in SRST mode. Currently the following Alert-Info is sent to SIP phones for an external call:

  ```
  Alert-Info: bellcore-dr2
  ```
  The alert-parameters should be bracketed by < and >.

  Conditions: The symptom is observed with SIP phones in SRST mode.

  Workaround: There is no workaround.

- CSCty42626

  Symptoms: Certificate enrollment fails for some of the Cisco routers due to digital signature failure.

  Conditions: This symptom was initially observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  This issue potentially impacts those platforms with HW crypto engine. Affected platforms include (this is not a complete/exhaustive list)

  - c3925E, c3945E
  - c2951, c3925, c3945
  - c7200/VAM2+/VSA,
  - possibly VPNSPA on c7600/cat6K
  - 819H
  - ISR G2 routers with ISM IPSec VPN accelerator

  Workaround: There is no workaround.

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3 (SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty80074

  Symptoms: A Cisco 3800 router running Cisco IOS Release 15.0(1)M7, with only Multilink or Serials, shows aborts and input errors during normal traffic conditions.

  Conditions: This symptom is observed with normal traffic load. In addition, when a ping sweep is done, aborts and input errors are seen more frequently.

  Workaround: There is no workaround.

- CSCtz19769

  Symptoms: Failure to verify addition/deletion and modification of bookmark using personal bookmark add/delete/edit icon.

  Conditions: The name should show under “User Defined bookmarks” in portal page and clicking that should open the link in a new browser.

  Workaround:

  1. Log in to the WebVPN gateway portal page.
  2. Click the personal bookmark add icon.
  3. Complete the “name” and “URL” for bookmarking in the “Add Bookmark” page.
  4. Verify the name/URL is bookmarked.

- CSCtz27137

  Symptoms: An upgrade to the S639 or later signature package may cause a Cisco IOS router to crash.

  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T

  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.
  - TFTP a modified configuration to the router’s running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the **write memory** command and reload.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.

1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.

Dialing directly to a number with no extension or extra digits works as expected.

Workaround: There is no workaround.

- CSCtz48615

  Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

  Conditions: The symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

  Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz72044

  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

- CSCua15003

  Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

  Conditions: The problem can happen in the following situation:

  – CUBE receives 180 ringing with SDP session.
  – “media transcoder high-density” is enabled.

  Workaround: Disable “media transcoder high-density”.

- CSCub13317

  Symptoms: Cisco 2900 with VWIC2-2MFT-T1/E1 in TDM/HDLC mode doesn’t forward any traffic across the serial interface after certain amount of time.

  Conditions: Configure frame relay over VWIC2 channel-group in TDM/HDLC mode.

  Workaround: Configure VWIC2 channel-group in NMSI mode.

  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 4.3/3.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C CVE ID CVE-2012-3918 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

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

Resolved Caveats—Cisco IOS Release 15.0(1)M8

Cisco IOS Release 15.0(1)M8 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M8 but may be open in previous Cisco IOS releases.

- CSCsk94026

  Symptoms: AuthProxy sessions on a Cisco 871 router can be deleted immediately after completing the authentication.

  Conditions: This issue is seen only on a Cisco 871 router. It occurs with a basic AuthProxy configuration on a BVI interface.

  Workaround: There is no workaround.

- 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 symptom is observed on a Cisco 3750 router running Cisco IOS Release 12.2(46)SE, as well as on Cisco 4500 and Cisco 4900M routers 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 minutes) 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, reload the switch.

  Further Problem Description: On the Cisco 3570 router, 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.

- CSCtb55479

  Symptoms: A router may crash by the “BGP Router” process.

  Conditions: This symptom is observed if the memory is corrupted.

  Workaround: There is no workaround.

- CSCtb55851

  Symptoms: The router crashes pointing to RF code.

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

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

- CSCtc73441

  Symptoms: A CPUHOG message is observed on the key server (KS) when the **show crypto gdoi ks members** command is executed. As a result of the CPUHOG, the BGP session goes down between the KS and the iBGP neighbor.

  Conditions: The symptom is observed on primary or secondary key servers that have more than 1000 group members.

  Workaround: There is no workaround.

- CSCtd63242

  Symptoms: A traceback or a crash may be seen while deleting a subinterface that has ipv6 EIGRP configured on it.

  Conditions: This symptom is observed on the subinterface when the following commands are configured on it successively:

  3. **ipv6 eigrp** *as*
  4. **no interface** *subinterface*

  Workaround: Remove EIGRP from the subinterface using the **no ipv6 eigrp** *AS* command before deleting the subinterface.

- CSCtd93883

  Symptoms: In a redundant implementation, a few processes in RF running even after a crash leads to a Cisco router reloading with lower IP.

  Processes like “rf_interdev_delay_timer”, “rf_interdev_sctp” need to set their crashblock (Process_set_Crashblock) to TRUE. If the crashblock is not set, then the processes will continue to run even after crashing. This will lead to a reload during the “watchdog timeout” process.

  Conditions: This symptom is observed as a result of the root cause analysis of CSCsy84312.

  Workaround: Ensure that the above processes do not run if the system crashes. However, if the system crashes even before these processes are executed once, schedule the processes in exception path as their crashblock needs to be set.

- 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.

- CSCte61096

  Symptoms: Traceback is seen on the loading image.

  Conditions: This symptom is observed while loading Cisco IOS Release 15.1(0.25) T.

  Workaround: There is no workaround.

- CSCte62190

  Symptoms: A router crashes when the RSA key is generated with redundancy option and then the RSA key pair is deleted using the **crypto pki zeroise** command. All other possible triggers are not known at this time.

Conditions: Device running IOS and crypto.

Workaround: There is no workaround.

- CSCtf71673

  Symptoms: A Cisco router shows a PRE crash.

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

  Workaround: There is no workaround.

- CSCtg06045

  Symptoms: A Cisco router may reload with traceback from a crypto ACL configuration.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(15)T12 and experiencing a high CPU stress load while the ACEs are being changed periodically. This symptom is specific to the ACE entries in crypto ACL downloaded from KS.

  Workaround: Simplify and consolidate the ACE entries in the crypto ACL. In addition, reducing the CPU stress level may help.

- CSCth36114

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

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

  Workaround: Use Cisco IOS 12.4 versions.

- CSCth64271

  Symptoms: Routers in redundant configuration end up in “Manual Swact = disabled”.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCth80642

  Symptoms: IOS SSLVPN fails to accept a new SSL connection. This causes the sessions to get stuck in Time Wait until the TCP queue is full.

  Conditions: This symptom is observed with SSLVPN on Cisco IOS software.

  Workaround: Use the **clear tcp tcb** command to clear the Time Wait sessions.

- CSCti46171

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtj21237

  Symptoms: The following error message is received:

  ```
  %SYS-2-LINKED: Bad enqueue, Bad dequeue
  ```

  This might result an in unexpected reboot due to SegV Exception.

  Conditions: The symptom is observed on a router configured with “control plane policing and protection” feature.

  Workaround: Disable the feature in order to prevent any further crash.

- CSCtj33003

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause an affected device to reload. Affected devices must be configured to process SIP messages and for pass-through of Session Description Protocol (SDP) for this vulnerability to be exploitable.

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

  This advisory is available at the following link:

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

- CSCtj79476

  Symptoms: Traffic loss and VLAN related errors seen when the traffic is sent for a prolonged duration on an HWIC-4ESW.

  Conditions: The symptom is observed when traffic is sent for a prolonged duration (more than 12hrs) on an HWIC-4ESW.

  Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a Voice Gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a Voice Gateway.

  Workaround: There is no workaround.

- CSCtk37395

  Symptoms: A Cisco 2921 router cannot process fax calls and reports the following error message:

  ```
  %MSPI-1-NOMEMORY: Unit 770, no memory for mspi_on_xmit, disconnect connection
  ```

  Conditions: This symptom may be observed when the free memory of the processor is more than 4 GB/6.

  Workaround: Check to see if the free memory of the processor is causing this issue by executing the following commands. These commands will help reduce the processor memory and then increase the input-output memory.

  1. On systems with more than 1GB processor memory, use the **memory- size iomem 25** command to increase the input-output memory.
  2. On systems with less than 1GB processor memory, input-output memory cannot exceed 10% of the processor memory. In this case, use the logging buffer of 200MB to decrease the free processor memory.

- CSCtk65429

  Symptoms: In an encrypted CE-PE session, traffic sourced by the VRF (for example, ping) works, but traffic coming from MPLS does not reach the crypto map.

  The PE CE IKE and IPsec SA will go up if initiated from CE side and traffic will go through the tunnel unidirectionally (from CE to PE).

  Conditions: This issue is observed in new CEF code images, like Cisco IOS Release 12.4(22)T2, Cisco IOS Release 12.4(24)T4, and Cisco IOS Release 15.1(3)T. This issue is not observed in Cisco IOS 12.4 mainline releases, such as Cisco IOS Release 12.4(25d).

  Workaround: There is no workaround.

- CSCtn04277

  Symptoms: Time-based WRED does not work.

  Conditions: The symptom is observed when time-based WRED is used in Cisco IOS Release 15.1(3)T.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtn68643

  Symptoms: OSPFv3 hellos are not processed and neighbors fail to form.

  Conditions: This symptom occurs when configuring OSPFv3 IPsec authentication or encryption.

  ```
  ipv6 ospf encryption ipsec spi 500 esp null sha1
  1234123412341234123412341234123412341234
  ```

  or

  ```
  ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd
  ```

  Workaround: There is no workaround.

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

  Conditions: This symptom is observed when IPIP gateways are involved.

  Workaround: There is no workaround.

- CSCto08135

  Symptoms: When a deny statement is added as the first ACL, the message gets dropped.

  Conditions: An ACL with deny as the first entry causes traffic to get encrypted and denied.

  Workaround: Turn off the VSA, and go back to software encryption.

- CSCto10485

  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the "%CRYPUO-4-PKT-REPLAY" drops as shown in the syslog.

  Conditions: This issue typically occurs during high traffic load conditions.

  Workaround: There is no workaround.

- CSCto32044

  Symptoms: The interface hangs and fails to pass traffic. It will still show an "up/up" status but the input and output rates will go to 0. The following errors will be seen:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000040000000000
  %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset
  ```

  The interface number will vary.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCto60047

  Symptoms: A crash occurs either due to a chunk corruption or at "ssh_send_queue_data".

  Conditions: This symptom occurs under the following conditions:

  - An SSH session exists between two routers.
  - The **show tech** command is issued and then aborted.

  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.

- CSCto88178

  Symptoms: Packet corruption is observed when NAT processes an H.323 packet that has some trailing data beyond the User-User Information Element.

  Conditions: This symptom occurs when NAT is configured to process H.323 packets, and it encounters an H.323 packet that has some trailing data beyond the User-User Information Element.

  Workaround: Although it is not feasible for most implementations, using the **no ip nat service H225** command prevents the packet corruption. Additionally, this issue is not present in those releases that have NAT TCP ALG support enabled.

- CSCto89536

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtq36153

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtq45553

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- 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, (that is, before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However 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 packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- CSCtq63625

  Symptoms: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4 is not getting trained with some DSLAMs without “line rate” configured manually. It gets trained with a manual line rate configured.

  Conditions: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.

  Workaround: There is no workaround.

- CSCtq63838

  Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP",
ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz
0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch) exception, CPU signal 10,
PC = 0x2581FB94
```

  Conditions: This symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCtq76005

  Symptoms: Configuring the **atm route-bridge** *ip* command on an MPLS-enabled ATM interface makes router punt all incoming MPLS packets to CPU.

  Conditions: The symptom is observed when RBE is configured on an MPLS-enabled ATM interface.

  Workaround: Remove RBE.

- CSCtq92940

  Symptoms: An active FTP transfer that is initiated from a Cisco IOS device as a client may hang.

Conditions: This symptom may be seen when an active FTP connection is used (that is, the **no ip ftp passive** command is present in the configuration) and there is a device configuration or communication issues between the Cisco IOS device and the FTP server, which allow control connections to work as expected, but stopping the data connection from reaching the client.

Workaround: Use passive FTP (default) by configuring the **ip ftp passive** command.

Further Problem Description: Please see the original bug (CSCtl19967) for more information.

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

  Conditions: No special configuration is needed.

  Workaround: There is no workaround.

  Further Problem Description: At bootup, when the **show memory debug leaks** command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr11620

  Symptoms: In a simple HSRP setup with Cisco 2900 devices, a ping to the virtual IP address fails intermittently.

  Conditions: This symptom is observed when a Cisco 2911 is used.

  Workaround: Replace the Cisco 2900 with a Cisco 18XX or Cisco 1941.

- CSCtr14763

  Symptoms: A BFD session is always up, although the link protocol is down.

  Conditions: First the BFD session is up between the routers. After the VLAN is changed on the switch between the routers, the BFD peer is not reachable but the BFD sessions are always up.

  Workaround: There is no workaround.

- CSCtr19078

  Symptoms: An IO memory leak in a Cisco router occurs with the following error message:

  ```
  SYS-2-MALLOCFAIL: Memory allocation of x bytes failed
  Pool: IO  Alternate Pool: None  Free: 0  Cause: No Alternate Pool
  ```

  Conditions: This symptom is observed in a Cisco 3270 router with QoS enabled.

  When IPSEC encryption is configured on an SVI (3270 FESMIC Port) using the QoS pre-classify option, the router's memory is quickly exhausted. This happens because traffic routed out of this interface is encrypted but when the same traffic with pre-classify enabled is directed through the native Layer 3 port (MARC card ports), the Cisco 3270 router works fine.

  Workaround: Disable QoS pre-classify using the **no qos pre-classify** command.

- CSCtr28857

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

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

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

- CSCtr29338

  Symptoms: A router crashes with the error message "%ISDN-6-DISCONNECT".

  Conditions: The symptom is observed after an "%ISDN-6-DISCONNECT" message from "unknown" followed by a couple of Illegal Access to Low Address" messages.

  Workaround: There is no workaround.

- CSCtr46123

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

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

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

- 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 using the **interface x/y ipv6 enable** command.

  Workaround 2: Reconfigure the IPv6 address on the subinterface using the **interface x/y.z no ipv6 address ipv6 address ...** command.

- CSCtr54327

  Symptoms: A Cisco router may crash due to a SegV exception or may have spurious access when a fax comes in.

  Conditions: This symptom is observed on a voice gateway that is configured with transcoding and fax passthrough. When a fax call comes in for a codec, but is not configured for a codec, then the "a=silenceSupp:off" option is set in SDP.

  Workaround: Disable fax by going into the "voice service voip" mode and configuring the **fax protocol none** command.

- 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.

- CSCtr72685

  Symptoms: Keyserver is sending rekey for all groups after a change.

  Conditions: Keyserver is configured for multiple GDOI groups. A change is made (e.g. ACL, sa receive only) triggering a rekey. The rekey is being sent to all the groups instead of the impacted one(s). This was observed on Cisco IOS Release 12.4(24)T, Cisco IOS Release 15.0M, and Cisco IOS Release 15.1M.

  Workaround: There is no workaround.

- CSCtr86077

  Symptoms: MGCP call drops 10 seconds after IP phone puts call on hold.

  Conditions: The symptom is observed under the following conditions:

  - IP phone -- CUCM -- MGCP -- GW -- PRI.
  - “mgcp rtp unreachable timeout 10000” is configured on gateway.
  - “no MOH” is configured for the IP phone so Tone on Hold (TOH) is used.
  - IP phone make calls to PSTN and is answered.
  - IP phone puts call on hold.
  - PSTN user hears TOH.
  - 10 seconds after hold is initiated, call is dropped.

  Workaround: Remove “mgcp rtp unreachable timeout” from the MGCP gateway.

- CSCtr86437

  Symptoms: NAT-PT function does not work properly after an interface flap occurs.

  Conditions: The symptom is observed when you configure NAT-PT on the router.

  Workaround: Reconfigure “ipv6 nat prefix”.

- 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

- CSCtr97640

  Symptoms: Start-up configuration could still be retrieved bypassing the “no service password-recovery” feature.

  Conditions: None.

  Workaround: There is no workaround. Physically securing the router is important.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.9/1.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2011-3289 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

- CSCts18257

  Symptoms: MGCP modem pass-through call is failing.

  Conditions: The issue is observed on a Cisco AS5400 router running Cisco IOS Release 15.1(4)M.

Workaround: Use Cisco IOS Release 15.0(1)M6, if possible.

- CSCts24348

  Symptoms: The PBR “set vrf” feature can cause unnecessary ARP requests and packet drops if some other feature is configured on the same router interface and packets are punted to process-switching path. This issue slows down TCP traffic considerably as first SYN in a flow may always be dropped.

  Conditions: The symptom is observed with multi-VRF selection using the Policy Based Routing (PBR) feature. It was observed in all Cisco IOS versions with the new CEF code (Cisco IOS Release 12.4(20)T and later). The issue was not seen in Cisco IOS Release 12.4(15)T and Cisco IOS Release 12.4(25).

  Workaround: This issue can be alleviated by using proxy ARP on the upstream device. Otherwise, there is no workaround.

- CSCts33952

  Symptoms: An **rsh** command fails from within TclScript. When **rsh** command constructs are used within TclScript, bad permissions are returned and the rsh aspect fails to execute, causing the script to fail.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(15)T14 and later.

  Workaround: There is no workaround.

- 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

- 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.

- CSCts76410

  Symptoms: Tunnel interface with IPSec protection remains up/down even though there are active IPSec SAs.

  Conditions: The symptom is observed during a rekey when the IPSec lifetime is high and the control packets do not reach the peer. The issue was observed on Cisco IOS Release 12.4(20)T and Cisco IOS Release 15.0(1)M7.

  Workaround: Shut/no shut the tunnel if the situation occurs. You can use EEM to recover automatically.

- CSCts78348

  Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.

  Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.

  This issue may be seen on Cisco 1900 series routers and Cisco 2900 series routers (except Cisco 2951) This issue may occur when manual set duplex on the affected platform.

  Workaround 1: Perform a **shut/no shut** command on the interface and this issue will recover.

Workaround 2: Use auto negotiation.

- CSCts80643

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this 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-rsvp

- CSCts86510

  Symptoms: Unable to build dIOU images.

  Conditions: This symptom is observed while compiling unused dIOU images.

  Workaround: There is no workaround.

- 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.

- CSCtt07878

  Symptoms: A Cisco 7206 router running IPSec sees this message in syslog output:

  ```
  WARNING: start sending an incomplete HAPI bundle with errors
  ```

  Conditions: The symptom is observed with a Cisco 7206 router that is running IPSec with Cisco IOS Release 15.0(1)M4.7 or later.

  Workaround: There is no workaround.

- CSCtt20215

  Symptoms: Controller goes down after reload.

  Conditions: The symptom is observed with a VWIC3-2MFT-T1E1 (in E1/CAS mode) connected to a PBX.

  Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt21228

  Symptoms: Router crashes while trying to configure Tcl script via SSH connection.

  Conditions: SSH to the router and then try to configure Tcl script.

  Workaround: There is no workaround.

- CSCtt97905

  Symptoms: Multiple demandNbrCallDetails traps generated.

Conditions: Multiple demandNbrCallDetails traps are generated for connect under normal conditions.

Workaround: There is no workaround.

- CSCtu02835

  Symptoms: While running Cisco IOS Release 15.1(4)M2, slow performance is exhibited through the Fast Ethernet WAN ports.

  Conditions: This symptom is observed when the **scheduler interval** command is configured. This causes the Fast Ethernet WAN ports to display many throttles in the **show interface** command.

  Workaround: Remove the **scheduler interval** command.

- CSCtu11140

  Symptoms: When there is no reachability cache on a DLSw router, the DLSw router sends CUR_EX unexpectedly if receiving XID_F.

  Conditions: The symptom is observed if a DLSw router receives XID_F when there is no reachability cache.

  Workaround: There is no workaround.

- CSCtu21636

  Symptoms: Sometime calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

```
Power alarm on DSP channel ch=1 is ON 0001 0001 **
Power alarm on DSP channel ch=1 is OFF 0001 0000 **
Power alarm on DSP channel ch=1 is ON 0001 0001 **
Power alarm on DSP channel ch=1 is OFF 0001 0000 **
```

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtu36224

  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

  Conditions: This symptom is observed on a Cisco router that is used for SSLVPN.

  Workaround: There is no workaround.

- CSCtv22140

  Symptoms: A Cisco 891 router cannot communicate with the on-board Cisco V.92 modem. This communication failure prevents the router from connecting externally via the modem.

  Conditions: This symptom is observed on a Cisco 891 router while it is booting up and causes occasional failure.

  Workaround: There is no workaround.

- CSCtw48553

  Symptoms: When MPLS-IP is configured on a Cisco router and QoS policy-map actions are applied, classification fails and packets are dropped. This prevents the committed information rate (CIR) from getting updated on the output interfaces.

  Conditions: This symptom is observed on any Cisco router that is running Cisco IOS Release 15.0(1)M7.10 or later, or Cisco IOS Release 15.1(4) M2.5 or later.

  Workaround: There is no workaround.

- CSCtx08011

  Symptoms: A Cisco IOS router crashes at “ipname_domain_lookup”.

  Conditions: This symptom is observed on a Cisco router while executing *vrf/vt1* or any WORD from “user exec” mode.

  Workaround: There is no workaround.

- CSCtx38806

  Symptoms: SSL VPN users get disconnected once their Microsoft Windows machine is updated with the Microsoft Security update KB2585542. This affects Cisco AnyConnect clients.

  This symptom may also be observed on Microsoft Internet Explorer browsers or browsers that have the BEAST SSL vulnerability fix. This fix uses SSL fragmentation (record-splitting).

  Google Chrome browser v16.0.912 is affected for Clientless WebVPN on Windows and MAC machines. Mozilla Firefox v10.0.1 also displays the error message:

  ```
  The page isn't redirecting properly.
  ```

  Conditions: This symptom is observed with routers running Cisco IOS releases that act as the headend for SSL VPN connections.

  Workaround 1: Use a Clientless browser to start the client. This works only in some Cisco IOS releases.

  Workaround 2: Uninstall the update.

  Workaround 3: Use rc4. This is a less secure encryption option. Hence, use it only if it meets your security needs. To use rc4, then you configure the following commands:

  – **webvpn gateway** *gateway name*

  – **ssl encryption** *rc4-md5*

  Workaround 4: Use AC 2.5.3046 or 3.0.3054.

  Workaround 5: Use older versions of Mozilla Firefox (v9.0.1).

  Further Problem Description: AnyConnect users receive the following error message:

  ```
  Connection attempt has failed due to server communication errors. Please retry the
  connection.
  ```

  The AnyConnect event log displays the following error message snippet:

  ```
  Function: ConnectIfc::connect
  Invoked Function: ConnectIfc::handleRedirects
  Description: CONNECTIFC_ERROR_HTTP_MAX_REDIRS_EXCEEDED
  ```

Resolved Caveats—Cisco IOS Release 15.0(1)M7

Cisco IOS Release 15.0(1)M7 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M7 but may be open in previous Cisco IOS releases.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login

with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this 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-ssh

- CSCso46409

  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

  Conditions: This symptom is observed using WebVPN on a Cisco 3845 with an AIM-VPN/SSL-3.

  Workaround: There is no workaround.

- CSCsw70555

  Symptoms: A Cisco 1811 V.92 interface sees CRC errors against different modems using Pagent.

  Conditions: 50 PPS of 64-byte frames were being sent in each direction through the V.92 interface on the Cisco 181x.

  Workaround: Configure the **no ppp microcode** command under the async interface.

- CSCsy22787

  Symptoms: Existing NBAR HTTP implementation does not do correct subport classification in some cases.

  Conditions: NBAR is used for HTTP subport classification.

  Workaround: There is no workaround.

- CSCtb64686

  Symptoms: When a VC bundle is configured and traffic is passed at a high rate, the output packet counters may show an incorrect and very large value.

  Conditions: This symptom is observed only in Frame Relay PVC counters. The **show interface** command displays proper output.

  Workaround: There is no workaround.

- CSCtd10735

  Symptoms: A router crashes with a Cisco 7200 platform image.

  Conditions: Configuring the sgbp test commands as given in the “Steps to reproduce” enclosure.

  Workaround: There is no workaround.

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

  Workaround: There is no workaround.

- 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.

- CSCtf41721

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

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.

  2. Hub 2 tunnel is shut and unshut.

  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtg68047

  Symptoms: The router reloads.

  Conditions: The symptom is observed if several tunnels with crypto protection are being shut down on the router console and the **show crypto sessions** command is executed simultaneously on another terminal connected to the router.

  Workaround: Wait until the tunnels are shut down before issuing the **show** command.

- 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.

- CSCth11006

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCth46251

  Symptoms: IPv6 OSPF cannot form a neighborship using an IPv6 ESP transport mode configuration.

  Conditions: This symptom is observed on some platforms with an onboard crypto engine.

  Workaround: Use a software crypto engine. Also, the symptom is not observed with an AIM.

- CSCti10928

  Symptoms: Xcoder sends empty RTP stream in one direction only.

  Conditions: The symptom is observed on a CUBE that is running Cisco IOS Release 12.(24)T3 with an incoming fast start call.

  Workaround: There is no workaround.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- CSCti48483

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCti48504

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtj46670

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

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

  Workaround: Reload the router.

- CSCtj47829

  Symptoms: A buffer leak is experienced with “traffic-export” configured.

  Conditions: The issue seen when you export traffic to an interface and to an NME-APPRE-502-K9. All conditions are not completely known yet.

  Workaround: Disable the traffic-export functionality, for example:

```
! Traffic Export Configs
ip traffic-export profile axp-netscout
interface Integrated-Service-Engine1/0
bidirectional
mac-address 0080.8c00.0001

interface FastEthernet0/0.99
encapsulation dot1Q 99
ip address xxx.xxx.xxx.xxx 255.255.255.0
ip traffic-export apply axp-netscout

! Remove the Configs
interface fa0/0.99
no ip traffic-export apply axp-netscout
no ip traffic-export profile axp-netscout
```

- CSCtk34885

  Symptoms: Crosstalk being heard intermittently on inbound calls.

  Conditions: Inbound calls from PSTN to Ingress gateway hearing crosstalk on Rout call leg (DSP to PSTN) on AS5400XM.

  Workaround: The following command in Cisco IOS software can mitigate this for SIP:

  voice service voip sip source filter

  This eliminates the risk for crosstalk since the gateway blocks all rogue audio out to the PSTN with this command.

  The above command only works for SIP, so H323, MGCP, and SCCP are still affected.

  The following enhancement requests have been filed:

- CSCtq47019—Support on H.323, SCCP, and MGCP. This will allow the command to be used in all VoIP environments.
- CSCtq47431—To get this feature added to IP phones.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.8/1.6:

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

No CVE ID has been assigned to this issue.

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

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

- CSCtk53674

  Symptoms: A router that is running Cisco IOS Release 12.4(15)T14 and Cisco IOS Release 15.0M will crash when the SNMP v3 configuration is removed.

  Conditions: This symptom occurs when the running configuration contains the following depending on the Cisco IOS release:

  Cisco IOS Release 12.4(15)T14

  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST> priv aes 128 qosQOO!priv acc SNMP

  Cisco IOS Release 15.0(1)M4

  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST> priv aes 128 qosQOO!priv acc SNMP

  When you remove the above configuration using the **no snmp-server user** command, the router crashes.

  Workaround: There is no workaround.

- CSCtk55107

  Symptoms: A router crashes due to SIP.

  Conditions: This symptom is observed when SIP is configured.

  Workaround: The only workaround is to disable SIP.

- CSCtl54975

  Symptoms: A small number of Cisco 1812 routers have been observed to unexpectedly restart due to software-forced crashes, repeatedly.

  Conditions: Unknown.

  Workaround: While the root cause is being investigated, units that are experiencing this problem should be replaced. Please replace the Cisco 1812 and send the unit for Failure Analysis, after contacting the Cisco TAC and referencing this bug ID.

- CSCtl74521

  Symptoms: Crackling voice is heard on the PSTN rx side.

  Conditions: This symptom occurs under the following conditions:

  - RTP comes from Multilink interface. There is no audible crackling in the RTP stream.
  - If used, codec g711ulaw with packetization > 80 bytes.

  Workaround: Set codec packetization to 80 bytes on dial-peer or voice-class codec.

- CSCtl90341

  Symptoms: A router crashes due to an NHRP stack overflow.

  Conditions: This symptom occurs very inconsistently.

  Workaround: There is no workaround.

- CSCtn00405

  Symptoms: A Cisco router may crash when “isdn test call” is run.

  Conditions: This symptom has been experienced on multiple Cisco IOS versions, including Cisco IOS Release 12.4(15)10, 12.4(24)T4, and 15.0(1)M4.

  Workaround: There is no workaround.

- CSCtn12119

  Symptoms: There is no change in functionality or behavior from a user perspective. This DDTS brings in changes to padding used during signing/verification from PKCS#1 v1.0 to PKCS #1v1.5.

  Conditions: This symptom is observed during signing/verification for releases prior to Cisco IOS Release 15.1(2)T4.

  Workaround: The Rommon is capable of verifying images signed using both v1.0 and v1.5. As such no workaround is necessary from a usability perspective, the image boots and runs as expected. However, it will not be in compliance with FIPS 140-3 requirements.

- CSCtn19496

  Symptoms: Packet loss is seen when the service policy is applied on the tunnel interface. The **show hqf interface** command output shows drops in a particular queue with the following:

  ```
  Scheduler_flags 177
  ```

  The above value of 177 indicates an ATM driver issue. Once the issue is seen, the tunnel interface transitions to the down state.

  Conditions: This symptom is seen when the service policy is applied on the tunnel/GRE interface and when the source of the tunnel interface is the ATM interface (hwic-shdsl).

  Workaround: There is no workaround.

  Further Problem Description: The above-described symptom is seen only with the SHDSL link.

- 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(24T).

  Workaround: There is no workaround.

- CSCtn74169

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

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

  Workaround: Do not use long banner in HTTP intercept.

- CSCtn77090

  Symptoms: Gradual increase of CPU with CPU topping at 99% and increase in holding memory for IP SLA process may cause crash on routers that are running IP SLA probes, generally above 300 probes.

Conditions: This symptom is observed when there are more than 20 SNMP simultaneous probe restarts from IP SLA management software.

Workaround: Limit SNMP probe restarts to under 20 from IP SLA management software.

- CSCto05108

  Symptoms: A Cisco 7206 with VSA card is used as a GETVPN GM. After some time of operation, the router prints VSA-related traceback and completely stops encrypting/decrypting any traffic:

  ```
  %008720: Feb 24 11:11:01.674 GMT+5: VSA shim: crypto_ike_encrypt_callback ctx_next
  NULL -Traceback= 0x1BF4364z 0x3D38AE4z 0x3D007FCz 0x3CFA77Cz 0x3CFE108z 0x15829FCz
  0x15857ACz 0x1584800z 0x15822C8z 0x5580000z 0x1584E78z 0x1582384z 0x3D00DD8z
  0x3D00A64z 0x3D3852Cz 0x3D411B0z
  ```

  After that, all encrypted traffic is dropped. Crypto debugs (debug crypto isakmp, etc.) do not produce any messages. The only way to recover is to reboot the router.

  Conditions: This symptom is observed on a Cisco 7206 where a VSA card is used as a GETVPN GM and running Cisco IOS Release 15.0(1)M4 or Release 12.4(24)T3.

  Workaround: Disable encryption.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCto08754

  Symptoms: The crypto VTI interface with ip unnumbered VTI may experience input queue wedge. When the interface becomes wedged, all incoming traffic from the tunnel drops.

  Conditions: This symptom occurs when the crypto VTI interface becomes wedged.

  Workaround: There is no workaround.

- CSCto13254

  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

  ```
  Hash verification failed for file <temp location of profile>
  ```

  Conditions: This symptom is observed with Anyconnect 3.x when connecting to a Cisco IOS headend that is configured with a profile.

  Workaround: Remove the profile from the Cisco IOS headend.

- CSCto16597

  Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

  Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

  Workaround: There is no workaround.

- CSCto39885

  Symptoms: A router crashes.

  Conditions: gcid and callmon is turned on.

  Workaround: There is no workaround.

- CSCto41173

  Symptoms: A voice gateway crashes by TLB (store) exception with BadVaddr = 00000244.

  Conditions: This symptom is observed with a platform that acts as an H.323 gateway and runs Cisco IOS Release 15.1(3)T.

  Workaround: Revert to Cisco IOS Release 12.4(20)T.

- CSCto53332

  Symptoms: A router configured for IPSEC accounting may display the following error message:

  ```
  %AAA-3-BUFFER_OVERFLOW: Radius I/O buffer has overflowed
  ```

  This does not seem to result in any impact apart from intermittently lost accounting messages.

  Conditions: This symptom occurs when ipsec accounting is active.

  Workaround: There is no workaround.

- CSCto65352

  Symptoms: A system crashes randomly when an Apex module is in the system.

  Conditions: The system crashes under normal conditions.

  Workaround: There is no workaround.

- CSCto68554

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features.

  These vulnerabilities are:

  - Memory leak in Cisco IOS Software
  - Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw.

- CSCtq01250

  Symptoms: A memory leak in the SNMP ENGINE process is observed while the HDSL2-SHDSL-LINE-MIB is being polled.

  ```
  Router# show processes memory | include ENGINE
   130   0     125944    2384248      36056          0          0 SNMP ENGINE
  Router# show processes memory | include  ENGINE
   130   0     135996    2397784      46108          0          0 SNMP ENGINE
  Router# show processes memory | include ENGINE
   130   0     146048    2424856      56160          0          0 SNMP ENGINE
  ```

  Conditions: The symptom is observed when:

  1. The device has an HWIC-2SHDSL in one of its slots and a DSL group is configured under the SHDSL controller.

2. The device is polled via SNMP for OID 1.3.6.1.2.1.10.48.1.3.1 - hdsl2ShdslInventoryEntry.

Workaround: Block the above OID from being polled by SNMP.

Create a View:

snmp-server view cutdown internet included

snmp-server view cutdown 1.3.6.1.2.1.10.48 excluded

Apply the View:

snmp-server community <string> view cutdown ro

snmp-server community <string> view cutdown rw

- CSCtq05004

  Symptoms: A dialer loses its IP address sporadically.

  - "show interface atm x" will record output drops during the issue.

    ```
    ATM0 is up, line protocol is up
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
    31956 << Incrementing during the issue
    ```

  - "show interface queueing atm0.1" (hidden command) will show as follows:

    ```
    Interface ATM0 VC 8/35
    Queueing strategy: fifo
    Output queue 40/40, 31956 drops per VC << Incrementing during the issue
    ```

  - During the issue, if "debug ppp negotiation" is on, we will see the following:

    ```
    PPP: Missed 5 keepalives, taking LCP down
    PPP DISC: Missed too many keepalives
    ```

  - There will be no ATM (physical interface) flap in this case (during the issue).
  - A shut/no shut on the ATM interface does not help.

  Conditions: No conditions so far. The behavior is sporadic.

  Workaround: Reload.

- CSCtq05636

  Symptoms: When sending calls between two SIP endpoints, alphanumeric characters (non-numeric) are stripped when forwarding the invite to the outgoing leg.

  For example:

  ```
  Received: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  Sent: INVITE sip:18 669863384**83782255@10.253.24.35:5060 SIP/2.0
  ```

  In Cisco IOS Release 15.1(3)T1, the * character is not forwarded.

  Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1(3)T1.

  Workaround: Upgrade the code to Cisco IOS Release 15.1(3)T or Cisco IOS Release 15.1(M4).

- CSCtq07413

  Symptoms: A hardware crypto engine may fail to decrypt packets. An "invalid parameter" error is seen after decryption. Software encryption works fine.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(15)T6.

  Workaround: Use software encryption.

- CSCtq09899

  Symptoms: The VXML gateway crashes.

  Conditions: This symptom occurs during the load test when the **show mrcp client session active** command is used.

  Workaround: There is no workaround.

- CSCtq10356

  Symptoms: When video is enabled under a call manager profile, the Zone-Based Firewall SIP inspection engine will not create the RTP pinhole for voice.

  Conditions: This symptom is observed when video is enabled under the phone profile.

  Workaround: Disable video under the phone profile; the two options to disable are “Cisco Camera” and “Video Capabilities.”

- CSCtq10684

  Symptoms: The Cisco 2800 crashes due to a bus error and the crash points to access to free internal structures in ipsec.

  Conditions: This symptom occurs when tunnel flap is observed before the crash.

  Workaround: A possible workaround is to reload the box.

- CSCtq12007

  Symptoms: Using a c7200 VSA in a 15.0M image, when there are multiple shared IPsec tunnels using the same IPsec protection policy, removing the policy from one tunnel could cause other tunnels to stop working until the next rekey or tunnel reset.

  Using a c7200 VSA in a 15.1T or 15.2T image, you can also see a similar problem but one that is less sever; you may see one every other packet drop, until the next rekey or tunnel reset.

  Conditions: In a 15.0M, 15.1T, and 15.2T image, VSA is used as the crypto engine.

  Workaround: Force a rekey after removing the shared policy from any shared tunnels by using the **clear crypto session** command or resetting all the tunnels.

- CSCtq15247

  Symptoms: The router crashes when removing the virtual PPP interface. The crash is more common if the L2TP session is flapping when the virtual PPP interface is removed.

  Conditions: This symptom occurs if the L2TP session is flapping when the virtual PPP interface is removed.

  Workaround: Remove the **pseudowire** command from under the **virtual-ppp interface** command before removing the interface.

  For example:

```
LAC1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
LAC1(config)# interface virtual-ppp1
LAC1(config-if)# no pseudowire
LAC1(config-if)# exit
LAC1(config)# no interface virtual-ppp1
```

- 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.

- CSCtq39406

  Symptoms: When you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM, the module shuts down after 2 minutes. Then, all IP connectivity and console connectivity to the router is lost.

  Conditions: This symptom occurs when you set up an energywise domain via the CLI and then set the energywise level to zero on a SM or ISM.

  Workaround: Remove the HWIC-3G-HSPA. When you remove the 3G module from the system, energywise works as expected. You can shut down power modules using the above configuration. As soon as the 3G card is installed in slot 2 or 3 and the energywise level is set to zero, the service module shuts down and the entire router crashes. It has no IP connectivity and the console is inactive. The only workaround is a hard reset (along with removal of the card).

- CSCtq55173

  Symptoms: A device that is configured with NAT crashes. SIP appears to be translated trough NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

  Conditions: The crash is triggered when the **clear ip nat translation ***, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

  Workaround: There is no workaround.

- CSCtq61850

  Symptoms: When the SNR call is forwarded to CUE after the SNR call-forward noan timer (cfwd-noan) expires, the call gets dropped unexpectedly after CUE answers the call.

  Conditions: This symptom occurs when calls to the SCCP SNR phone and SNR call-forward noan timer (cfwd-noan) are configured. Both SNR and mobile phones do not answer the call and the call is forwarded to voice mail.

  Workaround: There is no workaround.

- CSCtq64951

  Symptoms: The following message is displayed:

  ```
  %CERM-4-TUNNEL_LIMIT: Maximum tunnel limit of 225 reached for Crypto functionality
  with securityk9 technology package license.
  ```

  The **show platform cerm** command output shows all tunnels in use by SSLVPN.

  ```
  Number of tunnels 225 ... SSLVPN D D 225 N/A
  ```

  The **show webvpn session context all** command output shows no or very few active sessions.

  ```
  WebVPN context name: SSL_Context
  Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
  ```

  Conditions: This symptom occurs on SSLVPN running Cisco IOS Release 15.x. This issue is seen only on ISR G2 platforms.

  Workaround: Upgrade to Cisco IOS Release 15.1(4)M1 or later releases.

- CSCtq75008

  Symptoms: A Cisco 7206 VXR crashes due to memory corruption.

  Conditions:

  – The Cisco 7206 VXR works as a server for L2TP over IPsec.

  - Encryption is done using C7200-VSA.
  - More than two clients are connected.

  If client sessions are kept up for about a day, the router crashes.

  Workaround: There is no workaround.

- CSCtq84635

  Symptoms: Trunk DNs can act as if busy (such as by triggering CFB) even though they have no calls and show commands for ephone-dns or ports report nothing unusual.

  Conditions: This symptom occurs in Cisco IOS Release 15.0(1)M after heavy use; it is believed not to occur in Cisco IOS Release 12.4(20)T or prior releases.

  Workaround: Delete and re-add trunk DNs.

- CSCtq86500

  Symptoms: With the fix for CSCtf32100, clear text packets destined for the router and coming into a crypto-protected interface are not switched when VSA is used as the crypto engine.

  Conditions: This symptom occurs with packets destined for the router and coming in on an interface with the crypto map applied and VSA as the crypto engine.

  Workaround: Disable VSA and use software encryption.

- CSCtq91176

  Symptoms: When the Virtual-PPP interface is used with L2TP version 2 and the topology uses an L2TP Tunnel Switch (LTS) (multihop node) and L2TP Network Server (LNS), and PPP between the client and the LNS does renegotiation, then the PPP session cannot be established.

  Conditions: This symptom occurs when the LTS forwards the call based on the domain or full username from the PPP authentication username, and the LNS does PPP renegotiation.

  Workaround 1: Disable LCP renegotiation on the LNS and clear the L2TP tunnel at the LNS and LTS.

  Workaround 2: Forward the call on the LTS using an L2TP tunnel name instead of the PPP username/domain name.

- CSCtr15891

  Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

  Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.0(1)M6

Cisco IOS Release 15.0(1)M6 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M6 but may be open in previous Cisco IOS releases.

- CSCso33003

  Symptoms: If a child policy is attached to a parent policy twice, the router will reload if the child policy configuration is removed.

  Conditions: The parent policy needs to be attached to the target interface.

Workaround: Do not attach the same child policy twice in the same parent policy. Use a different policy instead.

- CSCtb72734

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

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

  Workaround: There is no workaround.

- CSCtb74547

  Symptoms: A Cisco ASR 1000 DMVPN HUB reloads at the process IPSEC key engine.

  Conditions: This symptom is observed when the “Dual DMVPN with Shared Tunnel-Protection” feature is enabled and the interface is shut down and brought up again.

  Workaround: There is no workaround.

- CSCtc00851

  Symptoms: The output of the **show mfib table** command on a line card may show tables not in “sync” state, and instead 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: This symptom is observed 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.

- CSCtc49086

  Symptoms: When configuration changes are performed within a multicast-enabled VRF that cause the PIM register tunnel interface to go down and come up again, spurious memory access appears when traffic is sent at the same time.

  Conditions: This symptom occurs when traffic is sent while configuration changes are being made.

  Workaround: There is no workaround.

- CSCtd23069

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

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

  Workaround: There is no workaround.

- CSCtd42628

  Symptoms: Router reloads due to bus error following tunnel flaps.

  Conditions: The symptom is observed following tunnel flaps.

  Workaround: There is no workaround.

- CSCtf24052

  Symptoms: On a Cisco router loaded with Cisco IOS Release 15.0(1)M or Release 15.1(1)T, traffic may not match the ACL configured with a port range inside a class-map.

  Conditions: This symptom is observed when the port range ACE is configured after a few ACEs, as in the following example:

  ```
  Flashcard#show access-lists 101 Extended IP access list 101 10 permit icmp any any 20 permit udp any any eq domain 30 permit udp any eq domain any 40 permit tcp any any range <start> <end> 50 permit tcp any range <start> <end> any <removed> 220 permit tcp any any range <start> <end>
  ```

  Workaround: Use ACE with a specific port to match the traffic, or use IP source/destination.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPsec SA has been deleted.

  Conditions: This symptom is observed on a Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the following syntax may vary depending on the versions used):

  ```
  ############ configure terminal ! event manager applet SR_000000526 event timer cron name SR_000000526 cron-entry "0 3 * * *" action 1 cli command "en" action 2 cli command "reload"! end ############
  ```

- CSCtg72652

  Symptoms: On Cisco 2900 series routers, the following warning message might display on the console:

  ```
  %ENVMON-1-POWER_WARNING: : Chassis power is not good in the PSU 1
  ```

  Conditions: Under rare conditions, the power supply sometimes sends a false alarm status to the system, even though the system power is working fine.

  Workaround: There is no workaround.

- 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: This symptom is observed on a dual RP Cisco 7600 series router with linecards 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.

- CSCti35326

  The Cisco IOS Software Network Address Translation (NAT) feature contains a denial of service (DoS) vulnerability in the translation of Session Initiation Protocol (SIP) packets.

  The vulnerability is caused when packets in transit on the vulnerable device require translation on the SIP payload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates the vulnerability is available.

This advisory is available at the following link:

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

- CSCti66454

  Symptoms: A Cisco router crashes when using the **show crypto session detail** command after using the **clear crypto session** command.

  Conditions: This symptom is observed when the router is running any form of tunnel protection, SAs have been cleared, and the user executes a **show** command.

  Workaround: Wait a few moments (30 seconds) between the **show** command and the **clear** command.

- CSCtj21045

  Symptoms: Header compression decodes the RTP timestamp incorrectly.

  Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.

  Workaround: Use IETF format compression.

- CSCtj23189

  Symptoms: Packet drops occur on low-rate bandwidth-guarantee classes, even if the offered rate is less than the guaranteed rate.

  Conditions: This symptom is observed when highly extreme rates are configured on the classes of the same policy. An example of extreme rates would be a policy-map with 3 classes: one with 16kbps, one with 1Mbps, and one with 99Mbps.

  Workaround: There is no workaround.

- 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 observed only for packets switched in software and not in platforms where packets are policy-base routed in hardware. This symptom is observed with route-map configuration, as follows:

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

  Workaround: There is no workaround.

- CSCtk06548

  Symptoms: Using CCBU CVP solution, SIP calls are disconnected during a stress test.

  Conditions: The symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by the SIP stack. This symptom is observed with PI14 image testing.

  Workaround: There is no workaround. The fundamental issue involves the selective ack (SACK) feature. A possible workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk58027

  Symptoms: The router crashes with the “ip sla icmp jitter” operation.

  Conditions: This symptom is observed when the “ip sla icmp jitter” operation is running with a high number of packets, along with voice and data traffic. To recreate the symptom, when the status of the ip sla is “OK,” enter the **no ip sla schedule** command, then enter the **no ip sla** *operation-number* command.

Workaround: There is no workaround.

- CSCtk64020

  Symptoms: A Cisco 7600 router crashes.

  Conditions: This symptom is observed when the **clear ip subscriber** command is entered.

  Workaround: There is no workaround.

- CSCtk67709

  Symptoms: The Cisco AnyConnect 3.0 package does not install correctly on the Cisco IOS front-end. It fails with the following error:

  ```
  ssl2-uut-3845a(config)#crypto vpn anyconnect flash:anyconnect-win-3.0.0432- k9.pkg
  SSLVPN Package SSL-VPN-Client (seq:1): installed %%Error: Invalid Archive
  ```

  Conditions: This symptom is observed with Cisco AnyConnect 3.0.

  Workaround: There is no workaround.

- CSCtk67934

  Symptoms: A Cisco router is forced to reload after a few days of encryption and decryption while processing high traffic.

  Conditions: This symptom is observed when VSA is enabled as a hardware crypto engine used for processing both firewall and encryption/decryption on the same interface.

  Workaround: Switch from VSA HW crypto engine to either SW crypto engine or VAM2+ HW crypto engine.

- CSCtk74660

  Symptoms: The Network Time Protocol (NTP) tries to re-sync after the server clock changes its time and after the NTP falls back to the local clock.

  Conditions: This symptom is observed when the server clock time drifts too far away from the local clock time.

  Workaround: There is no workaround.

- CSCtk76748

  Symptoms: After adding a new subinterface under interface gig0/2, there is a loss of connectivity over interface gig0/0.

  Conditions: This symptom is observed when creating a subinterface with **encapsulation** and **vrf forwarding** commands.

  Workaround: There is no workaround.

- CSCtk83638

  Symptoms: A client is assigned an IP address from an incorrect pool when it reconnects with a different profile.

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

  Workaround: There is no workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in “show crypto session summary” output.

  Conditions: This symptom is observed

  - when running EzVPN and if Xauth is performed by a different username during P1 rekey
  - when NAT is used in the VPN path.

  Workaround: Use the "save-password" feature (without interactive Xauth mode) to avoid sending the different username and password during P1 rekey.

- CSCtl20508

  Symptoms: A Cisco router fails to decrypt a packet, and for all packets received, the following message is logged:

  ```
  %IPSEC(epa_des_crypt): decrypted packet failed SA identity check
  ```

  In "sh crypto ipsec sa," the counter which increases is the "#recv errors."

  Conditions: This symptom is observed on a Cisco 3270 running Cisco IOS Release 15.0(1)M4. The Ttunnel interface has a crypto ipsec profile. Transport mode is being used. Packets received on this tunnel are not properly decrypted.

  This issue is not observed when reverting to default tunnel mode.

  Workaround: There is no workaround.

- CSCtl67079

  Symptoms: The following error message is seen on a Cisco router with an HWIC_1GE_SFP card inserted:

  ```
  %HWIC_1GE_SFP-3-INTERNAL_ERROR: GigabitEthernet0/0/0 SNMP high capacity counter
  register failed
  ```

  Conditions: This symptom is observed during bootup.

  Workaround: There is no workaround.

- CSCtl70143

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

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

  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.

- CSCtl73914

  Symptoms: A Cisco 2921 Gateway running Cisco IOS Release 15.1(1)T1 is unable to register with IMS.

  Conditions: The symptom is observed if the P-Associated-URI of the "200 Ok" response contains any special characters (!*.!) in Tel URI Parsing.

  Workaround: There is no workaround.

- CSCtn04686

  Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unplugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

Workaround: Unplug/plug in the cables.

- CSCtn08208

  Symptoms: Clicking on the Citrix bookmark causes multiple windows of the browser to open. The web page tries to refresh itself a few times, and finally the browser window hangs.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.0(1)M4.

  Workaround: Revert to Cisco IOS Release 15.0(01)M2.4.

- 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 symptom 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.

- CSCtn18784

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

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn26785

  Symptoms: Incoming traffic on DS3 atm 1/0 is process-switched:

  ```
  3845#sh int atm 1/0 stat ATM1/0 Switching path Pkts In Chars In Pkts Out Chars Out
  Processor 98170 10995040 1 68 Route cache 0 0 98170 10995040 Total 98170 10995040
  98171 10995108 3845#
  ```

  ```
  3845#sh cef int atm 1/0 ATM1/0 is up (if_number 5) Corresponding hwidb fast_if_number
  5 Corresponding hwidb firstsw->if_number 5 Internet address is 64.65.248.174/30 ICMP
  redirects are never sent Per packet load-sharing is disabled IP unicast RPF check is
  disabled Input features: Ingress-NetFlow Output features: Post-Ingress-NetFlow IP
  policy routing is disabled BGP based policy accounting on input is disabled BGP based
  policy accounting on output is disabled Hardware idb is ATM1/0 Fast switching type 9,
  interface type 138 IP CEF switching enabled IP CEF switching turbo vector IP prefix
  lookup IPv4 mtrie 8-8-8-8 optimized Input fast flags 0x0, Output fast flags 0x0
  ifindex 5(5) Slot Slot unit 0 VC -1 IP MTU 4470 3845#
  ```

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCtn27599

  Symptoms: The OIR of an NM-1T3/E3 line card crashes the router.

  Conditions: This symptom is observed only on the Cisco 3945 router.

  Workaround: There is no workaround.

- CSCtn57655

  Symptoms: A Cisco router running Cisco IOS Release 15.0M crashes during a SIP call.

  Conditions: This symptom occurs when a Cisco router is running Cisco IOS Release 15.0M. This symptom occurs only when the “callmonitor” CLI under “voice service voip” is configured.

Workaround: There is no workaround.

- CSCtn63109

  Symptoms: After reload or on a freshly upgraded router, Ping fails when the MTU is set above 1500 bytes on the FastEthernet 4-WAN interface of a Cisco 800 series router connected directly to another router.

  ```
  Router# ping 10.1.1.1 rep 5 df-bit size 1650 Type escape sequence to abort. Sending
  5, 1650-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds: Packet sent with the DF
  bit set .....
  ```

  Conditions: This symptom is observed only with Cisco IOS Release 15.0(1)M4 and is specific to Cisco 800 series routers. To be more specific, only the Cisco 881SRST router with the Cisco IOS image c880voice-universalk9-mz.150-1.M4.bin is affected. This issue is consistently seen with subinterface configurations based on the Fa4 interface.

  Also, the following Traceback is noticed:

  ```
  *Feb 28 15:26:19.639: %LINK-4-TOOBIG: Interface FastEthernet4, Output packet size of
  1664 bytes too big, -Traceback= 0x81056958z 0x81056EF8z 0x8112CBF4z 0x8200073Cz
  0x82001264z 0x82001978z 0x820019D4z 0x8201BBF4z 0x8201C16Cz 0x8203F5C8z 0x8203FDACz
  0x82D86B9Cz 0x81A1DC70z 0x819E6FD8z 0x819F6114z 0x8128C0CCz
  ```

  Workaround: Remove and reconfigure MTU on the interface.

- CSCtn65060

  Symptoms: A Cisco device crashes.

  Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

  Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn72939

  Symptoms: The L2tpv3 feature is not working on Cisco 181x platforms.

  Conditions: This symptom occurs with Cisco 1812 devices running Cisco IOS Release 15.(0)M and later releases.

  Workaround: Configure bridge-group under that xconnect interface.

- CSCtn76183

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

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

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

- CSCtn77154

  Symptoms: The Stateful Inspection feature is enabled after reload when an “ip nat outside” statement is configured on two interfaces, which results in packets being punted to the CPU. This causes overall performance degradation.

  Conditions: This symptom is observed when two outside NAT interfaces are configured and “no ip nat service nbar” is configured on the interface.

  Workaround: Configure “ip nbar protocol discovery” on the interface.

- CSCtn87012

  Symptoms: FXS ports that are SCCP-controlled stay in the “ringing” state, and the DSP thermal alarm pops up.

  Conditions: This symptom is observed on a Cisco VG200 series voice gateway running Cisco IOS Release 15.0(1)M4 if the phone is answered during the ringing ON cycle.

  Workaround: Pick up the phone during the ringing OFF cycle.

- CSCto03446

  Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

  Conditions: This symptom occurs with a flat policy attached to frame-relay interface with traffic shaping enabled.

  Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto14435

  Symptoms: A Cisco 7200 router with a C7200-VSA module may crash when the tunnel interface is enabled.

  Conditions: This symptom is observed on a Cisco 7200 router with a C7200-VSA module enabled. This symptom is observed with Cisco IOS Release 12.4(24)T4 and Cisco IOS Release 15.0(1)M.

  Workaround: Disable ip route-cache and ip route-cache cef on the tunnel source interface.

- CSCto63954

  Symptoms: A router with GETVPN configurations continuously crashes.

  Conditions: This symptom is observed with GETVPN-related configurations with the “fail-close” feature activated.

  Workaround: There is no workaround.

- CSCto88686

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip.

- CSCtq27180

  Symptoms: After a Cisco IOS upgrade, any permanent licenses are erased and evaluation licenses do not work.

  Conditions: This symptom is observed only on IOS internal releases.

  Workaround: There is no workaround.

  Further Problem Description: The following LOG messages and errors are found:

```
Mar 30 01:27:38.003: %LICENSE-2-LIC_STORAGE: Storage validation failed -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z Mar
30 01:27:38.447: %LICENSE-2-VLS_ERROR: 'VLSsetInstallLicenseStorage' failed with an
error - rc = 136 - 'Error[136]: Specified license store doesn't exists.' -Traceback=
604D93C0z 637CE110z 637CE1BCz 637CE334z 61C73250z 61C734E0z 63765DE4z 63765DC8z
```

- CSCtq30875

  Symptoms: A Cisco ISR G1 will display "March 11, 2011" when the **show clock** command is entered. This will affect functionality that depends on the clock to be accurate (for example, certificates to make secure connections or calls).

  Conditions: This symptom is observed only on Cisco ISR G1 routers running ISR licensing software.

  Workaround: The clock can be set manually via CLI.

- CSCtq36726

  Symptoms: Configuring the **ip nat inside** command on the IPSEC dVTI VTEMP interface does not have any effect on the cloned virtual-access interface. The NAT functionality is thus broken, because the V-access interface does not get this command cloned from its respective VTEMP.

  Conditions: This symptom is observed on Cisco ASR1006 (RP2/FP20) routers with ikev2 dVTI. This issue may be service impacting and is easily reproducible.

  Workaround: Reconfigure the virtual-template interface such that the **ip nat inside** command is applied first, followed by other commands.

Resolved Caveats—Cisco IOS Release 15.0(1)M5

Cisco IOS Release 15.0(1)M5 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M5 but may be open in previous Cisco IOS releases.

- 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: Occurs on a router running Cisco IOS Release 12.4.

  Workaround: There is no workaround.

- CSCsl28726

  Symptoms: A Cisco router crashes when the routemap used by IPv6 PBR is deleted.

  Conditions: This symptom is observed on a Cisco router with IPv6 PBR configured on an interface when traffic is being PBR routed and the user deletes the routemap used by IPv6 PBR.

  Workaround: Unconfigure PBR before deleting the routemap.

- 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 linecards 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
```

- CSCsz89093

  Symptoms: A Cisco 2800 router may drop multicast packets.

  Conditions: This symptom is observed when stream sources are connected to an NM-16ESW switch module.

  Workaround: Disable IGMP snooping.

  Further Problem Description: Packet loss can be seen with as little as 1 stream consisting of 1500 byte packets @ >= 1470pps. Packet loss can be viewed as follows:

  ```
  zmrd# zmrd#sh int Fa1/1 stat
  FastEthernet1/1 Switching path Pkts In Chars In Pkts Out Chars Out Processor 100000
  150000000 53 4028 Route cache 0 0 0 0 Total 100000 150000000 53 4028 <--- 100,000 pkts
  received zmrd# zmrd#sh int Vlan200 stat
  Vlan200 Switching path Pkts In Chars In Pkts Out Chars Out Processor 0 0 0 0 Route
  cache 99997 149595512 0 0 Total 99997 149595512 0 0 <--- 3 pkts dropped zmrd#
  ```

- CSCta38476

  Symptoms: When removing the tunnel interface with CDP enabled, tracebacks are generated. CDP does not come up in all interfaces.

  Conditions: The symptom is observed with large numbers of CDP neighbors in an MCP router.

  Workaround: Disable CDP before deleting the tunnel interface.

  Further Problem Description: CDP tries to send a packet over a deleted tunnel interface causing the issue.

- CSCtb66963

  Symptom: A SIP call from a call-forwarded phone to a Cisco IOS VoIP gateway is rejected when INVITE contains a comma in the Diversion Header.

  Conditions: Example of an inbound SIP invite that contains a Diversion field such as this:

  ```
  ---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
  172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
  <sip:5555555555@xxx.xx.xxx.xxx>;party=calling;screen=yes;privacy=off From:
  <sip:5555555555@xxx.xx.xxx.xxx>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879?
  To: <sip:15551111111@xx.x.xxx.xxx> Date: Sat, 29 Aug 20xx 08:06:56 GMT Call-ID:
  e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
  User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK,
  UPDATE, REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact:
  <sip:5555555555@xxx.xx.xxx.xxx:5070> Expires: 180 Allow-Events: presence
  Session-Expires: 1800 Diversion: "Smith, John"
  <sip:87007@xxx.xx.xxx.xxx>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
  Content-Type: application/sdp Content-Length: 214 ----
  ```

```
The IOS gateway will respond back with the following:
---- Sent: SIP/2.0 400 Bad Request - 'Malformed CC-Diversion/Diversion/CC-Redirect
Header' Reason: Q.850;cause=100 From:
<sip:5555555555@xxx.xx.xxx.xxx>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879
Content-Length: 0 To: <sip:1551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
```

Workaround: Modify the diverting name associated with the redirecting device so that it does not contain a comma.

- CSCtc65347

  Symptoms: A Cisco 3845 may have a processor pool memory leak in the SNMP Engine.

  Conditions: This symptom is observed on a Cisco 3845 running Cisco IOS Release 12.4(20)T1 and polling specific VoIP mibs.

  Workaround: Do not poll VoIP Peer CFG Entry mibs or use an snmp view to block the router from replying to said poll, such as:

  ```
  snmp-server view leak internet included snmp-server view leak cvVoIPPeerCfgEntry
  excluded snmp-server community <community name> view leak
  ```

  Further Problem Description: "Show proc mem <pid>" (where <pid> is the process ID for SNMP ENGINE) should decode to VoIP Peer Cfg Entry mibs being polled.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- 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.

- CSCte27828

  Symptoms: Call forward does not work. "Call forward no answer" scenario does not work, but not systematically: sometimes it works, sometimes not.

  Conditions: This symptom is observed with the following topology:

  ```
  call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider.
  ```

```
IP addresses: CUCM10.10.10.3 Cube SUD10.10.10.2 CUBE North192.168.101.10 SBC
192.168.100.5
```

When the “call forward no answer” fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC doesn’t answer due to this.

Workaround: There is no workaround.

- CSCte50870

  Symptoms: A Cisco AS5400 crashes due to a watchdog timeout. CPU hogs due to the “SERIAL A’detect” process are seen before the reload:

  ```
  %SYS-3-CPUHOG: Task is running for (36000)msecs, more than (2000)msecs (36/6),process
  = SERIAL A’detect.
  ```

  After some time the device crashes:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SERIAL A’detect.
  ```

  Conditions: The symptom is seen on a Cisco AS5400 that is running Cisco IOS Release 12.4(24)T2. The serial interfaces of the device are configured with “autodetect encapsulation xxx” and the router system clock has been updated:

  ```
  %SYS-6-CLOCKUPDATE: System clock has been updated from 10:42:09 UTC Wed May 19 2010 to
  11:42:09 MET Wed May 19 2010, configured from console by console. %SYS-6-CLOCKUPDATE:
  System clock has been updated from 11:42:09 MET Wed May 19 2010 to 12:42:09 MET-DST
  Wed May 19 2010, configured from console by console.
  ```

  Workaround: If possible, remove this command.

- 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.

- CSCte94221

  Symptoms: PPP connection over CDMA link is flapping.

  Conditions: The symptom is observed when using Cisco IOS Release 15.0M.

  Workaround: Shut / no shut the interface and wait for 2 minutes.

- 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.

- CSCtf56107

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

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

  Workaround: There is no workaround.

- 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

- 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.

- CSCtg41606

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

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

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

- CSCtg42904

  Symptoms: Router crashes with the following error message:

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

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

  Workaround: There is no workaround.

- CSCtg55338

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

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

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

- CSCtg90518

  Symptoms: The output of “sh ip inspect statistics” shows negative or irrelevant values and the following log is generated:

  ```
  %FW-4-ALERT_ON: getting aggressive, count(6/2147483647) current 1-min rate: 4294967295
  ```

  Conditions: This symptom is observed with an IOS Firewall on Cisco IOS Release 15.0(1)M when “ip inspect tcp” is enabled.

  Workaround: There is no workaround.

- CSCth03022

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-sip.

- CSCth06812

  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

  ```
  R1(config)#parser view SUPPORT
  R1(config-view)# secret cisco
  R1(config-view)# commands exec include ping
  R1(config-view)# commands exec include configure terminal
  R1(config-view)# commands exec include show ip ospf neighbor <--Where we see the hang
  ```

  Workaround: Do not configure the <CmdBold>commands exec include show ip ospf neighbor<noCmdBold> command in parser view configuration.

- CSCth20696

  Symptoms: Address Error (load or instruction fetch) exception, CPU signal 10 on a Cisco 7204VXR (NPE-G1).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(25c).

  Workaround: There is no workaround.

- 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.

- CSCth61759

  Symptoms: In a SIP-SIP video call flow, CUBE may not correctly negotiate video stream.

  Conditions: This symptom is observed in two scenarios.

  Scenario 1:

  This problem was observed in the following SIP-SIP Delayed Offer - Delayed Offer (DO-DO) call flow:

  7985-- CUCM -- CUBE -- Tandberg VCS -- Tandberg Telepresence server

  1. Call is originated by 7985
  2. Tandberg Telepresence Server provides multiple video codecs in the SDP (Session Description Protocol) of the SIP “200 OK” response

```
m=video 53722 RTP/AVP 96 97 34 31 b=AS:1920 a=rtpmap:96 H264/90000 a=fmtp:96
profile-level-id=42e016;max-mbps=108000;max-fs=3600 a=rtpmap:97 H263-1998/90000
a=fmtp:97 CIF4=1;CIF=1;CIF=1;QCIF=1 a=rtpmap:34 H263/90000 a=fmtp:34
CIF4=1;CIF=1;CIF=1;QCIF=1 a=rtpmap:31 H261/90000 a=fmtp:31 CIF=1;QCIF=1 a=sendrecv
```

3. CUBE sets video m-line to 0 in the SDP of the SIP "ACK" response

```
m=video 0 RTP/AVP 96
```

Scenario 2:

End to end SIP Flow Around call with Cisco Video Telephony Advantage (CVTA).

CVTA -- CUCM -- CUBE -- CUBE -- CUCM -- CVTA

Workaround: There is no workaround.

- CSCth68038

  Symptoms: After a simulated failover of an L2L tunnel, a Cisco 7200 series router with VSA will fail to encrypt traffic for a period of time, typically for several minutes. VSA will then begin to encrypt traffic correctly.

  Conditions: This symptom is observed when manually failing over a spoke from one hub Cisco 7200 (without VSA) to a secondary hub Cisco 7200 with VSA. The issue only affects virtual-template interfaces.

  Workaround: Use software encryption.

- CSCth70437

  Symptoms: Crypto sessions drop after the following error message:

  ```
  000059: *Jul 1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
  ptr=83D91910, count=0, -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z 0x8039460Cz
  0x80397B40z 000060: *Jul 1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in
  datagram_done, ptr=83D91CE4, count=0, -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z 000061: *Jul 1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in
  datagram_done, ptr=83D920B8, count=0, -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z 000062: *Jul 1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in
  datagram_done, ptr=83D82F8C, count=0, -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z
  ```

  Conditions: This symptom is observed on Cisco IOS 8XX series routers and when crypto is applied to dialer interface.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCti03808

  Symptoms: A Cisco 7200 may crash with a fatal error.

  Conditions: This symptom is observed only when PA-POS-1OC3 and C7200-VSA port adapters are installed and the encrypted traffic is being sent through the POS interface. The problem is more likely as traffic load increases.

  Workaround: Use a different POS port adapter or VAM module instead of the VSA encryption module.

  Further problem description: During investigation the router would also occasionally hang instead of crash. With the fix for this symptom the hangs were not seen.

- CSCti07805

  Symptoms: Router reloads @sipSPIUpdSrtpSession.

  Conditions: This symptom is observed during Hold/Resume on a basic SRTP call with Cisco IOS Release 15.1(2.3)T.

  Workaround: There is no workaround.

- CSCti22544

  Symptom: IKE fails to come up while using RSA signature. PKI debugs show the following message:

  ```
  PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
  ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
  ```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and vrf-label is configured under trustpoint; for example, `crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke`

  Workaround: There is no workaround.

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

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

CVE ID CVE-2010-3050 has been assigned to document this issue.

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

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

- CSCti51145

  Symptoms: After a reload of one router, some or all of the BGP address families do not come up. The output of **show ip bgp all summary** will show the address family in NoNeg or idle state, and it will remain in that state.

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  - The non-reloading device must have a "neighbor x.x.x.x transport connection- mode passive" configuration, or there must be an ip access list or packet filter which permits connections initiated by the reloading device, but not by the non-reloading device. In Cisco IOS, such ip access-lists typically use the keyword 'established' or "eq bgp".
  - It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
  - When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
  - Both peers must be multisession capable. * "transport multi-session" must not be configured on either device, or enabled by default on either device.
  - "graceful restart" must not be configured.

  Workarounds:

  1. Remove the configuration "neighbor x.x.x.x transport connection-mode passive" or edit the corresponding filter or ip access list to permit the active TCP opens in both directions.
  2. Configure "neighbor x.x.x.x transport multi-session" on either the device or its neighbor.
  3. Configure a very short keepalive interval (such as one second) on the non-reloading device using the neighbor x.x.x.x timers 1 holdtime command.
  4. Configure graceful restart using the command neighbor x.x.x.x ha- mode graceful-restart.
  5. If the issue occurs, use the clear ip bgp * command to cause all sessions stuck in the NoNeg state to restart. You can also use clear ip bgp x.x.x.x address Family to bring up individual stuck sessions without resetting everything else.

  Further Problem Description: This is a day one problem in the Cisco IOS multisession implementation which impacts single-session capable peers. CSCsv29530 fixes a similar problem for some (but not all) situations where "neighbor x.x.x.x transport single-session" is configured and NSF is not configured.

  The effect of this fix is as follows: when the neighbor is in single-session mode, AND the router sees an OPEN message for a neighbor which is in the ESTABLISHED state, then the router will send a CEASE notification on the new session and close it (per section 6.8 of RFC 4271). Additionally, it will send a keepalive on the ESTABLISHED session. The keepalive is not required, but will cause the established session to be torn down if appropriate.

Note that the fix does not solve the problem when interacting with Cisco IOS Release 12.2(33)SB based releases if the Release 12.2(33)SB router is the one not reloading.

- CSCti61949

  Symptoms: Unexpected reload with `"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.

- CSCti62801

  Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

  Conditions: The symptom is observed with a SIP analog endpoint on a Cisco IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

  Workaround: There is no workaround.

- CSCti66153

  Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging the following error:

  `%VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.`

  Conditions: The following conditions need to be met:

  - A Cisco 7200 series router with VSA in receive-only mode.
  - Key server in receive-only mode.
  - Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the “inside” of the Cisco 7200.
  - Traffic matching a key server delivered crypto ACL matching L4 ports (e.g.: **permit tcp any any eq 23**).

  Workaround: Use one or more of the following workarounds.

  1. Use VAM2+ instead of VSA
  2. Use GETVPN ACL without l4 ports (e.g.: permit ip any any).
  3. Have the Cisco 7200 in passive mode as well
  4. Do not use receive-only mode on the keyserver.

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- 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.

- 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.

- CSCti75666

  Symptoms: Calls from CUCM through H.323 to SIP CUBE get disconnected when remote AA does transfer.

  Conditions: The symptom is observed on CUCM 4.1.3 and 6.1.3. It is seen on an ISR gateway that is running Cisco IOS Release 12.4(24)T2.

  Workaround: Convert H.323 leg to SIP.

- CSCti77879

  Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.

  Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.

  Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

  Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny {jump | clear | drop}** command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.

- CSCti79848

  The Cisco IOS Software contains two vulnerabilities related to Cisco IOS Intrusion Prevention System (IPS) and Cisco IOS Zone-Based Firewall features. These vulnerabilities are:

  – Memory leak in Cisco IOS Software
  – Cisco IOS Software Denial of Service when processing specially crafted HTTP packets

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-zbfw.

- 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.

- CSCti88897

  Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2) T1, the command **service-policy output QOS_CUST_BASIC_OUT** disappears when the router is reloaded or power cycled.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti93175

  Symptoms: NAT router does not translate address of the last TCP ACK in the 3- way handshake.

  Conditions: The symptom is observed with the following conditions:

  - VRF NAT is involved
  - “ip nat outside source translation” has to exist
  - NAT flow-entries are disabled by **no ip nat create flow- entries**.

  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.*

- CSCtj03381

  Symptoms: NAT traffic is getting process switched when you configure “nat entry” or you reload the router.

  Conditions: The symptom is observed when you enable VRF-aware NAT with the “match-in-vrf” option.

  Workaround 1: Reconfigure “ip cef”.

  Workaround 2: Do a **clear ip route vrf** <*vrf*> *.

- 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.

- CSCtj09256

  Symptoms: AnyConnect client fails to connect. The following error messages may be seen:

  ```
  Unable to Process Response from server <servername or IP address of gateway>
  Connection attempt has failed due to server communication errors. Please retry the
  connection
  ```

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(24)T4.

  Workaround 1: Use the clientless portal to launch AnyConnect.

  Workaround 2: Use Cisco IOS Release 12.4(24)T3 or earlier.

- CSCtj14738

  Symptoms: Router crash. Before the crash we see the following error messages:

  ```
  %ISDN-6-DISCONNECT: Interface Serial0/0/0:4 disconnected from 6406418 , call lasted
  1410 seconds
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x244, pc=0x247BE87Cz ,
  ra=0x247BE878z , sp=0x3175D388
  ```

  Conditions: The symptom is observed on a Cisco 2911 router that is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtj21696

  Symptoms: The virtual access interface remains down/down after an upgrade and reload.

  Conditions: The issue occurs on a router with the exact hardware listed below (if HWIC or the VIC card is different the problem does not happen):

  ```
  Router1#sho inv NAME: “chassis”, DESCR: “2801 chassis” PID: CISCO2801 , VID: V04 , SN:
  FTX1149Y0KF
  NAME: “motherboard”, DESCR: “C2801 Motherboard with 2 Fast Ethernet” PID: CISCO2801 ,
  VID: V04 , SN: FOC11456KMY
  NAME: "VIC 0", DESCR: “2nd generation two port EM voice interface daughtercard” PID:
  VIC2-2E/M= , VID: V , SN: FOC081724XB
  NAME: “WIC/VIC/HWIC 1", DESCR: “4 Port FE Switch” PID: HWIC-4ESW , VID: V01 , SN:
  FOC11223LMB
  NAME: “WIC/VIC/HWIC 3", DESCR: “WAN Interface Card - DSU 56K 4 wire” PID:
  WIC-1DSU-56K4= , VID: 1.0, SN: 33187011
  NAME: “PVDM 1", DESCR: “PVDMII DSP SIMM with one DSP with half channel capacity” PID:
  PVDM2-8 , VID: NA , SN: FOC09123CTB
  ```

  Workaround: Shut/no shut the serial interface.

- CSCtj24453

  Symptoms: The following traceback is observed when **clear ip bgp *** is entered:

  ```
  %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: This symptom is observed when the **clear ip bgp *** command is entered 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
  ```

This symptom is rare, since 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 symptom will not be observed.

- 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.

- 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.

- CSCtj39558

  Symptoms: Subinterface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj39777

  Symptoms: A Cisco 2921 router crashes with IPSec and QoS.

  Conditions: The symptom is observed on a Cisco 2921 router when QoS pre-classify is enabled.

  Workaround: There is no workaround.

- CSCtj41194

  Cisco IOS Software contains a vulnerability in the IP version 6 (IPv6) protocol stack implementation that could allow an unauthenticated, remote attacker to cause a reload of an affected device that has IPv6 enabled. The vulnerability may be triggered when the device processes a malformed IPv6 packet.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6.

- CSCtj47696

  Symptoms: A Cisco router supporting HWIC-2CE1T1-PRI WAN module will not process any in/outgoing ISDN calls once the network derived clock is configured (i.e.: “network-clock-participate wic 0”).

  Conditions: The symptom is observed on a Cisco 3800/3900 series router with NM-8CE1T1-PRI, HWIC-2CE1T1-PRI or VWIC3-2MFT-T1/E1 running Cisco IOS Release 15.1 (1)T or Release 12.4(24)T4 and deriving the clock from the network.

Workaround: Configure “national reserve 0 0 0 0 0 0" under the affected E1 port followed by shut/no shut of the E1 port. Complete the workaround by configuring “national reserve 1 1 1 1 1 1” and flapping the port one more time.

If modem calls are not required, “no network-clock-participate” can also be used as a workaround.

Further Problem Description: Problem is not seen on VWIC2-2MFT-T1/E1.

- CSCtj52077

  Symptoms: Policy at subinterface is not accepted with CBWFQ.

  Conditions: This symptom is observed when policy is used in Ethernet subinterface.

  Workaround: There is no workaround.

- CSCtj61657

  Symptoms: IO memory leak is seen followed by TCP no buffer logs:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0xXXXXXXXX, alignment
  xxx Pool: I/O Free: xxxx Cause: Not enough free memory Alternate Pool: None Free: 0
  Cause: No Alternate pool -Process= “Pool Manager”
  %TCP-6-NOBUFF: TTY0, no buffer available -Process= “SCCP Application”, ipl= 0, pid=
  XXX
  ```

  Conditions: The symptom is observed in the presence of VOIP phones using multicast applications with the **session protocol multicast** dial-peer configuration command.

  Workaround: There is no workaround.

- CSCtj66392

  Symptoms: Tunnel interface does not go up on standby router and IKE and IPSec SAs are not synchronized to the standby router. Even if tunnel protection is configured, crypto socket is not opened.

  Conditions: This symptom is observed when IPSec stateful failover for tunnel protection is configured.

  Workaround: Use Cisco IOS Release 12.4(11)T4.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

  Conditions: This symptom is observed when a multicast server is multiple hops away from multicast clients.

  Workaround: There is no workaround.

- CSCtj77285

  Symptoms: Router CPU becomes high, tending towards 80%+ from normal operating conditions. The command **show mem | inc FNF OCE** will show multiple rows rather than just a couple of rows.

  Conditions: The symptom is observed with voice calls and VOIP in use. It is seen when Flexible NetFlow is configured.

  Workaround: Switch off Flexible NetFlow (although that leaves memory consumption in place and CPU higher than normal) or reboot the router.

- CSCtj78210

  Symptoms: One-way audio, which moves from one port to another when the router is rebooted.

Conditions: The symptom is observed when using multiple session protocol multicast connection trunk configurations for LMR, E&M Immediate, and/or other multicast applications such as the conditions where this was first detected (in a Radio over IP solution). This symptom only affects PVDM3.

Workaround: Configure conference bridge that is associated with SCCP. The exact numbers to be used to force these ports to be in use will depend on the individual platform.

For example, configure:

```
voice-card 0 (1... 2... etc...) dspfarm dsp service dspfarm
dspfarm profile x conf max sessions xx << use the maximum max partic << use the
maximum associate app sccp no shutdown
dspfarm profile x2 conf max sessions xx << use the maximum max partic << use the
maximum associate app sccp no shutdown
dspfarm profile x3 conf max sessions xx << use maximum (if allowed) max partic << use
the maximum (if allowed) associate app sccp no shutdown
dspfarm profile x conf shutdown no dspfarm profile x conf
```

The idea behind this workaround is to consume all of the upper VOICE DSP channels to disallow them for use by a multicast session.

This workaround will only work if you have enough DSP resources to remove all DSP channels above 16 and still have enough DSP resources for the needed DSP channel/multicast sessions.

- CSCtj81533

  Symptoms: The following error message is seen:

  ```
  np_vsmgr_modify_connection: invalid service id 11 passed
  ```

  No detrimental consequences or effects on the correct operation of the router are observed; however, thousands of these error messages may appear on the console.

  Conditions: This symptom is observed on Cisco AS5400 platforms during VoIP calls, and is more evident when the router is handling multiple calls.

  Workaround: There is no workaround.

- CSCtj84901

  Symptoms: Cisco routers crash when traffic passes from the MGF port of any module towards the router CPU with a PVDM module present in the router.

  Conditions: This symptom is observed on Cisco 19xx, 2911 and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The modules that currently connect to MGF are

  1. Service Ready Engine modules (ISM and SM SRE)
  2. Etherswitch modules (SM and EHWIC)

  If any traffic from these modules flows over the MGF port towards the router CPU, then the router will crash.

  This symptom is not observed on Cisco 2951, 39XX, or 39XXe routers.

  Workaround: For the EHWIC Etherswitch module with PVDM on the router, there is no workaround.

  For the Etherswitch SM modules and Service Ready Engine modules, as long as the MGF port on these modules is not configured to send traffic to the router, there will be no issue. For traffic between modules over MGF there is no issue. If the MGF port on these modules has to be used, then the PVDM would have to be removed from the router. There is no workaround if both the PVDM and the MGF port on these modules has to be used.

- 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 Cisco 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 message from the multihop peer:

  ```
  "Error code(9): Try another directed and Optional msg: SSS Manager disconnected
  session <<<< INVALID"
  ```

  Workaround: There is no workaround.

- CSCtj89941

  Symptoms: A Cisco device may crash when using the command **clear crypto session** on an EzVPN client.

  Conditions: This symptom is observed with the following 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.

- CSCtj90342

  Symptoms: A Cisco HWIC-2T module installed on a Cisco 2901, 2911 or 2921 router configured with "physical-layer async" (Async mode) delays printing the characters that you type in the terminal window.

  Conditions: This symptom is observed on Cisco 2901, 2911, and 2921 platforms with Cisco HWIC-2T modules installed and running any Cisco IOS 15.X release.

  This symptom is not observed on a Cisco 2951 platform.

  Workaround: There is no workaround.

  Further Problem Description: In a production environment, the first data string may not be transmitted until you enter the second string. For example, reverse telnet to the line using the command prompt of PC. A blank screen is opened where you will type. Now, using hyperterminal software, connect HWIC- 2T to your PC (similar to the console connection). You will see a blank screen on the software. Start typing numbers such as 1,2,3,4, and 5 at the command prompt. "2" will not be displayed until you press "3" at the command prompt, "4" will not show up until you press "5," and so forth.

- CSCtj96915

  Symptoms: LNS router hangs up at interrupt level and goes into an infinite loop.

Conditions: Unknown. See Further Problem Description below.

Workaround: There is no workaround. Only a power cycle can remove the symptom.

Further Problem Description: This is a hypothesis based on analysis of the data provided for the failures experienced by the customer, together with an extensive code review. The issue can happen during L2TP session creation and removal, specifically where a session removal/addition is prevented from being completed by an interrupt, which is raised. We believe this is a timing issue. While this is a rare event, the probability of it occurring increases with load and number of sessions.

- CSCtk01638

  Symptoms: Analog endpoint and connection trunk is torn down due to the following Q.850 cause code in SIP BYE request:

  ```
  Port will show in a S_TRUNK_PEND ****************************************** show
  voice call summary | inc 0/2/0 0/2/0 - - - S_TRUNK_PEND
  ```

  Conditions: This symptom is observed when the **clear counters** command is invoked. This triggers the gateway to stop sending rtcp events, which causes media inactivity to be activated on the far-end gateway and the connected trunk to be torn down.

  Workaround: There is no workaround.

- CSCtk02647

  Symptoms: On an LNS configured for L2TP aggregation, it might be that per- user ACLs downloaded via Radius cause PPP negotiation failures (IPCP is blocked).

  Conditions: This symptom is observed when LNS multilink is configured and negotiated for PPP/L2TP sessions and per-user ACL downloaded for PPP users via radius.

  Workaround: There is no workaround.

- 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 172.16.0.1 remote-as 200 neighbor
  172.16.0.1 ebgp-multihop 255 no auto-summary !
  ip route 0.0.0.0 0.0.0.0 10.10.200.1 ip route 172.16.0.1 255.255.255.255 10.0.12.2 ip
  route 172.16.0.1 255.255.255.255 10.0.120.2
  Router 2: interface Loopback200 ip address 10.10.200.1 255.255.255.0 ! interface
  Loopback201 ip address 172.16.0.1 255.255.255.0 ! interface Ethernet0/0 ip address
  10.0.12.2 255.255.255.0 !
  interface Ethernet1/0 ip address 10.0.120.2 255.255.255.0 ! router bgp 200 no
  synchronization bgp log-neighbor-changes network 10.10.200.0 neighbor 10.0.12.1
  remote-as 100 neighbor 10.0.12.1 update-source Loopback201 no auto-summary ! ip route
  0.0.0.0 0.0.0.0 10.0.12.1 !
  ```

  Workaround: Use static routes tied to a specific interfaces instead of using “floating static routes.”

- CSCtk12681

  Symptoms: Enabling IP SLA trace for VoIP RTP causes a crash.

  Conditions: This symptom is observed when IP SLA TRACE is enabled for VoIP RTP probe.

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk13720

  Symptoms: A Cisco router may crash when trying to remove an entry from an extended access-list.

Example:

```
Extended IP access list < NAME > 10 permit tcp any any ack 20 permit tcp any any fin
30 permit tcp any any ack fin 40 permit tcp any any rst
router(config)#ip access-list extended < NAME >
router(config-ext-nacl)#no 10
```

Conditions: This symptom was first found on a Cisco router running Cisco IOS Release 15.0(1)M4 with extended access-lists and QoS configured. After further testing, we were able to determine that Cisco IOS Release 15.1(3)T did not crash due to this bug.

Router will crash only if we have TCP flags in the ACL.

Workaround: To modify an ACL, follow these steps:

1. Remove ACL filter from the class. For example: class-map match-any c1 no match access-group name QOS-TCP-OPTIONS
2. Modify the ACL ip access-list extended QOS-TCP-OPTIONS no 10
3. Re-add the ACL filter in class: class-map match-any c1 match access-group name QOS-TCP-OPTIONS

In summary, DO NOT modify ACL if the ACL is configured as a filter under any class. Remove filter first, modify ACL and re-add filter to class.

- CSCtk35960

  Symptoms: The line protocol status is changed to “down” after configuring speed or duplex. The **show ip int brief** command shows “up/up,” but the status is actually “up/down.” This symptom may be observed even if speed and duplex are not configured.

  Conditions: This symptom is observed with Cisco IOS Release 15.0(1)M4.

  Workaround: There is no workaround.

- 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.

- CSCtk56570

  Symptoms: When there are some call loads on CUBE, one-way call occurs while call proceeding, after sending SIP CANCEL.

  Conditions: This symptom occurs when media transcoder-high-density is enabled on CUBE.

  Workaround: Disable media transcoder-high-density.

- CSCtk60909

  Symptoms: Router crashes due to interrupt stack low.

  Conditions: This symptom occurs when the router is as SWMTP and makes more than six transfer calls.

  Workaround: There is no workaround.

- CSCtk66979

  Symptoms: Hold queue on an ATM interface does not work.

  Conditions: This symptom is observed when hold-queue per VC is configured on ATM interfaces (NM-1A-T3/E3) on ISRG2.

Workaround: There is no direct workaround. It will work only for default hold- queue size or maximum hold queue size under an ATM interface.

- CSCtk68647

  Symptoms: DMVPN stops allowing connections after operating for some time (based on number of connections). The **show crypto socket** command shows sockets are leaking and never decrease even when the SA is inactive.

  Conditions: This symptom occurs on Cisco ASR code prior to Cisco IOS Release XE 3.2.0. Multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0. Remove other DMVPN tunnels (or shutdown tunnels).

- CSCtk74685

  Symptoms: When H225 messages for a call are sent out to the wrong TCP socket by an IOS gateway, they may sent to a completely different IP than the one that is aware of the call. When this occurs, the new socket gets paired to the call and the H323 stack tries to tear down the H245 socket for a call that is being disconnected. Instead, it erroneously tears down an unrelated calls H225 socket. This causes the unrelated call to drop.

  Observed with “debug cch323 all” and “debug ip tcp trans”:

  ```
  13090333: Dec 3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm: received
  IWF_EV_H245_DISCONN while at state IWF_ACTIVE 13090334: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_send_event_to_h245_connection_ sm: Changing to new
  event H245_DISCONNECT_EVENT 13090335: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: state=0, event=4, ccb=C5E442B8,
  listen state=2 13090336: Dec 3 13:18:20.965:
  //137091/80C6B1F78F31/H323/cch323_h245_connection_sm: H245_CONNECT: Received event
  H245_DISCONNECT_EVENT while at H245_NONE state 13090337: Dec 3 13:18:20.965: TCP0:
  state was ESTAB -> FINWAIT1 [24696 -> 192.0.2.100(1720)] 13090338: Dec 3 13:18:20.965:
  TCP0: sending FIN
  ```

  Conditions: This symptom occurs with all IOS images with the fix for CSCin76666.

  The cascade issue noted in this bug is triggered by an event where CM closes down an H225 or H245 TCP socket mid-call. Due to the cascading nature of CSCtk74685, identifying the root call that triggers this socket conflict may be extremely difficult, until the fix for CSCtk74685 is applied.

  Workaround: Use one of the following workarounds:

  1. Enable call preservation on CM, which does not prevent the socket from getting torn down, but minimizes user impact and does not drop audio on the call.

     voice service voip h323 call preserve

     System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced > Allow Peer to Preserve H.323 Calls > False > Save

  2. Run a Cisco IOS release that does not have the fix for CSCin76666.
  3. Change the signaling protocol to SIP.

- CSCtk84116

  Symptoms: A GETVPN ks crash may occur when split-and-merge is happening between the key servers.

  Conditions: This symptom is observed when a split-and-merge occurs between the key servers.

  Workaround: There is no workaround.

- CSCtk95992

  Symptoms: DLSw circuits to not come up when using peer-on-demand peers.

Conditions: This symptom occurs when DLSw uses UDP for circuit setup.

Workaround: Configure the command **dlsw udp-disable**.

Further Problem Description: This symptom occurs in the following (and later) releases:

Cisco IOS Releases 12.4(15)T14, 12.4(24)T4, 15.0(1)M3, 15.1(1)S, 15.1(2)T, 12.2(33)SXI4, and 12.2(33)SXI4a.

- CSCtl04285

  Symptoms: After a BGP flap or provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

  Conditions: This symptom is observed with BGP session flap or when provisioning a new session.

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

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

  Conditions: This symptom occurs when performing switchover or Online Insertion and Removal (OIR), while MLP sessions are initiating.

  Workaround: There is no workaround.

- CSCtl20509

  Symptoms: CME/SRST 4.0 when ATA unregister/ fall back to Cisco Unified CallManager, the virtual POTS dial-peers stay up and calls to ATA do not go out the H323 dial-peer to Cisco Unified CallManager. The calls fail with user busy. This issue affects only ATA. Dialpeers of the IP phones behave normally.

  Conditions: This symptom occurs when the ATA fallback to the CCM occurs and registers with the CCM. However, The virtual pots dial peer for the ATA are up.

  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.

- CSCtl47666

  Symptom: Intermittent call drops for CME SNR calls that go to voicemail.

  Conditions: This symptom is observed on a Cisco IP phone with SNR configured. When the “no answer” timer is reached, the call will intermittently drop instead of going to voicemail.

  Workaround: There is no workaround.

- CSCtl77735

  Symptoms: Saving a configuration to NVRAM may fail.

  Conditions: This symptom may be observed on a Cisco 2900 platform while saving the Cisco IOS configuration.

  Workaround: Erasing the startup configuration and saving again may recover the configuration.

- CSCtl87067

  Symptoms: Priority class will drop traffic before explicit police rate is reached.

  Conditions: This symptom is observed on Cisco ISR platforms when strict priority with explicit police is configured.

  Workaround: There is no workaround.

- CSCtl87879

  Symptoms: MGCP calls fail as the DTMF detection and reporting via NTFY message does not occur.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T5 but not in Cisco IOS Release 12.4(24)T4

  Workaround: There is no workaround.

- CSCtl92014

  Symptoms: After a reprompt element, “enumerate”, using internal variables like _prompt or _dmtf, no longer produces a valid list of options and repeats the last option.

  Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T and later releases.

  Workaround: There is no workaround.

- 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.

Resolved Caveats—Cisco IOS Release 15.0(1)M4

Cisco IOS Release 15.0(1)M4 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M4 but may be open in previous Cisco IOS releases.

- CSCso02147

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCso20810

  Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. Occurs when multicast subsequently flows out a crypto-enabled interface.

Conditions: This bug 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.

- CSCsu95339

  Symptoms: Output from the **show idmgr session** command displays a corrupted service name.

  Conditions: Enter the **show idmgr session** command.

  Workaround: There is no workaround.

- CSCsw38009

  Symptoms: Packet drops are seen on an ATM interface when it is used as a tunnel source.

  Conditions: This symptom is observed as soon as Per SA QoS is configured on the tunnel interface.

  Workaround: This symptom is not seen on Ethernet.

- 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 Catalyst 4000 releases:

  - Cisco IOS Release 12.2(52)SG/XO
  - Cisco IOS Release 12.2(50)SG4/5/6/7
  - Cisco IOS Release 12.2(53)SG/SG1/SG2

  This bug applies to all hardware, not specific to 4500 switches.

  Workaround:

  1. Configure the interfaces one by one.

  2. Force a switchover “redundancy force-switchover”.

  3. Use Cisco IOS Release 12.2(50)SG3 until the fix code is released.

  Resolution:

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

- CSCta50110

  Symptoms: A GM does not register.

  Conditions: This symptom is observed when a crypto map is attached to a tunnel interface only.

  Workaround: Apply the crypto map to the tunnel source physical interface as well.

- 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.

- CSCta91928

  Symptoms: A Cisco 881GW with a 3G modem may crash when the modem is reset or power-cycled.

  Conditions: This symptom is observed on a Cisco 501 or 880 with a 3G modem when “test cellular 0 modem-power-cycle” or “test cellular 0 modem-reset” is entered.

  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.

- CSCtb55576

  Symptoms: When an HWIC-3G-GSM cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing the other interfaces is delayed for approximately 160 to 250 ms during the %LINK-3-UPDOWN event.

  Conditions: The symptom is observed on a Cisco 2811 router with an HWIC-3G-GSM. Any time the cellular interface experiences a state change, traffic routed through the Cisco 2811 router is delayed for approximately 160 to 250 ms.

  Workaround: There is no workaround.

- 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 ...
```

- CSCtc06935

  Symptoms:

  Packet loss occurs between two Cisco 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios after upgrading to Cisco IOS Release 12.4(22)T2.

  Conditions: The symptom is observed with the following conditions:

  – After a code upgrade.

  – On Cisco 3200s connected via wireless radios.

  – It does not occur on devices directly connected via fiber.

  Workaround: Use Cisco IOS Release 12.4(1a).

- 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.

- CSCtd31465

  Symptoms: An H323 to SIP CUBE may get stuck in a race condition if a reINVITE with delayed media is quickly followed by a reINVITE with early media while still renegotiating the H323 side of the call for the delayed media INVITE. This may lead to one-way or no-way audio.

  Conditions: This symptom was observed with the following topology:

  IP phone---CUCM---H.323 Fast Start---CUBE---SIP---3rd-party SIP server--- CallCenter

  Calls flow from the IP phone to the CallCenter hanging off a third-party device. The third-party device re-INVITEs, rapidly, as calls traverse through its menu/IVR system.

  Workaround: There is no workaround.

- CSCtd39579

  Symptoms: A router crashes when we try to remove service-policy/waas from an interface.

  Conditions: Traffic should be hitting the interface, CPU utilization should be high, and NAT should be applied on the interface as well.

  Workaround:

  1. Remove NAT from the interface.

  2. Remove the service policy.

  3. Re-apply NAT.

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

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

  Workaround: There is no workaround.

- CSCtd62885

  Symptoms: IKE renegotiation might fail for minutes while one peer displays:

  ```
  %CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from <ip> was not encrypted and it should've
  been
  ```

Conditions: The symptom is observed when certificates are used. The signature verification might fail after MM5 or MM6 messages are exchanged preventing the tunnel establishment. The issue seems to hit Cisco IOS Release 12.4(20) T3 and Release 12.4(24)T2. It affects only Cisco 7200 series routers with VSA modules.

Workaround: Use pre-shared keys.

- CSCte18124

  Symptoms: Ping over back-to-back ATM interface fails, if ATM PVC is created with “atm vc-per-vp 1024”.

  Conditions: The issue is seen only with HWIC-4SHDSL line cards and only when “atm vc-per-vp 1024” is configured.

  Workaround: Create ATM PVC without “atm vc-per-vp 1024”.

- CSCte89130

  Symptoms: Router experiences a memory leak.

  Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **show mem alloc total** command).

  Workaround: There is no workaround.

- CSCte91259

  Symptoms: A Cisco router may unexpectedly reload due to a bus error after displaying an “%IDMGR-3-INVALID_ID” error.

  Conditions: The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

  Workaround: There is no workaround.

- CSCte92581

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

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

  Workaround: There is no workaround.

  Further Problem Description: The stuck VRF cannot be reused.

- CSCte93792

  Symptoms: Virtual access bound to an ATM interface does not come up.

  Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

  Workaround: There is no workaround.

- CSCte94301

  Symptoms: IPv6 PBR is not applied to locally-originated ping packets.

  Conditions: This symptom occurs when IPv6 PBR is configured for application to locally-originated ping packets.

  Workaround: There is no workaround.

- CSCtf26639

  Symptoms: A router crashes when turning on WAAS, adding a couple of specific class maps, and then turning off WAAS.

Conditions: This is a corner case that is seen only when a specific type of filter is used with two or more classes; for example, for a WAAS class of the following type:

```
class-map type waas DT-40
 match tcp source ip 192.168.1.116 dest port 10040 10049
class-map type waas DT-50
 match tcp source ip 192.168.1.116 dest ip 192.168.101.117 port 10050 10059
policy-map type waas waas_global
 class DT-40 insert-before waas-default
 optimize tfo application DT-40
 class DT-50 insert-before waas-default
 optimize tfo application DT-50
 end
```

The router will crash with such a configuration. Here, we have all TCP filters with same source IP address. This is the special condition.

Workaround: There is no workaround.

- CSCtf48179

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

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

  Workaround: There is no workaround.

- 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.

- CSCtg08496

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

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

  Workaround: There is no workaround.

- CSCtg41206

  Symptoms: In a Cisco 7200VXR NPE-2 with VSA crypto accelerator enabled and GDOI crypto-map applied to an interface, egress QoS classification is not happening for non-encrypted packets. As the result, these packets end up in class-default and being treated accordingly. Packets/bytes/rate counters in class-default are not counting these packets properly. Encrypted packets are processed correctly.

  Conditions: This behavior is observed in all Cisco IOS Releases 12.4(24)T and 15.0(1)M.

  Workaround: Disable VSA crypto accelerator with the **no crypto engine slot 0** global configuration command. Switching to software crypto engine may adversely affect router's crypto processing performance, CPU load, and control plane stability.

- 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

- CSCtg52885

  Symptoms: The HSRP state on dot1q subinterfaces remain in INIT state.

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

  Workaround: Perform a shut/noshut on the 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.

- CSCtg69202

  Symptoms: CUBE modifies the RTP port number before passing it to the remote end, which causes one-way audio.

  Conditions: This symptom is observed only when the RTP port number is higher than the RTCP port number in the incoming request from the endpoint. Instead of sending the same RTP port number, CUBE decrements the RTP port number by one less than the RTCP port number when it forwards the OLC Ack to the destination side. This causes the destination to send the audio packets to the wrong port on the originating side, causing one-way audio.

  Workaround: There is no workaround.

  Further Problem Description: Under some specific conditions, when CUBE receives the OLC acknowledgement with the media control information from an H323 client, instead of passing the same RTP port number to the remote end, it modifies the RTP port number, causing the one-way audio.

- CSCtg71332

  Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

Workaround:

1. Use SP services feature set.

2. Upgrade router to Cisco IOS Release 12.4(24)T.

3. Install one or more PVDM sLOTS.

- CSCtg91336

  Symptoms: A Cisco router may crash during show command **show ip ospf rib** execution.

  Conditions: This symptom is observed in 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.
  - The 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 to use the command, enter **terminal length 0** and print the entire output.

- 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).

- CSCtg94872

  Symptoms: Packets are not classified correctly by the QoS class map in the CEF switching path, resulting in priority packets being dropped below bandwidth reservations. This is shown by the **show policy-map interface** command.

  Conditions: This symptom occurs under the following conditions:

  - Use a 64k leased line.
  - Configure LLQ on the egress port by policy map.

  Workaround: Disable CEF.

- CSCtg96518

  Symptoms: Fast memory leak occurs in CCSIP CCB Pool.

  Conditions: This symptom is observed on a Cisco 2951 integrated services router with Cisco IOS Release 15.1(1)T.

  Workaround: Reload the router.

- CSCth03379

  Symptoms: A Cisco router reloads while booting with DSL configurations.

  Conditions: Router is configured with a DSL controller.

  Workaround: Changing the line-term to “cpe” prior to a reload should allow the box to come back normally at which point the termination can be re-configured to “co”.

- CSCth15268

  Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

  Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit on.

  Workaround: Set “llc2 local-window” to 1.

- 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.

- CSCth18146

  Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

  Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

  Workaround: There is no workaround.

- CSCth23787

  Symptoms: 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 to 20 seconds.

  Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth23814

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

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

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

- CSCth26441

  Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 controller that connects to the NME module.

  Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

  Workaround: There is no workaround.

- CSCth31395

  Symptoms: Frame Relay PVC stays in INACTIVE state.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

  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.

- 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.

- CSCth35377

  Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

  Conditions: This symptom is observed on a GigabitEthernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters: encapsulation dot1Q xxx ip pim sparse-mode.

  Workaround: Remove "ip pim sparse-mode."

- CSCth36261

  Symptoms: A router crashes.

  Conditions: This symptom occurs when the router is configured for fax calls (specific to T.37 only).

  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.

- CSCth40506

  Symptom: A Cisco voice gateway does not have its GigabitEthernet link connected to the network, but the call is not cleared from the PRI when the Application Ack Timer expires.

Conditions: This symptom is observed on a Cisco 2911 voice gateway with Cisco IOS Release 15.0(1)M and a Cisco 2951 voice gateway with Cisco IOS Release 15.0(1)M1.

Workaround: There is no workaround.

Further Problem Description: When a voice call is placed, a SIP INVITE is sent:

Sent: INVITE sip:x@x.x.x.x:5060 SIP/2.0

Because the Cisco gateway does not have network connectivity, no SIP reply is received from the network. Sixty seconds later, the Application Ack Timer expires:

```
-- .May 4 17:49:29.120 GMT=+1: ISDN Se1/0:15 **ERROR**: CCPCC_TApplnAckExpiry:
Application Ack Timer expired. b channel 1 cref 0x8021 call_id 0x0045
```

The call, however, is not cleared from the PRI.

- CSCth46540

  Symptoms: Configuring **memory-size iomem** returns an error:

  Maximum IO percent supported for 2560MB memory is 0 (0MB)

  Conditions: The symptom is observed on a Cisco 1941 installed with 2.5 GB of DRAM.

  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.

- CSCth47765

  Symptoms: Once a router boots up, FXS/FXO voice-port in slot2 stays in “S_OPEN_PEND” state. The DSP from the MB that provides resources to the EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards in slot 2 goes into “FW_DNLD_FINISHED” state which causes the voice ports on EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards to go into “S_OPEN_PEND state”.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(1) T0.9 with 26.8.0 DSPware.

  Workaround: There is no workaround.

- CSCth48457

  Symptoms: A crash is seen at qos_classify_opttype.

  Conditions: The symptom is observed when changes are being made to the service policy while traffic is running. It is seen when using the same child policy-map in multiple classes of the parent and then removing the child policy-map by unconfiguring the parent classes. It happens with the following Cisco IOS Releases: 12.4(15)T, 12.4(20)T, 12.4(22)T, 12.4(24)T, 15.0(1)M, and 15.1(1)T.

  Workaround 1: Define the policy-map you wish to run before applying it on the interface level.

  Workaround 2: Do not use the same child policy in multiple classes of the parent.

- CSCth52720

  Symptoms: With client-initiated L2TPv2, IPCP packets are not sent when MLP is enabled.

Conditions: The symptom is observed when PPP multilink is configured with Cisco IOS Releases 12.4(24)T3, 12.4(11)XJ, and 15.1(1)T.

Workaround: Remove the PPP multilink configuration or use Cisco IOS Release 12.3(14)T6.

- CSCth58283

  Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

  Conditions: NAT is enabled.

  Workaround: There is no workaround.

- CSCth62136

  Symptoms: The ISDN L2 goes to "Layer 2 NOT Activated."

  Conditions: This symptom is observed when a service policy is attached to the dialer interface.

  Workaround: Remove the service policy from the interface.

  Further Problem Description: This symptom is not seen with:

  - 12.4(13d)
  - 12.4(15)T12

  This symptom has been seen with:

  - 12.4(22)T5
  - 12.4(24)T3
  - 15.0(1)M3

- 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.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- 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.

- CSCth66251

  Symptoms: You are not able to configure a policy-map for the second time in a Cisco 860 router. An "internal data base error" message is seen.

  Conditions: The symptom is observed when configuring a policy-map for the second time and with a Cisco 860 router.

Workaround: There is no workaround.

- CSCth67788

  Symptoms: sVTI stops forwarding traffic when a local policy is configured on a device.

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

  Workaround 1: Do not use a local policy.

  Workaround 2: Configure “no ip route-cache cef” on the tunnel interface.

- CSCth69361

  Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

  Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

- 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.

- CSCth83508

  Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

  Conditions: The problem is seen when using WSMA to run the **session install** command.

  Workaround: Perform the install manually from a VTY session.

- CSCth84233

  Symptoms: Router may crash due to Redzone memory block corruption (I/O) when “qos pre-classify” is configured under tunnel interfaces. The packet is overwriting the next block.

  Conditions: The trigger for this issue is configuring “qos pre-classify”.

  Workaround: Remove “qos pre-classify”.

- CSCth85829

  Symptoms: On an async tunnel, enabling “ip cef” can introduce latency/packet drop. You will see the following:

  – Packet loss is observed for CEF-switched traffic.

  – Very high latency is seen for successful packets.

  Conditions: The symptom is observed when:

  – “ip cef” is enabled.

  – Service-policy is attached to either dialer or async interface.

  Workarounds:

  1. Disable “ip cef”.

  2. Remove service policy from async interface.

  3. Use record option for ping from LAN host.

  4. Use a mainline code, for example: Cisco IOS Release 12.4(25).

- 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”.

- CSCth87638

  Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

  Conditions: The symptom is observed on WIC-based platforms. It was seen originally on an IAD243x using a HWIC-CABLE-D-2.

  Workaround: Manually change the MAC address problem card.

  Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- CSCth90593

  Symptoms: A Cisco Router may crash from a corrupted program counter: “%ALIGN-1-FATAL: Corrupted program counter” from an IPIP call.

  Conditions: This symptom is observed only when the router is acting as a voice gateway.

  Workaround: There is no workaround.

- CSCth97996

  Symptoms: A Cisco 39xx router may crash.

  Conditions: The symptom is observed during regular operations and with an extensive QoS configuration. The issue is seen when running Cisco IOS Release 15.0(1)M3.

  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.

- 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.

- 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.

- CSCti06686

  Symptoms: On a Cisco 2900, the async interface drops all outbound packets.

  Conditions: This symptom is observed with data packets that are exiting the async interface through the CEF path.

  Workaround: Disable hardware framing under the async interface using the following hidden command:

  no ppp microcode

- 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.

- CSCti10016

  Symptoms: After the **format** command is run on a 32GB or larger disk, the **show** command displays that only 4GB is free on the device.

  Conditions: The symptom is observed when formatting disk that is larger than 32GB in capacity.

  Workaround: Use a smaller size disk that has no more capacity than 32GB.

- CSCti10222

  Symptoms: The following exceptions are seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of XXXX bytes failed from 0xYYYYYYYY, alignment #
Pool: I/O Free: # Cause: Memory fragmentation Alternate Pool: None Free: 0 Cause: No
Alternate pool -Process= "IGMP Snooping Receiving Process", ipl= #, pid= #,
-Traceback= 0x81E8B6BCz 0x81EB0660z 0x802EC198z 0x802EC8E4z 0x802ED88Cz 0x802F1988z
0x803BBD88z 0x803BBF2Cz 0x8045E5CCz 0x804615F4z
Can't duplicate packet Can't duplicate packet Can't duplicate packet
```

Conditions: This symptom is observed when VLANs are added while multicast traffic is flowing through the router.

Workaround:

1. Prune the multicast feed that is coming from the respective VLAN using the following command: "switchport trunk allowed vlans except <mcast vlan#>".

or

2. Upgrade to Cisco IOS Release 15.1(2)T1.

- 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.

- CSCti10828

  Symptoms: In Cisco IOS Release 12.4T, there is no response to SNMP queries of:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive
  1.3.6.1.4.1.9.9.276.1.1.2.1.12 cieIfHighSpeedReceive
  ```

  within the CISCO-IF-EXTENSION-MIB although supported at the CLI:

  ```
  interface GigabitEthernet0/3
   bandwidth receive 100 <<<<<
  ==> , BW 100000 Kbit/sec, RxBW 100 Kbit/sec
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip
   version 2
   no validate-update-source
   network 10.0.0.0
   no auto-summary
  !
  address-family ipv4 vrf test
   no validate-update-source
   network 172.16.0.0
   no auto-summary
   version 2
   exit-address-family
  ```

  And doing a reload causes the "no validate-update-source" statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

  Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti15990

  Symptoms: EzVPN will not come up if the dialer interface flaps.

  Conditions: This symptom is observed when the dialer interface is profile- based.

  Workaround: Change the dialer interface to non-profile-based.

- CSCti17190

  Symptoms: A router crashes when trying to do sre install.

  Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

  Workaround: There is no workaround.

- CSCti18745

  Symptoms: If user has configured http port 80 or default http port, then reboots the router, it will produce invalid connection url with port 0. Later the connection from ACS to CPE might fail.

  Conditions: This symptom occurs if user has default http port 80 configured and then reboots the router.

  Workaround: Once router is up and running, again configure some port other than 80, and then reconfigure port 80.

  ```
  Router(config)# ip http port 8000
  Router(config)# no ip http port or ip http port 80
  ```

- CSCti19627

  Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

  Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

  Workaround: Remove “call-park system application”.

- 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.

- CSCti25280

  Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

  ```
  **ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
  ```

  Conditions: The symptom is observed when there is also a VWIC installed in the chassis (example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

  Workaround: Remove the VWIC.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti27128

  Symptoms: A Cisco 2911 router crashes repeatedly when trying to boot up.

  Conditions: This symptom occurs when an IPVS module is installed in the NME slot with an SM-NM adaptor in a Cisco 2911 router. The Cisco 2921 is not affected.

  Workaround: There is no workaround if the IPVS module is required. Otherwise, the IPVS module can be removed from the Cisco 2911.

- CSCti32334

  Symptoms: DDNS process gets stuck and marks all updates as duplicates. The command **debug ip dhcp server packet detail** shows:

  ```
  DDNS: Duplicate update rejected 'host.somedomain.com.' <=> 192.168.0.1 server 0.0.0.0
  ```

  Conditions: This happens in a day or so under moderate load following a router reboot. DDNS updates are performed by IOS DHCP server ("update dns" is configured in a pool).

  Workaround: There is no workaround.

- CSCti39902

  Symptoms: An RRI route is still seen on the UUT via router1 after the deletion of the IPsec SA.

  Conditions: Configure RRI on the UUT.

  Workaround: There is no workaround.

- CSCti47649

  Symptoms: A router may crash with the message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04
  ```

  Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

  Workaround: There is no workaround.

- CSCti48014

  Symptoms: A device reloads after executing the "show monitor event <comp> ... all detail" command (where <comp> is an option listed under "show monitor event ?").

  Conditions: This symptom is observed if the configurations are done in the order below,

  ```
  monitor event-trace <comp> stacktrace <depth>
  monitor event-trace <comp> size <size value>
  ```

  And any related event gets recorded in between the above two configurations.

  Workaround: To avoid the crash, change the order of the above configurations; that is, configure the "size" command first and then configure the "stacktrace" command.

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen sometime after having leaked all the processor memory. This causes the router to reload.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCti55261

  Symptoms: On a phone button that has an overlay with call waiting DNs configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

  Conditions: The symptom is observed on a phone button that has an overlay with call waiting DNs and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti62226

  Symptoms: Voice port(s) that are created with PRI/ds0 configurations are active even after shutting down those ports. Because of this, unconfiguring PRI/ds0 configurations throws an error.

  Conditions: The symptoms are observed with Cisco IOS Release 15.0(1)M3 when shutting down the voice-port to unconfigure the controllers.

  Workaround: Do **no shut** first then **shut**.

  Further Problem Description: If you are running a script for regression which cannot be changed there is no workaround. If it is a user interactive case, the above workaround may help.

- CSCti72836

  Symptoms: The router crashes when removing an ACL.

  Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hashtable.

  Workaround: There is no workaround.

- 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.

- CSCti87502

  Symptoms: CP Express does not launch. A blank or garbage characters appear in the browser.

  Conditions: This symptom is observed when attempting to launch CP Express.

  Workaround: A power cycle fixes the issue temporarily.

- CSCti90602

  Symptoms: The PPTP connection is not getting established when “ip nat outside” is configured on the NAT router. The NAT router is between the client and the server.

  Conditions: This symptom is observed only with the PPTP connection; all other traffic works fine.

  Workaround: There is no workaround.

- CSCti93398

  Symptoms: A Cisco 1861 router reloads.

  Conditions: The reload occurs upon booting.

  Workaround: There is no workaround.

- CSCti96028

  Symptoms: A build failure is seen due to the fix committed using CSCti67511 (“Borghetti DSL PHY Firmware upgrade through usb flash”).

  Conditions: When you try to build Cisco 180x platform IOS images.

  Workaround: There is no workaround.

- CSCti98219

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat.

- CSCti99419

  Symptoms: An HWIC-1DSU-T1 card is not recognized after a reload.

  Conditions: This symptom is observed on an HWIC-1DSU-T1 card after a reload. It occurs only about 1 to 2 percent of the time.

  Workaround: Power-cycle the router.

- 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.

- CSCtj07885

  Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the ccmeActiveStats MIB.

  Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with “srst mode auto-provision none”, when interworking with SNMP, using the MIB browser query ccmeActiveStats.

  Workaround:

  1) Configure CME-as-SRST with “srst mode auto-provision all”.

  2) Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:

  a) Stop the MIB on the NMS device that is doing the polling.

  b) Turn off SNMP polling on the device.

  c) Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj35792

  Symptoms: The onboard GE on a Cisco 3900 (driver PQ3_TSEC) with “media-type sfp” goes to 1000/HD when it is connected by fiber to a gig port that is not doing autonegotiation.

  Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation.

  Workaround: Configure autonegotiation on the other side, if possible.

  The Cisco 3945-E does not have this problem.

  Further Problem Description: It is impossible to disable autonegotiation on the Cisco 3900 because of CSCth72105.

- CSCtj53407

  Symptoms: When WAN interfaces of 860, 880, and 890 are configured for fixed speed/duplex settings (100/full, 100/half, 10/full, 10/half), the link goes down. Autonegotiation works fine.

  Conditions: Both the ends of the link should be configured for fixed speed/duplex settings.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.0(1)M3

Cisco IOS Release 15.0(1)M3 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M3 but may be open in previous Cisco IOS releases.

- CSCsk55161

  Symptoms: Cisco IOS XE software crashes when enabling multicast feature of scaled-up config:

  Conditions: This symptom is observed if the configuration has more than 4000 VLANs on Port Channel configured, and all VLANs have V6 configuration and multicast is enabled on each of them at once.

  Workaround: There is no workaround.

- CSCsl64247

  Symptoms: Router crashes 20 to 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.

- 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.

- CSCsu31853

  Symptoms: TCP sessions in TIMEWAIT state cause buffer usage until they move to CLOSED state.

  Conditions: This symptom is observed with almost all TCP applications. It is mainly seen on low end switches.

  Workaround: There is no workaround.

- CSCsv97424

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

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

  Frequency: Always.

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

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

- 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.

- CSCsz70049

  Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the telco side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

  Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

  Workaround: Issue the **clear interface bri** command to restore this state.

- 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** command 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 listens 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 a customer environment.

- CSCta36701

  Symptoms: Group member with VSA runs out of memory and starts dropping traffic with continuous traffic for 12 hours.

  Conditions: The packet size of the traffic sent is near the MTU so that the packets are fragmented before encryption. Crypto map on multilink interface with VSA as the crypto engine will cause a memory leak for every packet decrypted.

  Workaround: Disable VSA.

Note This is specific to crypto map on multilink interface with VSA as the crypto engine. This is not specific to GETVPN config.

- 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 under the following conditions:

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

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

  1. OSPF routing protocol is enabled on all the networks in the topology.

  2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99).

  3. MDT default is configured on all the mVRFs on the PE routers.

  4. PE routers have an iBGP session, ONLY with the RR (route-reflector).

  5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes.

  6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes.

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

  On PE and RR routers:

  1. IGP states = 100 OSPF routes.

  2. BGP states = 200,010 VPNv4 routes.

  On PE routers *only*:

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

  2. MDT sessions = 100 SSM sessions.

  Workaround: There is no workaround.

- CSCta59045

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

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

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

- CSCtb11373

  Symptoms: Enabling IPv6 inspection debugs may lead to a Cisco router crash when traffic is passing through the device.

Conditions: This symptom is observed in Cisco IOS Release 12.4(21) with the following debug commands:

- **debug ipv6 inspect tcp**
- **debug ipv6 inspect detailed**
- **debug ipv6 inspect events**

Workaround: Do not use the above IPv6 inspection debug commands.

- CSCtb29754

  Symptoms: After an SSO switchover, VC does not come up.

  Conditions: HA switchover.

  Workaround: There is no workaround.

  Further Problem Description: The VC that is transported over TE tunnel does not come up after SSO switchover even though the VC is UP before the switchover.

- CSCtb36521

  Symptoms: A Cisco Catalyst 6500 may stop processing IKE traffic, which results in IPSec tunnels not working. Under extreme circumstances, system IO memory might become completely depleted, at which point all traffic processing will stop.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 with a VPN-SPA module running a Cisco IOS SXH image when PKI infrastructure is used to authenticate IKE peers. The certificate in use must contain a CDP that uses HTTP protocol to retrieve the CRL. Revocation-check must be configured to fetch the CRL using the **revocation-check** *crl* or **revocation-check** *crl none* command.

  Workaround: Disable CRL validation by using the **revocation- check** *none* command instead of the **revocation-check** *crl* or **revocation-check** *crl none* commands in the trustpoint being used. Note that disabling CRL validation poses a possible security risk.

  Alternate Workaround: Create a certificate map tied to the trustpoint in use to override the CDP using a URL which specifies the IP address of the CDP server instead of a name.

- 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.

- CSCtb69859

  Symptoms: A Cisco router may crash with the following traceback: 0x40A0D7E8 0x40A0C870 0x409D4DC4 0x4098E0AC 0x42655B74 0x40E3CE4C 0x40E3D634 0x40E3DAB8 0x40974B78 0x40974B5C

  Conditions: This symptom is observed while configuring a DHCP address pool using the **ip dhcp pool** *TAL_DHCP_vrf_pool* command.

  Workaround: There is no workaround.

- CSCtb73450

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

  Conditions: This symptom occurs when the SCCRQ packets are sent with a wrong hash.

Workaround: There is no workaround.

- CSCtc11110

  Symptoms: System take exception.

  Conditions: Web Write Housekeeping process depleted its stack space. This can happen after configuration or after system bootup.

  Workaround: There is no workaround.

- CSCtc12002

  Symptoms: An NM-1A-OC3-POM can not achieve line rate. Router performance degradation is observed.

  Conditions: The symptom is observed with an NM-1A-OC3-POM module on a Cisco 3945 router. The performance degradation issue is observed for OC3 module while trying to reach OC3 line rate with small size (64Bytes) bi-directional traffic streams. Non-drop rate and CPU utilization performance is degraded due to this issue.

  Workaround: Avoid touching line rate with small size bi-directional traffic streams (uni-directional traffic can touch line rate without any problem).

- CSCtc40477

  Symptoms: A Cisco router may crash after disabling then re-enabling NBAR on an interface.

  Conditions: This symptom is observed when policy-map classification based on NBAR and NAT is configured on the router.

  Workaround: Create a dummy subinterface and enable NBAR using the **ip nbar protocol-discovery** command.

  Alternate Workaround: While migrating on the subinterface, disable NBAR using the **no ip nbar protocol-discovery** command on the old interface only after enabling NBAR on the newly-migrated interface.

- CSCtc59535

  Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

  Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

  Workaround: Unplug and plug back the cable.

- CSCtc68910

  Symptoms: Unnecessary retransmission and spurious TCP is reset.

  Conditions: The symptom is observed when using NAT and a large (already fragmented) “updatecabilitiesversion2” traverses the router.

  Workaround: There is no workaround.

  Further Problem Description: This problem seems to be correlated to: IP phone presents an updatecabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtc86075

  Symptoms: A router crashes when the **show aaa user all** command 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.

- CSCtc87699

  Symptoms: Conference bridge calls fail - no audio.

  Conditions: VRF is enabled on interface.

  Workaround: Disable VRF or upgrade the Cisco IOS software.

- CSCtc90779

  Symptoms: A router may crash after displaying align fatal errors pointing to PPPoE functions.

  Conditions: The symptom is observed on a Cisco 7206VXR router (NPE-G1).

  Workaround: There is no workaround.

- CSCtd32975

  Symptoms: On a Cisco 10000 series router with PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and ISG, the memory on the standby RP may become severely fragmented.

  After an SSO switchover, the new-active RP initially takes over with fragmented memory causing frequent malloc errors and eventually requiring a reload to recover.

  Conditions: The symptom is observed on a Cisco 10000 series router with PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and with 10K ISG sessions in a mix of web-login, TAL, prepaid, and passthrough.

  Workaround: Reload will recover memory.

- CSCtd33794

  Symptoms: VC will be UP, but ping will fail. Interface Drop counters (CRC error counter) will increase incrementally as you keep pinging.

  Conditions: The symptom is observed after a reload.

  Workaround: There is no workaround.

- CSCtd47338

  Symptoms: The following error message is constantly displayed:

  ```
  crypto_engine_ps_vec(): no subblock attached
  ```

  Conditions: This issue is observed on a Cisco 7200 series router with VSA cards, that is running Cisco IOS Release 12.4(15)T (other releases may be affected as well) and with DLSw configuration.

  Workaround: Configure the **dlsw udp-disable** command.

- CSCtd50195

  Symptoms: Pings fail when adding two member links one by one.

  Conditions: Configuring one multilink PPP member, checking it, and then adding the second member will bring the second member down, and pings will also fail.

  Workaround: Add two or more multilinks simultaneously.

- CSCtd73923

  Symptoms: RSA keys cannot be added to or removed from a token on a Cisco router.

  Conditions: This symptom is observed when the **crypto key zeroize rsa** command is entered. The command does not remove the keys, and a “no available resources” message is displayed. Keys cannot then be added to or removed from the token.

  Workaround: There is no workaround.

- CSCtd87788

  Symptoms: 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 unchannelized mode is added to multilink.

  Workaround: Reload the box to bring up the interface.

- CSCtd90367

  Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

  Workaround: There is no workaround.

- CSCtd92028

  Symptoms: The router reloads.

  Conditions: The symptom is observed when a VRF is unconfigured while there are one or more WCCP service groups configured with that VRF.

  Workaround: Unconfigure the relevant WCCP service groups prior to unconfiguring the VRF.

- CSCtd94789

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

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

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

- CSCtd97164

  Symptoms: LLQ packet drops on an ATM interface.

  Conditions: The symptom is observed when having QoS under an ATM interface. Packet drops are seen under a class with “priority” even though they have not reached the value configured. It does not matter if it is percent or absolute value.

  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.

- CSCte07862

  Symptoms: DSP crashes due voice card shutdown, with an intermittent CPHI error.

Conditions: The symptom is observed when the phones are connected to PBX. Users dial 5XXXX from the phone. The pattern then changes to 895XXX between PBX and the Cisco router. Over the IP, the call is transferred to 2821 voice card gateway where there is another PBX.

Workaround: There is no workaround.

- CSCte10790

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

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

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

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

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

  no 110
  no 120
  no 130

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

  120 ACE
  130 ACE
  CRASH will happen

  Follow the same order:

  ip access-list extended vlan959-out
   permit ip 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.

- CSCte17284

  Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.

  Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a web page through the SSL VPN with a URL longer than 1009 characters long.

  Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.

- CSCte38855

  Symptoms: Chunk leak is seen after exec-timeout expires.

  Conditions: The symptom is observed after the **interface range** command is configured and when the console timeout expires.

  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.

- CSCte41410

  Symptoms: TCP connections may get stuck when using SSLVPN with **webvpn cef** configured. These connections will be stuck in TIMEWAIT state and will not timeout after the usual minute or so and will stay around forever.

Conditions: This symptom occurs when using SSLVPN with **webvpn cef** configured.

Workaround: Issue the **no webvpn cef** command.

- 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.

- CSCte49283

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

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

  Workaround: There is no workaround.

- CSCte52369

  Symptoms: On a Cisco ASR 1000 router, RADIUS will send a NACK for the first COA request message, and RADIUS authentication will fail.

  Conditions: This symptom is observed when RADIUS recieves “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.

- CSCte54807

  Symptoms: Configuring PVC with Cisco IOS Release 15.0(1)M1 brings up a virtual-access interface, right after sending the ConfReq, even if there is no reply.

  Conditions: The symptom is observed when using a PPPoA setup on Cisco IOS Release 15.0(1)M1. It is seen only if some unused ATM PVCs are present at one end with the PPP configurations applied on them.

  Workaround: Use Cisco IOS Release 12.4(24)T2.

- 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.

- CSCte61495

  Symptoms: The following messages are seen with tracebacks:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process
  = Exec. %SYS-2-INTSCHED: 'suspend' at level 3 -Process= "Exec", ipl= 3, pid= 128,
  ```

  Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

  Workaround: Use small sized ACLs for the service-policy.

- 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").

- CSCte64544

  Symptoms: Calls fail following hook flash on a T1-CAS circuit.

  Conditions: The symptom is observed following outbound calls over a T1-CAS E&M, and after a hookflash.

  Workaround 1: Reorder circuits in CUCM RG.

  Workaround 2: Perform a shut/no shut on the T1-CAS controller.

- 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.

- CSCte76513

  Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

  ```
  %FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between zones
  with ip ident 0
  %FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan class
  admin due to Invalid Flags with ip ident 0
  ```

  Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

  Workaround: There is no workaround.

- CSCte76760

  Symptoms: A router acting as a voice gateway may unexpectedly reload due to bus error.

Conditions: The symptom is observed when the gateway is experiencing a low memory problem leading to seeing SYS-2-MALLOCFAIL errors.

Workaround: Resolve the low memory problem.

- 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.

- CSCte82917

  Symptoms: On a Cisco 7600 series RSP720, the **show proc cpu sort** command displays a CPU utilization of 0, but the per-process CPU utilization is 100% for some processes; no packet loss occurs, however.

  Conditions: This symptom is observed under the following conditions:

  - The router has recently loaded.
  - HSRP is enabled in an HA environment.
  - A large number of HSRP sessions are established.

  Workaround: Reduce the number of HSRP sessions to only a few. The router does not see any performance or functional impact. This is an issue only with internal CPU accounting.

- CSCte83779

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.

  Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for Cisco ASRs.

  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.

- CSCte89436

  Symptoms: A router crashes.

  Conditions: The symptom is observed when the encapsulation is changed from "frame-relay" to "hdlc."

  Workaround: There is no workaround.

- CSCte91471

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

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

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

- CSCte96453

  Symptoms: Switch intermittently crashes when configuring energywise features.

  Conditions: The symptom is observed when the port is configured with “energywise level 10” to bring up a previously down port.

  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.

- CSCte98702

  Symptoms: When using NAT, “%SYS-3-INVMEMINT” and “%SYS-2-MALLOCFAIL” are printed to the console and no traffic passes.

  Conditions: The symptom is observed when NAT is configured.

  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.

- CSCtf04954

  Symptoms: When the **cns config notify** command exists, some CLIs might misbehave or cause unexpected crashes during the configuration change.

  Conditions: The symptom is observed with the **cns config notify** command.

  Workaround: Remove all **cns config notify** commands from the configuration.

- CSCtf08864

  Symptoms: Incoming ISDN T1/E1 PRI voice calls may disconnect or fail to complete properly. When an incoming call is made, the following symptoms may be noticed in the output of debug isdn q921 and/or debug isdn q931:

  – Q.921 debugs may report “**ERROR**: L2_AdvanceVA: TX_ack_queue empty,” after which the B-channel used for the call attempt locks up. The ISDN provider needs to reset the B-channel in order to return it to service.

- Q.931 debugs may show that a voice call disconnected prematurely.
- Q.921 debugs may intermittently duplicate messages such as Receiver Ready (RR) Polling exchanges, Info frames, or SABME frames.

Conditions: The symptom is observed on a Cisco ISR G2 2900/3900 Voice Gateway which has been installed with a VWIC2 T1/E1 MultiFlex Trunk card, configured for ISDN PRI voice services, and running a Cisco IOS 15.0 or 15.1T release. The following conditions are observed:

- The VWIC2 generation of T1/E1 MultiFlex Trunk cards must be used.
- This is a problem affecting PRI voice installs. Data PRI installs are not affected.
- This is an ISR G2 2900/3900 platform-specific issue.

Not all PRI voice installs will be affected by this problem. It depends on how HDLC is configured on the PRI lines by the provider. To be specific, if the provider sends marks (all-ones) instead of HDLC flags during idle times, the call completion problem may manifest itself. Most provider installations are not configured this way and the provider may be able to switch the method of indicating an idle.

Workaround 1: Ask the service provider to send flags between frames instead of idle marks. Idle marks (11111111) may be sent to fill the gap between useful frames. Alternatively, a series of flags (01111110) may be transmitted to fill gaps between frames instead of transmitting idle marks. Continuous transmission of signals is required to keep both the transmitting and receiving nodes synchronized.

Workaround 2: If Workaround 1 is not possible, a Cisco IOS image with a candidate fix is available. The candidate fix has a high confidence level of resolving the PRI voice call issues described above, and has proven to be successful in several field deployments complaining of similar call problems. Please contact the Cisco Technical Assistance Center (TAC) for details on obtaining the candidate fix.

- CSCtf13014

  Symptoms: A DNS server on a router does not immediately serve its own primary zone, if next-layer DNS servers are configured (every query is forwarded to these servers first).

  Conditions: The symptom is observed when next-level (parent) DNS servers are configured on the router.

  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.

- CSCtf18077

  Symptoms: A CME router may unexpectedly reload due to a bus error when a Cisco Unified Contact Center Express (UCCX) unregisters from the CME.

  Conditions: The symptom is observed when the Cisco UCCX unregisters from the CME.

  Workaround: There is no workaround.

- CSCtf19461

  Symptoms: IP address is not leased out to the client from server.

Conditions: The symptom is observed when configuring the VPN sub-option at the interface level on the relay.

Workaround: There is no workaround.

- CSCtf21254

  Symptoms: WAAS communicates with the peer WAAS device in various states:

  1. Active client connections.

  2. Stale client connections.

  3. Its own connections.

  Zone-based Firewall (ZBFW) cannot inspect optimized/compressed WAAS traffic and hence allows such traffic to be bypassed in all the above states.

  Conditions: The symptom is observed with ZBFW.

  Workaround: There is no workaround.

- CSCtf25293

  Symptoms: SSH connection to a SSH server aborts abruptly after making the connection, while using public key-based authentication.

  Conditions: Authentication method used must be public key.

  Workaround: Use kbd-interactive or password-based authentication.

- CSCtf27303

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

  Conditions: The symptom is observed under the following conditions:

  - Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.
  - Third-party: only capability IPv6 labeled unicast advertised.

  Workaround: There is no workaround.

- CSCtf27324

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

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

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

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

- CSCtf31067

  Symptoms: There is no implementation for retransmitting MS-CHAP v2 challenge for PPP negotiation.

Conditions: The symptom is observed with a MS-CHAP v2 challenge.

Workaround: There is no workaround.

- CSCtf36117

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

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

  Workaround: There is no workaround.

- 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.

- CSCtf40425

  Symptoms: When executing the **service-module** *interface* **install** command on an SRE module on a Cisco Integrated Services Router (ISR) G2, the router may unexpectedly reload due to a bus error.

  Conditions: The symptom is observed only when executing the install on an SRE module.

  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.

- CSCtf47335

  Symptoms: Wrong typedef version is returned.

  Conditions: The symptom is observed on getTypedefs CT; the typedefVersion returned is “2008-08-01.” This is the wrong version with some undefined entries. Due to this, the signature parsing is failing in CCP.

  Workaround: There is no workaround.

- CSCtf47396

  Symptoms: A Cisco router may crash when a service-policy configured with bandwidth is removed from an interface.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCtf47929

  Symptoms: Tracebacks are seen on the router when creating a udp-jitter operation with a request-data size of more than 17,000 bytes (super jumbo packet).

  Conditions: This symptom is observed only when a large request data size is used.

  Workaround: Use a request data size that is less than 17,000 bytes.

- 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.

- CSCtf51690

  Symptoms: Router crashes when a packet with out-of-bound featureIndex values is sent to the CME.

  Conditions: The symptom is observed when malformed packets are sent to the CME with out-of-bound featureIndex values in fStationFeatureStatReqMessage.

  Workaround: There is no workaround.

- CSCtf52106

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

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

  Workaround: There is no workaround.

- CSCtf57641

  Symptoms: A router crashes after performing a DNS lookup.

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

  Workaround: Configure “no ip domain-lookup.”

- CSCtf62621

  Symptoms: Unable to push the firewall down to the VDSL chipset on a Cisco 887V modem.

  Conditions: The symptom is observed on a Cisco 887V router with no startup configuration in NVRAM.

  Workaround: Perform a **write memory** and reload the router.

- CSCtf67170

  Symptoms: There is a crash due to the following error:

  ```
  %ALIGN-1-FATAL: Illegal access
  ```

  Conditions: The symptom is observed when “call monitor” is configured.

  Workaround: Remove call monitor, if interfacing with UCCX is not needed.

- CSCtf68941

  Symptoms: BR router crashes.

  Conditions: When NBAR-based control is enabled, the BR router crashes due to fib invalid ptr.

  Workaround: There is no workaround.

- CSCtf70959

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

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

  Workaround: Use a non profile-based dialer interface.

- CSCtf71010

  Symptoms: Traffic does not flow through the hub.

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

  Workaround: There is no workaround.

- CSCtf71990

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

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

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

  Workaround: Remove “source-ip-address.”

- 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.

- 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.

- CSCtf78370

  Symptoms: A watchdog timeout exception occurs during a warm reload.

  Conditions: A watchdog timeout exception occurs during a warm reload.

  Workaround: Set the configreg to reload Cisco IOS software from ROMMON.

- CSCtf81271

  Symptoms: When “station-id name” or “station-id number” is configured on a voice port, “caller-id enable” will also be configured on that voice port.

  Conditions: The symptom is observed after upgrade to Cisco IOS Release 12.4(22)T or Release 12.4(24)T where the **caller-id enable** command gets auto-configured on the voice-port.

Workaround: Manually remove the **caller-id enable** command after a router reboot.

- 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.

- CSCtf83101

  Symptoms: Packets are not correctly classified by QoS class-map in CEF switching. Priority packets are dropped even if they are classified into LLQ. This is shown by the **show policy-map interface** command.

  Conditions: The symptom is observed under the following conditions:

  – A BRI interface.

  – LLQ is configured on egress port by policy-map.

  – The following devices/platforms are used: HWIC-4B-S/T or HWIC-1B-U, Cisco 181x, Cisco 180x, Cisco 800.

  Workaround: Disable CEF.

  Alternate Workaround: Use the other HWIC or WIC.

- 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.

- CSCtf84393

  Symptoms: Gateway is unable to place outbound calls out of BRI port when his MGCP gateway is in SRST mode. Call disconnects with cause value = 63 (service/option not available).

  Conditions: Cisco IOS of 880 - appears on 12.4(20)T4, 12.4(24)T2, and 15.0(1) SPSERVICES

  Workaround: There is no workaround.

  Other:

  debugs - call drops with vtsp ---- : //21/B05794988024/VTSP:(4):-1:1:1/vtsp_request_call: CALL_ERROR; Unable to Send Setup Request Return Code=-5, Cause Value=63 : //21/B05794988024/VTSP:(4):-1:1:1/vtsp_cc_call_disconnected: : //21/B05794988024/VTSP:(4):-1:1:1/vtsp_cc_call_disconnected: Cause Value=63

- CSCtf85219

  Symptoms: The following symptoms are seen:

  – No dial tone when going off hook, so other phone numbers cannot be dialed.

  – The hung port can receive incoming calls; however the originating phone hears ring back. The terminating phone rings, but when the call connects there is one-way audio.

Conditions: The symptom is observed with STCAPP-controlled FXS ports.

Workaround: Perform a shut/no shut on the voice port. If this does not work, perform a reload.

- CSCtf86556

  Symptoms: The middle router crashes when it receives a PathTear message.

  Conditions: The symptom is observed when the middle router (that does not have SREFRESH configured) receives a PathTear message, when the session debug is on.

  Workaround: Disable the session debugs.

  Alternate Workaround: Configure refresh reduction on the UUT.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

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

  Workaround: There is no workaround.

- CSCtf91428

  Symptoms: Router crashes in IP Input.

  Conditions: NAT is configured.

  The customer who reported the crash was using bit torrent when it crashed.

  The public interface was an ATM (DSL).

  Workaround: Disable ip nat service for h232 - rass. Disable CEF globally.

- CSCtf96538

  Symptoms: ATM interface does not pass/receive traffic. The configuration on the ATM interface shows “atm scrambling cell-payload” configured, but the **show controller ATM** command output shows “DS3 Scrambling OFF.”

  Conditions: The symptom is observed on a Cisco 3925 router, with an NM-1A-T3/E3 and running a Cisco IOS 15.0 release.

  Workaround: Disable scrambling on the network.

- CSCtf97322

  Symptoms: On Cisco 2900 and 3900 series routers, routers shaping is not working correctly when using one of the following serial modules: HWIC-1T, HWIC-2T, HWIC-4T, HWIC-1DSU-T1. An additional symptom on the Cisco 2900 series routers is the possibility of alignment errors and in rare situations a software-forced crash.

  Conditions: It does not drop traffic above the shape amount.

  Workaround: There is no workaround.

- CSCtg02719

  Symptoms: Informers reload.

  Conditions: The symptom is observed when enabling the **voice dsp crash-dump** or **debug vpm dsp** commands. These two commands may cause Informers to reload.

  Workaround: Do not enable the **voice dsp crash-dump** or **debug vpm dsp** commands on Informers.

- CSCtg05569

  Symptoms: Tracebacks are observed while reloading the router.

Conditions: This symptom is observed on a Cisco AS5400XM that is running Cisco IOS Release 15.1(1.9)T.

Workaround: There is no workaround.

- CSCtg06863

  Symptoms: The **show processes cpu sorted** command will incorrectly show processes with CPU utilization of 100 percent. Also, CPU utilization will vary randomly.

  Conditions: The symptom is always observed when traffic is flowing through the router and may or may not be seen without traffic flowing.

  Workaround: There is no workaround.

- CSCtg07557

  Symptoms: A reload of a Cisco 1941W-A/K9 causes the embedded AP 801 to go to ROMMON. The AP BOOT parameter is no longer set and the startup configuration is also erased.

  Conditions: The symptom is observed when a reload is issued on the router and you reload the AP at the same time when prompted.

  Workaround: When reloading router using CLI, answer “no” when prompted to reload the embedded AP. The embedded AP can be reloaded with the **service-module wlan-ap 0 reload** command from router console or the **reload** command from embedded AP console accessed via **service-module wlan-ap 0 session**.

- CSCtg11186

  Symptoms: A router may face a watchdog crash or hang while removing a port-channel.

  Conditions: The symptom is observed with a Cisco 3900/2951 router when removing a port-channel interface. It is seen when PPPoE is enabled on the GE interface.

  Workaround: There is no workaround.

- CSCtg13758

  Symptoms: Router can crash due to corrupted magic value in freed chunk.

  Conditions: The symptom is observed on a Cisco 881 router that is running Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCtg19546

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

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

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

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

- CSCtg19972

  Symptoms: Cisco 1811 running 150-1.M2 can reload due to IO memory corruption when enabling first nbar protocol-discovery as well as “ip pim sparse-dense-mode” on DMVPN/GRE tunnel Tunnel 0.

  Conditions: As soon as multicast traffic starts passing on DMVPN tunnel, the device will reload due to IO memory corruption.

  Workaround: There is no workaround.

  Release note will be updated as progress is made on this issue.

- CSCtg20254

  Symptoms: Router crashes.

  Conditions: The symptom is observed when “debug glbp event” is turned on.

  Workaround: There is no workaround.

- CSCtg20590

  Symptoms: A router may take a very long time to reload because it is printing too much crash information to the console.

  Conditions: This symptom is observed only for crashes during system init.

  Workaround: Resolve the crashes during system init. This is most often related to the router not having enough memory. You can perform disaster recovery by breaking into rommon during bootup and changing the config-register to ignore NVRAM or boot an image with smaller memory requirements.

- CSCtg23251

  Symptoms: Analog phones lock up and there is no dial tone.

  Conditions: The symptom is observed when the CME is in fallback as SRST and a directed call park is attempted on analog phones. The user cannot pick up a call from a park slot by direct dialing the slot. In the event that the user is able to retrieve the call, when the call is hung up the channel is not released. No dial tone is heard when the handset is picked up again.

  Workaround: Reset the ports.

- CSCtg28806

  Symptoms: A router crashes at PKI manual enroll.

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

  Workaround: There is no workaround.

- CSCtg38344

  Symptoms: Upon a reload, a router may lose most of its configuration after the pubkey-chain user/server sub-mode is gone. The following error is reported during the reboot:

  ```
  Installed image archive Cisco 1841 (revision 5.0) with 237568K/24576K bytes of memory.
  Processor board ID 6 FastEthernet interfaces 2 Virtual Private Network (VPN) Modules 2
  802.11 Radios DRAM configuration is 64 bits wide with parity disabled. 191K bytes of
  NVRAM. 62720K bytes of ATA CompactFlash (Read/Write)
  bridge irb ^ % Invalid input detected at '^' marker.
  interface FastEthernet0/0 ^ % Invalid input detected at '^' marker.
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 15.0(1)M2 with “ip ssh pubkey-chain” configured.

Workaround: Remove the SSH keys before upgrading to Cisco IOS Release 15.0(1)M2 or Release 15.1(1)T.

- 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.

- CSCtg41232

  Symptoms: Traffic, set to be exempted from inspection via an extended ACL, is still inspected even though the ACL registers counts for that traffic.

  Conditions: The symptom is observed on any Cisco access router that is running Cisco IOS 15.x code.

  Workaround: There is no workaround.

- CSCtg41733

  Symptoms: Certain crafted packets may cause memory leak on a Cisco IOS router.

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

  Workaround: Disable SIP if it is not needed.

- CSCtg44108

  Symptoms: Frequently recurring bus error crashes on a Cisco 3945e that is running c3900e-universalk9-mz.SPA.151-1.T

  ```
  System returned to ROM by bus error at PC 0x45C1498, address 0x45C1498
  ```

  This symptom was seen initially on a Cisco 3945e but may be seen on other platforms.

  Conditions: Configuration has IPsec configured on a GRE multipoint tunnel interface.

  Workaround: There is no workaround.

- CSCtg45905

  Symptoms: c18xx & c3270 builds failed.

  Workaround: There is no workaround.

- CSCtg50024

  Symptoms: Router experience crashes due to TLB (load or instruction fetch) exception.

  Conditions: Problem was observed on a Cisco 7206vxr.

  Workaround: There is no workaround.

- CSCtg55447

  Symptoms: GETVPN key server TEK sequence number goes out of synch during network split/KS failure. This causes the GM to reject the older key and re-register.

  Conditions: Primary key server failure or network failure between Primary KS and Secondary KS.

  Workaround: There is no workaround.

- CSCtg57623

  Symptoms: Music on hold does not work with iLBC codec when A Cisco IOS transcoder is used.

Conditions: The symptom is observed when the phone is configured to use iLBC codec and a transcoder is invoked to transcode MOH G.711 audio stream to iLBC codec. The phone rejects the RTP stream due to incorrect payload-type (it sends payload type 118 instead of the correct 116 for iLBC).

Workaround: There is no workaround if iLBC codec is needed, but using a different codec at the remote phone should work.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This symptom has been seen on a Cisco 7206VXR router.

  Workaround: There is no workaround.

- CSCtg57831

  Symptom: In some events, we wrongly increment the last issued serial number, resulting in serial number mismatch on the active and standby.

  Conditions: This symptom is observed in a High Availability CA server environment, using Cisco IOS Release 15.0(1)M2.

  Workaround: There is no workaround.

- CSCtg63096

  Symptoms: “deny ip any any fragments” shows a high number of hits for traffic that may not be truly fragmented.

  Conditions: “deny ip any any fragments” may be configured at the top of the ACL.

  Workaround: There is no workaround.

- CSCtg63942

  Symptoms: The output of the **show process cpu sorted** command is not proper. It shows some wrong values like “CPU utilization for five seconds: 0%/43%; one minute: 7%; five minutes: 3%.”

  Conditions: None.

  Workaround: There is no workaround.

  Further Problem Description: As it shows wrong values at **show process cpu sorted** for 5 seconds, it is showing 0%/43%. This is incorrect because the total CPU is the sum of the process-level and interrupt-level CPUs.

- CSCtg67425

  Symptoms: A router crashes at fr_vcb_dlci_status_change.

  Conditions: Removing Frame Relay encapsulation in a router that has T3 interfaces leads to the crash.

  Workaround: Remove all the PVCs that are configured under an interface before changing/removing Frame Relay encapsulation.

- CSCtg68208

  Symptoms: A router may repeatedly reload when an L2TPv3 xconnect configuration is present and there is no interface configured with an IP address.

  Conditions: This symptom has been observed when the **xconnect** command specifies **encapsulation l2tpv3**, and all interfaces on the router are either configured with **no ip address** or **ip address dhcp**.

  Workaround: To avoid this problem, ensure there is an interface which is able to reach the L2TPv3 peer and which has an IP address configured.

- CSCtg73604

  Symptoms: E1R2 compelled signaling calls fail.

  Workaround: There is no workaround.

- 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 symptom is observed 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.

- CSCtg79262

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

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

  Workaround: The only way to recover is to reload.

- CSCtg86714

  Symptoms: The **show cellular 0** command might not show any output.

  Conditions: The symptom is observed with the **show cellular 0** command.

  Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg88766

  Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

  Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

  Workaround: There is no workaround.

- CSCtg93243

  Symptoms: While testing a customer scenario, it was noticed that QoS+tunnel protection does not work if UUT2 is running VSA. Packets after being decrypted by VSA are dropped at UUT2.

  Conditions: Upon investigation, problem was isolated to crypto and to tunnel protection and VSA only.

If static crypto + VSA or tunnel protection + SW crypto is used, packets are forwarded after decryption as expected.

Cisco ASR is running MCP Dev RLS7 image, and Cisco 7200 is running 15.0 mainline image.

Workaround: There is no workaround.

- CSCth01939

  Symptoms: IPSEC packets are dropped on the router, and an error is displayed on the console.

  Conditions: This symptom is observed on a Cisco IAD2430 with VPN/GRE tunnel configuration and AES256 encryption.

  Workaround: There is no workaround.

- CSCth04193

  Symptoms: Router crashes @cce_dp_named_db_http_free_token_info.

  Conditions: Zone Based Firewall is configured to inspect HTTP or SIP traffic.

  Workaround: Do not use deep packet inspection.

- CSCth15518

  Symptoms: Ping through ISDN BRI interface fails.

  Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

  Workaround: There is no workaround.

- CSCth16382

  Symptoms: A cce-dp crash is observed @cce_dp_results_get_class_group_element.

  Conditions: Load the configurations and run the traffic, and wait for some time. And then:

  1) Router will crash by itself without doing anything while traffic is flowing.

  2) Sometimes. Just reload the router and you see the crash.

  Workaround: There is no workaround.

- CSCth29105

  Symptoms: On Cisco ISR G2 products—only on the Cisco 2901, 2911, and 2921—occasionally the SYSTEM LED will be OFF even when the router is operating normally.

  Conditions: There are no specific conditions that trigger this issue. The problem happens randomly.

  Workaround: There is no workaround. This issue does not affect any of the router functionality.

- CSCth35620

  Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

  Conditions: This symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

  Workaround: There is no workaround.

- CSCth49421

  Symptoms: Tbridge stops working.

  Conditions: When the interface goes to standby from active.

  Workaround: There is no workaround.

- CSCth59217

  Symptoms: Firewall sessions are not seen when ZBFW and gatekeeper are configured on the UUT.

  Conditions: This symptom is observed when ZBFW and gatekeeper are configured on the UUT.

  Workaround: There is no workaround.

- CSCth79353

  Symptoms: A Cisco 3900 series router may experience a software-forced reload when running Cisco IOS Release 15.0(1)M1.

  Conditions: This symptom is observed when the router has a QoS policy attached to one of the LAN interfaces. The QoS policy needs to match different ACLs and have shaping configured.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.0(1)M2

Cisco IOS Release 15.0(1)M2 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M2 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' next hops inaccessible, and those prefixes are not installed in to RIB, therefore traffic is stopped.

  Workaround: There is no workaround.

- CSCsk23520

  Symptoms: One of the below symptoms could be seen because of this defect:

  1. Cisco 720*x* VXR or Cisco 7600 router might crash due to memory corruption or unknown reload cause.
  2. Packet drops with MLP config with following traceback could be seen with below error message:

  `" %PPP-3-MLPFSREENTERED: Multilink fastsend reentered, bundle x (Springfield), packet discarded, "`

  Conditions: The issue would be with Cisco 7200/7600 series installed with any of below Port-Adaptors, under the conditions of heavy traffic, or reload with heavy traffic:

  1. DUAL_HSSI_B (PA-2H)
  2. E3_2PORT (PA-2E3)
  3. E3_1PORT (PA-E3)
  4. T3_2PORT_PLUS (PA-2T3+)
  5. T3_1PORT_PLUS (PA-T3+)

  Workaround: No direct workaround for this issue with the affected PAs.

  HW replacement options are shown below:

  For PA-2T3+, PA-E3, PA-3E3 and PA-T3+, please migrate to PA-2T3/E3-EC or PA-T3/E3/-EC PAs on Cisco 7200 and SPA-4XT3/E3 SPA for Cisco 7600.

  There is no HW replacement for PA-H and PA-2H.

- CSCsu50869

  Symptoms: Calls do not complete because Cisco Unified Border Element (CUBE) does not send PRACKs to all 1xx messages.

  Conditions: This symptom is observed with H.323 slow start to SIP delayed media call flow.

  Workaround: Enable fast start H.323 with an MTP in CUCM, which allows for SIP early offer. Reliable 1xx messaging can also be disabled to prevent the requirement of provisional acknowledgments.

- CSCsx26025

  Symptoms: Wireless clients are not able to ping each other after a few minutes.

  Conditions: Can occur on any of the following routers with 802.11 wireless interfaces: Cisco UC500, Cisco 85x, Cisco 87x, Cisco 1811, and Cisco HWIC-AP.

  Workaround: There is no workaround.

- CSCsx75520

  Symptoms: Ping is not working on a Cisco router with a ctunnel interface.

  Conditions: This symptom is observed after attaching a policy map to a ctunnel interface.

  Workaround: Delete the policy map from the ctunnel interface using the **no policy-map** command and reload the router.

- CSCsx93245

  Symptoms: A Cisco router may reload after the **show gatekeeper zone prefix all** command is entered.

  Conditions: This symptom is observed on a Cisco 3825 router running Cisco IOS Release 12.4(8a).

  Workaround: There is no workaround.

- 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 (>100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- CSCsz83570

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

  Conditions: This symptom is observed when large amounts of data are exchanged between both ends, client and server (for example, 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.

- CSCta20590

  Symptoms: A group member (GM) pseudotime may desynchronize after reregistering or at initial registration.

  Conditions: This symptom is observed when GETVPN with time-based anti-replay (TBAR) is enabled.

  Workaround: Disable TBAR or use a very large window (> 30 seconds).

Further Problem Description: After establishing phase I, the GM is supposed to obtain the KEK and TEKs. If a packet drop occurs (usually, this message is fragmented across multiple frames), then the router is not able to reassemble the packet. IKE will later resend this message, but if the pseudotime has not been recalculated the symptom will reoccur.

- CSCta32825

  Symptoms: A Cisco router may crash with a bus error after configuring a class-map or modifying a class-map.

  Conditions: This symptom is observed when using the **class-map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

```
router(config)#class-map match-any PRIO
router(config-cmap)#match dscp cs4
router(config-cmap)#match dscp cs4 af41
router(config-cmap)#match dscp cs4 af41 af42
router(config-cmap)#match dscp cs4 af41 af42 af43
router(config-cmap)#match dscp cs4 af41 af42 af43 ef
router(config-cmap)#match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here--->
```

  Workaround: Configure QoS changes when no traffic is passing through the router. This symptom has only been seen while traffic is trying to match against the policy while it is being updated.

- CSCta37063

  Symptoms: NAT fails to translate H323 payload information.

  Conditions: This symptom occurs when NetMeeting is dialing from outside NAT to inside NAT.

  Workaround: Initiate NetMeeting again. Note that once this NAT entry is cleared or has timed-out, the issue will reappear.

- CSCta69213

  Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

  Conditions: This symptom is observed on a Cisco router configured for NHRP and DMVPN.

  Workaround: There is no workaround.

- CSCta76251

  Symptoms: VPLS AD may not work after BGP has converged.

  Conditions: This symptom is observed when all of the PE routers are reloaded at the same time.

  Workaround: Configure MPLS IP by entering the **mpls ip** command on one of the tunnel interfaces.

- CSCta93129

  Symptoms: An IP fragment may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

  Conditions: This symptom is observed when encrypted IPSEC packets are fragmented by the remote device (fragmentation after encryption) or somewhere in the network between the VPN termination routers. When the fragmented IPSEC packets are reassembled and decrypted, if the decrypted inner packet is also an IP fragment, the IP fragment bypasses VFR processing. The following conditions may cause this symptom to occur:

  1. VFR is enabled on the decryption side
  2. Fragmentation happens after encryption on the encrypting router, or in the path
  3. The inner IP packet is fragmented when received by the encrypting router.

  Workaround: Perform fragmentation before encryption on the sending side, and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

Further Problem Description: When IPSEC packets corresponding to the first inner IP fragment bypass VFP processing, the second inner IP fragment, even if too small to require IPSEC fragmentation, is decrypted and then sent for VFR processing. Due to the timeout created when the first IP fragment bypasses VFR processing, the second inner IP fragment is dropped.

- 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.

- CSCta98321

  Symptoms: AAA server for HTTP authentication cannot be configured on a Cisco 861 integrated services router (ISR).

  Conditions: This symptom is observed when configuring the AAA server for HTTP authentication on a Cisco 861 ISR.

  Workaround: There is no workaround.

- CSCtb09167

  Symptoms: The following issues can be observed 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.

- CSCtb13421

  Symptoms: The GM may not register on a Cisco ASR 1000 series router.

  Conditions: This symptom is observed when a crypto map with local-address configured is applied on multiple interfaces, and one of these interfaces is then shut.

  Workaround: Disable local-address for the crypto map.

- 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 (in other words, to 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.

- CSCtb17152

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

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

Workaround: There is no workaround.

- CSCtb17856

  Symptoms: H323 calls may intermittently fail with Cause Code 41. After several days and depending on traffic, calls may start failing with Cause Code 47.

  Conditions: This symptom is observed when there is a race condition in setting up an H245 session between H323 peers and two separate H245 sessions are opened simultaneously.

  Workaround: There is no workaround for Cause Code 41. For Cause Code 47, reload the router to temporarily alleviate the symptoms.

- CSCtb21428

  Symptoms: An interface does not attempt to restart after restart-delay is configured.

  Conditions: When the serial interface is down for some reason and you have configured restart-delay on the serial interface, the interface should try to restart.

  Workaround: There is no workaround.

- CSCtb22889

  Symptoms: SIP (TLS--SIP CUBE) may experience up to 2-3 seconds of post-dial delay due to TLS processing. Processing delays of 1000 ms, 600ms, and 200ms are seen between the gateway TLS responses.

  Conditions: This symptom is observed with a TLS connection to another gateway.

  Workaround: Use the **sip-ua timers connection aging tls** *time* command to increase the time in the gateway TLS aging timer and therefore lower the frequency of the problem with the aging TLS timer.

- CSCtb41458

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

  Conditions: This symptom is observed when IPv6 Cisco Express Forwarding (CEF) is enabled, but IPv6 multicast traffic is process-switched on IPv6 RBE interface.

  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.

- CSCtb48397

  Symptoms: A Cisco integrated services router (ISR) may experience performance degradation due to corrupted TCP headers.

  Conditions: This symptom is observed on a Cisco ISR with Cisco IOS Release 12.4 or Release 12.4T running interface-based TCP header compression on any data link. Corrupted TCP headers may occur when all of the following are true:

  1. Frame-Relay, PPP, or HDLC is configured with “ip tcp header-compression”
  2. The queueing mechanism is fair-queue (either interface-based or in map- class frame-relay)
  3. >1 TCP sessions are traversing the compressing mechanism

4. The packets are in the hardware (CEF) switching path.

Workarounds:

1. Do not configure an interface to carry compressed TCP/IP headers using the **frame-relay ip tcp header-compression** command.
2. Disable hardware switching for all interfaces on the Cisco ISR using the **no ip route-cache** command.
3. Do not use any form of fair-queue on interfaces configured with the **frame-relay ip tcp header-compression** command. To remove fair-queue, use the **no fair-queue** command in policy-map class configuration mode.

Further Problem Description: With exactly two MS Remote Desktop Protocol TCP sessions, when the UUT's serial transmit-ring (or frame-relay shaper Bc) congests and the fair-queue invokes, the compressed header from the second- established TCP flow is erroneously written into headers of some packets from the first-established TCP flow, resulting in post-decompression frames erroneously added to the first-established TCP flow and erroneously removed from the second-established TCP flow, thereby causing a performance degradation.

- 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 7206 VXR 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.

- CSCtb64017

  Symptoms: A Cisco router may crash when removing ACL in class map while traffic is flowing.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.0.

  Workaround: There is no workaround.

- CSCtb66295

  Symptoms: No ip connectivity exists due to erroneous ARP tables.

  Conditions: This symptom is observed when NAT and HSRP are configured on the same interface.

  Workaround: There is no workaround.

- CSCtb72550

  Symptoms: Call Detail Record (CDR) files pushed via FTP are not created on the FTP server.

  Conditions: This symptom is observed when the **gw-accounting** *file* command is configured to point to an FTP server.

  Workaround: Push the CDR records locally to the flash instead of to an FTP URL.

- CSCtb81833

  Symptoms: A Cisco router crashes due to a watchdog timeout during interface range port-channel.

  Conditions: This symptom is observed on a Cisco router after entering the **interface range port-channel** command with PPPoE configuration.

  Workaround: There is no workaround.

- CSCtb83578

  Symptoms: A severe memory leak may occur on a Cisco CME router.

Conditions: This symptom is observed on a Cisco CME router with the CCSIP- REGISTER process.

Workaround: There is no workaround.

- CSCtb91992

  Symptoms: A Cisco router may crash with chunk-related errors.

  Conditions: This symptom is observed on a router with IOS IPS configured after several hours of traffic.

  Workaround: There is no workaround, other than removing IOS IPS.

- CSCtc04016

  Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience high CPU utilization, which causes additional calls through the router to fail.

  Conditions: This symptom is observed under rare conditions when SIP- associated processes on the Cisco IOS gateway (as seen when the **show process cpu** command is entered) cause extremely high CPU utilization, which causes further calls through the router to fail.

  Workaround: There is no workaround.

  Further Problem Description: This symptom occurs due to a SIP "491 Request Pending" and ACK loop between the gateway and a third-party device. This loop most often occurs in environments with a large number of SIP REFER transfers. To determine whether the loop is occurring, enter the **show sip statistics** command and look for the RequestPending value; a high and increasing output count could indicate the SIP loop.

- CSCtc12334

  Symptoms: A Cisco 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 when MDT is configured and the **clear ip bgp *** command is entered.

  Workaround: There is no workaround.

- CSCtc17162

  Symptoms: A Cisco router may crash due to a SegV exception.

  Conditions: This symptom is observed on a Cisco 2650XM router running Cisco IOS Release 12.4(15)T10 when VTI is configured inside the EzVPN.

  Workaround: Remove the VTI inside the EzVPN.

- CSCtc18562

  Symptoms: When Network Address Translation (NAT) of the outside source address is enabled, the static route to the local IP address is installed in the global RIB instead of the VRF RIB.

  Conditions: This symptom is observed when enabling NAT of the outside source address using the **ip nat outside source static** *global-ip local-ip* **vrf** *vrf name* **add-route extendable match-in-vrf** command.

  Workaround: Configure a static route within the VRF.

- CSCtc24937

  Symptoms: The **show cellular** command reports no valid statistics with autoconfig enabled.

```
router#sh cellular 0 radio history all
router#show cellular 0 all
```

```
Hardware Information ==================== Modem Firmware Version = Modem Firmware
built = Hardware Version = International Mobile Subscriber Identity (IMSI) = 00000
International Mobile Equipment Identity (IMEI) = Factory Serial Number (FSN) = Modem
Status = Offline Current Modem Temperature = 0 deg C, State = Normal
<..>
Network Information =================== Current Service Status = Normal, Service Error
= None Current Service = Circuit Switched Current Roaming Status = Home Network
Selection Mode = Automatic Country = , Network = Mobile Country Code (MCC) = 0 Mobile
Network Code (MNC) = 0 Location Area Code (LAC) = 0 Routing Area Code (RAC) = 0 Cell
ID = 0 Primary Scrambling Code = 0 PLMN Selection = Automatic Registered PLMN = ,
Abbreviated = Service Provider =
Radio Information ================= Current Band = None, Channel Number = 0 Current
RSSI = -0 dBm Band Selected = GSM 450
Modem Security Information ========================== Card Holder Verification (CHV1)
= Disabled SIM Status = OK SIM User Operation Required = None Number of Retries
remaining = 0
```

Conditions: This symptom is observed on Cisco 881 or Cisco 888 router platforms with a 3G wireless interface.

Workaround: The **test cellular 0 modem-reset** command can be used to reset the modem.

- 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.

- CSCtc28059

  Symptoms: HTTP CORE process might start consuming 99% of a Cisco router’s CPU time.

  Conditions: This symptom is observed on Cisco ISRs running Cisco IOS Release 12.4(24)T1 when IOS content-filtering is active and the reputation server is unreachable (that is, timing out during a three-way handshake of the registration SSL connection).

  Workaround: Disable the URL content-filtering.

- CSCtc32374

  Symptoms: ISDN Layer 1 is deactivated after a reload, and calls fail with a cause code 47 (Resource Unavailable).

  Conditions: This symptom is observed when busyout monitor is configured and the TEI controller comes up before the monitored interface.

  Workaround: Remove the busyout monitor configuration using the **no busyout monitor** command in voice-port configuration mode.

  Further Problem Description: Entering the **shutdown** command followed by the **no shutdown** command will bring the PRI Layer 1 to Active and Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc39592

  Symptoms: Classification is broken on an ATM PVC bundle.

  Conditions: This symptom is observed only when crypto is applied on an ATM PVC bundle.

  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 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.

- CSCtc42734

  Symptoms: A communication failure may occur due to a stale next-hop.

  Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

  Workaround: Reload the router.

- CSCtc46304

  Symptoms: Ping sweep and application-level traffic fail to go through, and connectivity is subsequently lost.

  Conditions: This symptom is observed when BFD and shaping are configured on the SHDSL interface.

  Workaround: After connectivity has been lost, flap the link to restore connectivity.

- 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.

- 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.

- 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.

- CSCtc79670

  Symptoms: A Cisco router crashes @chunk_free_caller and displays the following:

  ```
  chunk name is CCE 7 tuple dy
  ```

  Conditions: This symptom is observed when traffic is running through a router that has been configured with Zone-Based Cisco IOS Firewall.

  Workaround: Remove Cisco IOS Firewall from the router.

- CSCtc97503

  Symptoms: The following error may be seen on the console at bootup:

  ```
  Overly long password truncated
  ```

  Conditions: This symptom is observed when service password-encryption needs to be configured. This is seen only for the ftp password when the password for ftp is 12 characters or longer. It is not a problem for other passwords specified in the configuration.

  Workaround: Use a shorter password.

- 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.

- CSCtd07320

  Symptoms: Spurious memory access and Traceback is seen @ppp_ipfib_install_punt_adjacency.

  Conditions: This symptom is observed when running a conditional debug in a scenario with ISDN and MLP involved.

  Workaround: There is no workaround.

- 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.

- CSCtd22063

  Symptoms: Call-forward busy/all fails with no H.450 forwards.

  Conditions: This symptom is observed on secure IP phones with no H.450 forwards.

  Workaround: Configure with H.450 forwards, or configure no supplementary- service media-renegotiate with no H.450 forwards.

- 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.

- CSCtd26819

  Symptoms: A Cisco AS5400 series gateway does not pass cause code in a Progress message to the Cisco Unified Communications Manager (CUCM); therefore, Dialer cannot correctly categorize invalid numbers.

  Conditions: This symptom is observed on a Cisco AS5400 series gateway, which currently does not have this capability.

  Workaround: There is no workaround.

  Further Problem Description: SIT Detection non-standard SIT tones.

- CSCtd27247

  Symptoms: A Cisco 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.

- CSCtd31084

  Symptoms: GSM-AMR CODEC cannot be disabled on a Cisco MGCP gateway when using iLBC. The CODEC will be selected regardless and then rejected due to lack of license.

  Conditions: This symptom is observed under the following conditions:

  - iLBC is in use
  - GSM-AMR is not licensed for use
  - GSM-AMR is in SDP

  Workaround: Disable CODEC on the gateway CODEC choice list. Note that this option is not always possible.

- CSCtd34887

  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 xx.xx.xxx.xxx
  Outgoing interface list: Null (Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr xx.xx.xxx.xxx
  Outgoing interface list: Null
  ```
  and the following is configured on the interface:

  ```
  int FastEthernet4.3 encapsulation dot1Q 33 ip vrf forwarding management ip address <IP
  addr> xxx.xxx.xxx.xxx ip pim sparse-mode ip igmp join-group <group addr> source
  xx.xx.xxx.xx ip igmp join-group <group addr> source xx.xx.xxx.xx
  ```
  Workaround: Reboot. Reboot does not completely recover SSM VRF mroute entries. Only one of the entries is created. To populate the other entry, enter the **no ip igmp-join** and **ip igmp join** commands on the interface.

- 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 from 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.

- CSCtd43168

  Symptoms: A breakpoint exception crash occurs while configuring SNMP traps via Cisco Works after the following errors are displayed:

  ```
  %SNMP-5-WARMSTART: SNMP agent on host <host name> is undergoing a warm start
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk ########, data ########.
  -Process= "NAT MIB Helper", ipl= 0, pid= 277 -Traceback=
  ```

  Conditions: This symptom is observed after unconfiguring snmp-server, then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

  Workaround: There is no workaround.

- CSCtd44327

  Symptoms: After entering the **clear cry gdoi** command on the GM, the GM PST timer may become out-of-sync with the rest of the GETVPN network. As a result, data traffic could stop because of a TBAR checking error.

  Conditions: This symptom is observed after the following sequence of actions:

  1. The GM registers successfully to the KS initially, and sends traffic to other GMs correctly
  2. Clear the GETVPN database in KS
  3. After a few minutes (longer than the TBAR window), clear the GETVPN database on the GM to trigger reregistration.

  After the GM reregisters, the PST value is different from the KS.

  Workaround: Disable TBAR.

- CSCtd48005

  Symptoms: Some dialer sessions are not being freed after all calls are disconnected in an LSDO environment.

  Conditions: This symptom is observed when using SGBP (all the remaining sessions are passed to the SGBP peer).

  Workaround: Use the **clear dialer sessions** command to free the dialer sessions.

- CSCtd51715

  Symptoms: Unused links reserved for call-in are sometimes used for dial-out.

  Conditions: This symptom is observed when the **dialer reserved- links** *4 0* command is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCtd51744

  Symptoms: Too many BADSHARE messages are seen on reload.

  Conditions: This symptom is observed when MFR is in software mode on a Cisco 7200 router and the **wr mem** command is entered, followed by a router reload.

Workaround: There is no workaround.

- CSCtd54873

  Symptoms: A Cisco router may crash while resetting the mac address under the voice-gateway system.

  Conditions: This symptom is observed on a Cisco 2800 router running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- 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.

- CSCtd60858

  Symptoms: While testing dot1x accounting, spurious accesses are seen.

  Conditions: This symptom is observed while verifying the attributes in the Access-Request, Access-Challenge, and Access-Accept packets.

  Workaround: There is no workaround.

- CSCtd63792

  Symptoms: Calls may fail to a particular B channel in a PRI with cause code #47 (Resources Unavailable).

  Conditions: This symptom is observed on a Cisco gateway with H323 and PRI and Cisco IOS Release 12.4(15)T10.

  Workaround: Busy out the affected B channel.

- CSCtd66970

  Symptoms: IPv6 NHRP support is not included in the -advipservicesk9- feature set.

  Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

  Workaround: Use the -adventerprisek9- feature set instead of the - advipservicesk9- feature set.

- CSCtd67940

  Symptoms: A Cisco router may crash while traffic is flowing through the ATM AIM interface.

Conditions: This symptom is observed when a configuration is copied which affects the ATM AIM interface (NAT config in this case) while traffic is flowing through the ATM AIM interface.

Workaround: Stop traffic, copy the configuration, make sure the interface comes up with the new config, then restart traffic.

- 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.

- CSCtd72647

  Symptoms: Severe throughput degradation out an interface occurs when a plain QoS policy map (not hierarchical, with no parent shaper) is applied.

  Conditions: This symptom has been observed on Cisco integrated service routers (ISRs) with either HWIC-1FE or HWIC-2FE cards running Cisco IOS Release 12.4(20)T, Release 12.4(22)T, or Release 12.4(24) T. The symptom has not been observed in Cisco IOS Release 12.4(15)T.

  Workaround: Use a hierarchical policy map with a parent shaper.

- CSCtd73256

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

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

  ```
  router#show ip ospf int Vlan804 is up, line protocol is up Internet Address
  xx.x.x.x/xx, Area 0 Process ID 1, Router ID xx.x.x.x, 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) xx.x.x.x, Interface address xx.x.x.x
  ```

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

  ```
  Unexpected exception to CPUvector 2000, PC = 261FC60
  ```

  Workaround: There is no workaround.

- CSCtd74470

  Symptoms: Voice ports on gateways configured for E1 R2 intermittently get stuck in the “clearfwd” state and can only be returned to normal operation mode by manual intervention.

  Conditions: When this symptom occurs, the following states are observed by examining the stuck port with **show** commands:

  ```
  Router#sh vo po su | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y Show
  voice trace 0/3/0.1.24 0/3/0:1 24 State Transitions: timestamp (state, event) ->
  (state, event) ... 3440023.272 (R2_Q421_IDLE, E_HTSP_SETUP_REQ) -> 3440023.380
  (R2_Q421_OG_SEIZE, E_DSP_SIG_1100) -> 3440047.816 (R2_Q421_OG_SEIZE_ACK,
  E_R2_REG_ABORT_DIGIT_COLLECT) -> 3440047.816 (R2_Q421_OG_CLR_FWD, E_DSP_DIALING_DONE)
  -> 3440048.816 (R2_Q421_OG_CLR_FWD, E_HTSP_EVENT_TIMER) - > 3440050.816
  (R2_Q421_WAIT_IDLE, E_HTSP_EVENT_TIMER) -> 3440050.816 (R2_Q421_WAIT_IDLE,
  ```

```
E_DSP_SIG_1100) -> 3440050.820 (R2_Q421_BLOCKED, E_DSP_SIG_1100) -> 3440069.960
(R2_Q421_BLOCKED, E_HTSP_RELEASE_REQ) -> 3440113.512 (R2_Q421_BLOCKED, E_DSP_SIG_1000)
->) ->
```

Workaround: Shut/No shut the controller or Busy Out the channel:

```
Router#sh vo po sum | include clearfwd 0/3/0:1 24 r2-digital up up clearfwd idle y
0/2/0:1 21 r2-digital up up clearfwd idle y 0/2/0:1 29 r2-digital up up clearfwd idle
y 0/2/0:1 30 r2-digital up up clearfwd idle y
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z:

```
Router(config)#control
Router(config)#controll
Router(config)#controller E1 0/2/0
Router(config-controller)#ds0 busyout 21,29,30,24
Router(config-controller) #no ds0 busyout 21,29,30,24
Router(config-controller)#end
Router#sh vo po sum | include clearfwd
Router# -->
```

- CSCtd78882

  Symptoms: FXO ports can get stuck in offhook state.

  Conditions: This symptom is observed when FXO ports are members of a huntgroup where the first member port is disconnected or down. The trunkgroup has max-retry configured and rapid calls are connected and disconnected using the trunkgroup.

  Workaround: Unconfigure “max-retry.” Under each port, configure “timeouts power-denial 0” so that disconnected ports are moved to offhook state and will not be hunted.

- CSCtd87666

  Symptoms: The incoming MLPPP packets via the DSL interfaces are process- switched rather than CEF-switched.

  Conditions: This symptom is observed when MLPPP is configured on a Cisco 1861 ISR. The symptom does not occur with the same configuration on a Cisco 28xx router.

  Workaround: There is no workaround.

- CSCtd88274

  Symptoms: Secure conference resource (dspfarm) fails after reload of a Cisco gateway.

  Conditions: Secure conference-resources will not register after a gateway reload and shows the status unregistered in CM. The SCCP IOS configuration needs to be deleted then reinserted to bring the resource back to a registered state. When the condition occurs, entering the **show sccp** command displays “not an active oper state” and “no active callmanager.”

  Workaround: There is no workaround.

- CSCtd92203

  Symptoms: AAA accounting for voice does not produce the correct values for NASPort for the TDM path. In addition, the calling station ID is missing.

  Conditions: This symptom is observed with AAA accounting.

  Workaround: There is no workaround.

- CSCtd94704

  Symptoms: A Cisco router may reload due to a watchdog timeout in the SCCP application.

  Conditions: This symptom is observed when the router is configured for MTP and transcoding for SCCP DSPfarms.

  Workaround: There is no workaround.

- CSCtd94947

  Symptoms: A Cisco 2851 router running Cisco IOS Release 15.0(1)M and using onboard HW encryption may stop processing encryption traffic after receiving a multicast packet that matches the encryption policy.

  Conditions: This symptom is observed with GETVPN encryption when the time-based anti-replay feature is turned on and when multicast traffic matches a permit statement in the encryption policy.

  Workaround: Use software-based encryption by enabling “no crypto engine onboard 0” in the global CLI, or disable the CEF using the **no ip cef** command.

- CSCtd98344

  Symptoms: NAT/PAT does not create more than one translation entry for all VRFs after a translation in the first VRF.

  Conditions: This symptom is observed when there is more than one VRF.

  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.

- CSCte01303

  Symptoms: New Primary KS after failover does not allow KS policy changes.

  Conditions: This symptom is observed when a KS failover occurs first, then the policy change is applied on the new primary KS.

  Workaround: Apply the policy change in the primary KS once it comes up, then force a KS role re-election by entering the **clear crypto gdoi ks role** in the new primary KS. Once the previously primary KS is restored as the primary KS, apply the policy change.

- CSCte02947

  Symptoms: A Cisco IPv6 mobile router may crash.

  Conditions: This symptom is observed when IPv6 routing is canceled by entering the **no ipv6 unicast router** command while the IPv6 mobile router is running.

  Workaround: Stop the mobile router before entering the **no ipv6 unicast router** command. This can be done by entering the **shutdown** command in the mobile router CLI.

- CSCte03209

  Symptoms: On a Cisco 7206/NPE-G2 configured for IRB and L2TP, ingress ARP requests and replies may fail with the following message according to “debug arp”:

```
IP ARP: sent req src xx.xx.xx.x 0000.0c4d.4a20,dst xx.xx.xx.x 0000.0000.0000 BVI1 IP
ARP rep filtered src xx.xx.xx.x 000c.85ae.2e00, dst 10.10.10.2 0000.0c4d.4a20 wrong
cable, interface Virtual-Access5.
```

Conditions: This symptom is observed on Cisco IOS Release 12.4(15)T7, Release 12.4(15) T9, and Release 12.4(24)T2.

```
bridge irb bridge 1 protocol ieee bridge 1 route ip
interface BVI1 ip address <xx.xx.xx.x> ip directed-broadcast
interface Virtual-Template1 no ip address no peer default ip address ppp
authentication pap chap bridge-group 1 bridge-group 1 spanning-disabled end
interface Virtual-Access5 no ip address no peer default ip address ppp authentication
pap chap bridge-group 1 bridge-group 1 spanning-disabled
```

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.

- CSCte15982

  Symptoms: When a Cisco 877 DSL router running Cisco IOS Release 12.4(24)T2 is connected to a 3rd party DSLAM running in 4-wire mode, entering the **clear pppoe all** command may result in a PADS received on one PVC being incorrectly processed on a subinterface associated with a different PVC, which results in two PPPoE sessions transmitting data packets on the same PVC.

  Conditions: This symptom is observed under the following working scenario:

```
CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 7 xxxx.xxxx.xxxx
ATM0.38 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/38 UP N/A 8 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
```

  After entering the **clear pppoe all** command:

```
CPE#clear pppoe all CPE#show pppoe session 2 client sessions
Uniq ID PPPoE RemMAC Port Source VA State SID LocMAC VA-st N/A 9 xxxx.xxxx.xxxx
ATM0.40 Di0 Vi1 UP
xxxx.xxxx.xxxx VC: 0/40 UP N/A 10 xxxx.xxxx.xxxx ATM0.40 Di1 Vi2 UP
xxxx.xxxx.xxxx VC: 0/40 UP
controller DSL 0 mode atm line-mode 4-wire enhanced dsl-mode shdsl symmetric annex B
interface ATM0.38 point-to-point pvc data 0/38 pppoe-client dial-pool-number 1
interface ATM0.40 point-to-point pvc voip 0/40 pppoe-client dial-pool-number 2
interface Dialer0 ip address negotiated encapsulation ppp dialer pool 1 keepalive 60
ppp pap sent-username data@data.com password 0 data
interface Dialer1 ip address negotiated encapsulation ppp dialer pool 2 keepalive 60
ppp pap sent-username voip@voip.com password 0 voip
```

  In addition, this symptom is observed under the following conditions:

  1. This symptom is not reproducible when running in 2-wire G.SHDSL mode. It is reproducible only when running “line-mode 4-wire enhanced.”
  2. The symptom is reproducible in Cisco IOS Release 12.4(15)T7, Release 12.4(15)T10, Release 12.4(20)T, Release 12.4(22)T, Release 12.4(22)T1, Release 12.4(24)T, Release 12.4(24)T1, Release 12.4(24)T2, and Release 15.0(1)M.
  3. The symptom can be triggered three ways:

  a. Reload the router

  b. If the reload results in correct behavior, “clear pppoe all.”

c. If the reload results in correct behavior, any subsequent event which results in both PPPoE sessions being torn down simultaneously.

4. 4. The symptom is not reproducible if any packet layer debugs are enabled, such as “debug pppoe packet” or “debug atm packet.”

Workaround:

1. Reload the router.
2. After every reload, if the problem is not occurring, configure “debug pppoe packet” on the Cisco 878 router.
3. After every reload, if the problem is occurring, reload the router until it is not occurring.

- CSCte19478

  Symptoms: Entering the **crypto isakmp xauth timeout** command does not seem to have any effect.

  Conditions: This symptom is observed when the command is needed for a specific scenario where user input at xauth requires more time than the default timeout value--for example, for rsa authentication (in new pin mode).

  Workaround: There is no workaround.

- 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 xx.x.x.x 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.

- CSCte23299

  Symptoms: A Cisco 877W router is not responding to IPv6 neighbor solicitation.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCte28777

  Symptoms: A line is logged out from the hunt group if the user enables DND, then logs out with extension mobility, logs back in, and disables DND.

  Conditions: This symptom is observed when the “ephone-hunt logout DND” option is configured with EM login/logout.

  Workaround: Use the "ephone-hunt logout HLog” option instead.

- CSCte30224

  Symptoms: A Cisco IOS device may unexpectedly restart when executing a Tcl script that has been compiled into bytecode.

Conditions: This symptom is observed if the Tcl script tries to generate a random number using the **expr** *rand()* command.

Workaround: Do not use the **expr** command to generate random numbers, or do not compile the Tcl script into bytecode.

- CSCte34718

  Symptoms: Network Time Protocol (NTP) may lose synchronization.

  Conditions: This symptom is observed on a Cisco 871 router with board rev. C0

  Workaround: Revert to Cisco IOS Release 12.4(15)T3.

- 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 them again.

- CSCte39621

  Symptoms: Interface is wedged and does not pass traffic.

  Conditions: This symptom is observed when the interface is configured for bridge-group and associated to a bvi interface.

  Workaround: There is no workaround.

- CSCte41747

  Symptoms: The **show run | section** command displays incomplete output.

  Conditions: This symptom is observed on all Cisco IOS 15.0 releases.

  Workaround: Install an earlier Cisco IOS release (for example, Cisco IOS Release 12.4).

- CSCte42023

  Symptoms: In rare timing scenarios, abort may be ignored, resulting in an IOS state machine getting out of sync with module state.

  Conditions: This symptom is observed in a very rare scenario of abort being initiated by the user while IOS is simultaneously handling a message from the module that requires the state machine change.

  Workaround: Reload the router.

- CSCte42041

  Symptoms: Randomly, various DMVPN spokes lose connectivity with the hub.

  Conditions: This symptom is observed when NRRP mapping on a spoke does not trigger an IPSec Socket in the SA database. The following error may appear:

  ```
  NHRP: Failed to retrieve NHRP IDB in IF ctrl check
  ```

  Workaround: Remove and reapply the hub static mapping.

- CSCte43663

  Symptoms: RTCP packets are not forwarded across the network.

  Conditions: This symptom is observed in an IPIPGW configuration.

  Workaround: There is no workaround.

- CSCte53759

  Symptoms: The Cisco 1905 platform is missing the HWIC_1B_U module.

  Conditions: This symptom is observed on the Cisco 1905 platform.

  Workaround: This module will be supported as part of the M2 rebuild for the Cisco 1905 platform.

- 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 xx.xx.xxx.xx
  Outgoing interface list: Null (Src 2 Ip , Grp IP), 01:46:19/stopped, flags: sPLTXI
  Incoming interface: FastEthernet4.3, RPF nbr xx.xx.xxx.xx
  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> xxx.xxx.xxx.xxx ip pim sparse-mode ip igmp join-group <group addr> source
  xx.xx.xxx.xx ip igmp join-group <group addr> source xx.xx.xxx.xx
  ```

  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.

- CSCte62782

  Symptoms: A Cisco router may crash at bootup after service-policy is applied to ATM PVC, or the router may show spurious memory accesses and subsequently crash on removal or addition of service-policy to ATM PVC.

  Conditions: This symptom is observed when hierarchical QoS is applied to ATM PVC.

  Workaround: There is no workaround.

- CSCte78562

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

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

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

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

- CSCte81731

  Symptoms: A Cisco device may crash after configuring service-policy on an interface.

  Conditions: This symptom is observed on a Cisco device in the presence of ICMP filter ACE under the match access-group ACL of a class-map.

  Workaround: There is no workaround.

- CSCte81855

  Symptoms: The following symptoms occur when a Cisco Voice XML (VXML) gateway reaches 2048 open sockets:

  - Dead air on call and call drops
  - If customer has survivability TCL enabled in ingress gateway, the call will go to survivability

  - Agents can be reserved but voice calls do not reach the agent. Calls to the agent are placed after the original call failed and the call is handled by survivability TCL.
  - Errors displayed in the VXML gateway are related to Network Out of Order cause code 38 and ip transfer to 0.0.0.0 ip address failed

  Conditions: This symptom is observed in any Cisco gateway, specifically Cisco 2800, Cisco 3800, and Cisco AS53. The symptom occurs in Cisco IOS Release 12.4 (15)T6, Release 12.4(15)T7, Release 12.4(15)T8, Release 12.4(15)T9, Release 12.4 (15)T10, Release 12.4(15)T11, and Release 12.4(15)T12.

  Workaround:

  - Make sure the media server and VXML server are reachable
  - Make sure all media files requested exist in the media server and that the path to the media file is correct
  - Make sure media server backup is configured in the VXML gateway (for example, ip host mediaserver-backup)
  - Check the http client process with: show proc cpu | include http client show socket X --> Where X is the id of the http client process showing with the previous command.

  If the TCP sockets are getting closed to 2048, shutdown the voice service voip and wait for all the ip calls to finish to reboot the gateway. If this is also an ingress gateway, you will have to re-route the calls to another ingress gateway.

- CSCte83404

  Symptoms: A Cisco router may crash and report a bus error.

  Conditions: This symptom is observed on a Cisco router using SIP and CME 8.0.

  Workaround: Remove the following commands: **nat symmetric role active** and **nat symmetric check-media-src** from sip-ua.

- 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.

- CSCte93101

  Symptoms: A Cisco router running Cisco IOS may crash by Watchdog Timeout. The logs prior to the crash will have repeated errors similar to:

  ```
  %SYS-2-INTSCHED:'event dismiss' at level 3 -Process= "OSPF-100 Hello", ipl= 3, pid= 12
  ```

  The process listed is not relevant.

  Conditions: This symptom is observed on a router with an interface using HDLC encapsulation with traffic passing. HDLC is the default encapsulation type for serial interface.

  Workaround: Change encapsulations away from HDLC using the **encapsulation** *protocol* 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.

- CSCtf26045

  Symptoms: Ignored errors incrementing regularly even with low traffic when the traffic arrives on Multilink PPP, bundling multiple T1.

  Conditions: This symptom is observed only when odd byte packets of size 273 arrive on the onboard hdlc driver. This leads to total traffic stoppage, especially if "qos preclassify" is configured on the tunnel interface.

  Workaround: There is no workaround.

- CSCtf28498

  Symptoms: A Cisco router may crash when removing the service policy.

  Conditions: This symptom is observed with QoS ACLs containing ICMP ACEs with either TTL, Reflect, or Option field-related entries.

  Workaround: Do not use ICMP ACEs with TTL, Reflect or Option field-related entries.

- CSCtf31029

  Symptoms: A Cisco HWIC-16A module configured on a Cisco 2900 router for asynchronous tunneling may not transmit escape characters (data payload) properly over IP to connected devices even though “escape-character none” is configured under the line.

  Conditions: This symptom is observed on Cisco 2901, Cisco 2911, and Cisco 2921 platforms with Cisco HWIC-8A/16A or HWIC-4A/S modules and running any Cisco IOS release. This symptom does not occur on a Cisco 2951 platform.

  Workaround: Use the AUX port.

- CSCtf34853

  Symptoms: NS/NA packets are missing when enabling IPv6.

  Conditions: This symptom is observed on Cisco routers with onboard GE interfaces.

  Workaround: There is no workaround.

- CSCtf49816

  Symptoms: Tracebacks are seen while stressing the system.

  Conditions: This symptom occurs when the CPU is stressed at more than 90% capacity.

  Workaround: Reduce the CPU to below 90%.

Resolved Caveats—Cisco IOS Release 15.0(1)M1

Cisco IOS Release 15.0(1)M1 is a rebuild release for Cisco IOS Release 15.0(1)M. The caveats in this section are resolved in Cisco IOS Release 15.0(1)M1 but may be open in previous Cisco IOS releases.

- CSCsc62963

  Symptoms: The interface MTU is not user configurable. When you attempt to configure “interface level command mtu”, the following message is printed:

  ```
  % Interface {Interface Name} does not support user settable mtu.
  ```

  Conditions: The symptom is observed with a 2-Port FE on a Cisco 7200 series router.

  Workaround: There is no workaround.

  Further Problem Description: The Cisco.com document entitled “MPLS MTU Command Changes” further discusses this enhancement.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsy89795

  Symptoms: A Cisco ASR 1000 series router may fail, and the console will display an error message similar to the following:

  ```
  "A critical process ppc_linux_iosd_image has failed (rc 139)".
  ```

  Conditions: This symptom is observed when using the **clear counters** command after removing a crypto map from an interface.

  Workaround: Wait a minute or two after removing a crypto map from an interface before entering the **clear counters** command.

- CSCsz18573

  Symptoms: A number of problems are found in the early version of the NEMO mobile router:

  - MR tunnel will flap with NEMO explicit prefix configured
  - Roaming can be slow or fail installing routes
  - MR routes appear as static as opposed to mobile
  - Configuring the home address on a loopback is required
  - ND operates on the MIP tunnel
  - Ten seconds latency appears on MR at tunnel setup and on HA at roaming

  Conditions: These symptoms occur when running Cisco IOS Release 12.4(22)T1 and Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCsz39167

  Symptoms: If a tunnel is configured over the 880-3G cellular interface, traffic forwarding stops when the packet size is greater than the tunnel MTU.

  Conditions: The symptom is observed when a tunnel is configured over a cellular interface and running Cisco IOS Release 12.4(24)T.

  Workaround: Disable “ip cef”.

- 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.

- CSCsz89826

  Symptoms: The router starts reloading while testing the OAM management functionality over ATM using the encapsulation aal5mux ppp which is done after the encapsulation aal5snap.

Conditions: This symptom is observed after configuring “oam-pvc manage 9" under OAM feature.

Workaround: There is no workaround.

- CSCta08194

  Symptoms: A router may crash.

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

  Workaround: There is no workaround.

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

- CSCta14505

  Symptoms: No source group (SG) entry forms in the network for PIM sparse-mode groups. This leads to traffic failures.

  Conditions: This symptom is observed when PIM-SM is configured in the network and traffic is sent for PIM-SM groups.

  Workaround: Shut down the upstream interface, remove the IP address, configure it again, then perform a **no shutdown** on the interface.

- CSCta17774

  Symptoms: An abnormal/high interarrival jitter time is reported in RTCP from a Cisco AS54xx when Nextport DSPs are used.

  Conditions: This symptom is observed under the following conditions:

  - Nextport DSPs are used on a Cisco AS54xx
  - RTCP is used to measure interarrival jitter values

  Workaround: There is no workaround.

- CSCta22767

  Symptoms: A Cisco router may crash when unconfiguring class-map.

  Condition: This symptom is observed in a Cisco router using Cisco IOS Release 15.0M.

  Workaround: There is no workaround.

- CSCta39339

  Symptoms: Traffic loss occurs on a Cisco ES20 line card when configuring IPv4 IP address on the SVI interface.

  Conditions: This symptom is observed when an xconnect configuration exists.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SVI interface.

- CSCta49840

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

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

  Workaround: There is no workaround.

- CSCta66499

  Symptoms: The Cisco IOS MGCP gateway may experience a software-forced reload.

Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T4 or a later release when reenabling MGCP with version 1.0 after testing fgdos calls with MGCP version 0.1.

Workaround: There is no workaround.

- CSCta73534

  Symptoms: In rare cases, copying a file to Cisco IOS via the Cisco IOS SCP server fails, but the SCP server returns an OK (0) code. The file that failed to copy appears on the router as zero bytes.

  Conditions: This symptom occurs when the SCP server does not receive an EOF marker from the SCP client.

  Workaround: There is no workaround.

- CSCta77960

  Symptoms: TCP/TCB leak may occur on a Cisco voice gateway with an increasing number of sessions hung in CLOSEWAIT state.

  Conditions: This symptom occurs when the voice gateway is under normal use.

  Workaround: There is no workaround.

- CSCta79941

  Symptoms: A virtual interface is not created when invoked using the **ip unnumbered** *type number* command.

  Conditions: This symptom is observed under a PPP interface when the virtual interface has been previously deleted.

  Workaround: Recreate the virtual interface manually using the **interface** command.

- CSCta98976

  Symptoms: A Cisco IOS certificate server (CS) may crash during a CA certificate rollover.

  Conditions: This symptom is observed with similarly-named keys.

  Workaround: Rename similarly-named keys. For example, the keys named SubCA are a subset of the SSH keys named SubCA.server. Rename the SSH keys using the **ip ssh rsa keypair-name** command.

- CSCtb05195

  Symptoms: Throughput degradation may occur on a Cisco integrated services router (ISR).

  Conditions: This symptom is observed in CEF/SVI TOE configurations when comparing specific performance metrics between baseline Cisco IOS Release 12.4 (23.5)pi10 and target Release 12.4(24.6)PI11n.

  Workaround: There is no workaround.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

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

  Workaround: There is no workaround

- CSCtb26396

  Symptoms: HTTPS connections suddenly fail with the following error:

  ```
  //-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1
  //394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL socket_connect failed
  fd(0)
  ```

  Conditions: The symptom is observed with CVP Standalone deployment running with HTTPS and with Cisco IOS Release 12.4(22)T1 or Release 12.4(24)T1.

  Workaround: Reload the gateway.

- CSCtb39345

  Symptoms: Session timeout does not occur within the time configured in the session-timeout value on a per-user profile.

  Conditions: This symptom is observed in Cisco IOS Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCtb43293

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

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

  Workaround: There is no workaround.

- CSCtb44167

  Symptoms: A Cisco router may reload when running EA-FAST authentication with RADIUS Accounting.

  Conditions: This symptom is observed on a Cisco 1841 integrated services router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCtb45718

  Symptoms: A Cisco router may crash with traceback leading to checkheap.

  Conditions: This symptom is observed when endpoint agnostic port allocation has been enabled using the **ip nat service enable-sym-port** command**.**

  Workaround: Disable the endpoint agnostic port allocation using the **no ip nat service enable-sym-port** command.

  Further Problem Description: Under certain conditions, the symmetric port database is not in sync with the port list, resulting in the reuse of port ranges that had been free.

- 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.

- CSCtb52200

  Symptoms: A router may crash when configuring 3-level policies with strict priorities on each level.

  Conditions: This symptom is observed when:

  - the bandwidth value configured for the interface is very low
  - a class in the parent policy has a bandwidth of less than 1kb/s
  - a child policy is added with priority or Bandwidth Remaining Percentage (BRP).

  Workaround: When attaching a child policy with priority or BRP, ensure that the parent class bandwidth is greater than 1kb/s.

- CSCtb56567

  Symptoms: A Cisco voice gateway experiences a memory leak error on CCSIP SPI CONTROL process, which may lead the router to crash every 4-5 days.

  Conditions: This symptom is observed when a router is configured with sip-ua using the **mwi-server** command with transport set to *tcp*, but the server specified is not set up to receive sip and thus replies with tcp resets. This can be caused by misconfigured sip mwi.

  Workaround: Reload the device regularly to free the memory.

- CSCtb57237

  Symptoms: After a call is resumed from hold, the gateway sends a G.729 codec although a G.711 was negotiated in the H.245 messages.

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

  Workaround: There is no workaround.

- CSCtb60330

  Symptoms: SVTI tunnel flaps at phase 1 expiry when a DPD ACK is not received. The line protocol on the tunnel interface goes down.

  Conditions: The symptom is observed with SVTI tunnels and when DPDs are enabled.

  Workaround: Disable DPDs.

  Alternate workaround: Use the **no crypto isakmp keepalive** command.

  Further Problem Description: This may affect those scenarios where routing protocols like BGP are run over the tunnel. To diagnose this, the following debugs should be enabled on both sides:

  debug crypto isakmp debug crypto ipsec debug crypto kmi

  The following entry can be seen in debugs:

  ```
  DPD sent to 10.1.1.1:500 & waiting: But IKE sa expired. Killing IPSec sas.
  ```

- 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.

- CSCtb67967

  Symptoms: PPP fails at LCP stage with VPDN dial-out calls.

  Conditions: This symptom is observed in Cisco IOS Release 12.4T in a dial-out scenario.

Workaround: There is no workaround.

- 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.

- CSCtb70102

  Symptoms: When SRST and STCAPP are configured and running on the same router, SCCCP-controlled analog phones may be unable to make an outgoing call.

  Conditions: This symptom is observed when, upon WAN link failure, the phones register to an SRST gateway.

  Workaround: There is no workaround.

  Further Problem Description: This symptom occurs due to STCAPP automatically adding a *station-id* parameter under the **voice-port** command in order to save DN information for registration to SRST.

- CSCtb72664

  Symptoms: 100% ingress packet drop (IQD) with depletion of free IO memory.

  Conditions: This symptom is observed in a Cisco 3945 [NM-1A-OC3-POM] <-> [NM-1A-OC3-POM] peer setup. In this or a similar scenario, stressing the OC3 module at the line rate (~84Mbps) with bi-directional traffic will cause this symptom along with depletion of free IO memory.

  Workaround: Do not stress the NM-1A-OC3-POM module at the line rate. Stopping or reducing the traffic rate should resolve the depletion of free IO memory.

- CSCtb76775

  Symptoms: A Cisco 3900 series router may experience a large IO memory leak.

  Conditions: This symptom is observed with IPSec and QoS on a Cisco NM-1A- T3/E3 network module with NME-IPS in promiscuous mode.

  Workaround: Run IPS in inline mode.

- CSCtb78266

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

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

  Workaround: There is no workaround.

- CSCtb82256

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed when all of the following occur:

  - Cisco Unified CallManager XML configuration files are downloaded to the router while the router is processing the pri-group configurations
  - the **shutdown** and **no shutdown** commands are entered on the voice port
  - the **no ccm-manager** command is entered.

Workaround: Do not shut down the voice port at the time of configuration download.

- CSCtb88409

  Symptoms: A Cisco router may crash when configuring the object id in config-event-objlist subconfiguration mode

  Conditions: This symptom is observed when entering the **cns config notify** command.

  Workaround: There is no workaround.

- CSCtb89424

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

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

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- 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.

- CSCtb95801

  Symptoms: In certain network setups, every five days the router hangs and the following error message is seen:

  ```
  SYS-2-BADSHARE: Bad refcount in datagram_done
  ```

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCtb97176

  Symptoms: Router may reload unexpectedly shortly after boot up.

  Conditions: This symptom is observed when QoS is configured on a router running Cisco IOS Release 15.0M

  Workaround: Disable QoS by removing the service-policy statement applied to all interfaces.

  Alternate Workaround: Use a previous Cisco IOS release.

- CSCtb98508

  Symptoms: A Cisco router may experience a bus error crash.

  Conditions: The symptom has been experienced on a Cisco 2851 router that is running Cisco IOS Release 12.4(20)T3 and when “callmonitor” is enabled.

  Workaround: There is no workaround.

- CSCtc04228

  Symptoms: The command **mgcp behavior g729-variants static-pt** is the default and will show up in the configuration. This causes a problem when you save the configuration and downgrade to an earlier Cisco IOS Release where this behavior is not present. There, the command will now be enabled when it was not previously.

  Conditions: Using an earlier version of a Cisco IOS Release will enable the command.

Workaround: After downgrading to a lower version where **mgcp behavior g729-variants static-pt** is not the default, configure **no mgcp behavior g729-variants static-pt** to remove the CLI.

- CSCtc04351

  Symptoms: The GM router might reload.

  Conditions: This symptom is observed if the following conditions are met:

  - Many VRFs are configured on the same GM, each belonging to an individual GETVPN group
  - All the VRFs are triggered to register with the KS at the same time
  - While #2 is happening, the **clear crypto gdoi** command is entered on the GM.

  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.

- CSCtc06629

  Symptoms: A Cisco router may crash at crypto functions after upgrade to Cisco IOS Release 12.2(33r)XNC.

  Conditions: This symptom is observed on a Cisco ASR 1000 Series router after upgrading from Cisco IOS Release 12.2(33r)XNB to Release 12.2(33r) XNC.

  Workaround: There is no workaround.

- CSCtc09735

  Symptoms: CISCO-ICSUDSU-MIB does not report any values on SNMP query for a Cisco HWIC-1CE1T1-PRI card and its variants.

  Conditions: This symptom is observed when querying the CISCO-ISCUDSU-MIB by inserting a Cisco HWIC-2CE1T1-PRI card.

  Workaround: There is no workaround.

- CSCtc11521

  Symptoms: Invalid pointer value is displayed whenever NVRAM is accessed.

  ```
  "NV: Invalid Pointer value(460E460C) in private configuration structure"
  ```

  Conditions: This symptom is observed when upgrading NVRAM from an older version to a newer version.

  Workaround: Load a prior working image and backup all files in NVRAM, including the startup-config, to another device or tftp/ftp. Load the new image and enter the **erase/all nvram** command followed by the **write mem** command. NVRAM will now be restored. Copy the backup files back to NVRAM.

- CSCtc12312

  Symptoms: PKI might get stuck after 32678 failed CRL fetches, causing IKE to stop processing any further ISAKMP packets.

  Conditions: This symptom is observed in Cisco IOS Release 12.4.20T4 and Release 12.2(33)SXH5 when CRL checking is performed.

  Workaround: Do not perform CRL checking.

Further Problem Description: Normally, this symptom could take years to manifest in a well-designed environment, but in extreme conditions it could occur within hours.

- 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.

- 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 “route-map” as [set interface loop0].

- CSCtc14156

  Symptoms: A router crashes while testing Redial Enhancement feature.

  Conditions: This symptom happens during the unconfiguration part of ISDN dialer profile.

  Workaround: Wait for a period of 30 seconds before starting the unconfiguration.

- CSCtc16399

  Symptoms: NIOS watchdog timer times out.

  Conditions: This symptom is observed when an MC5727 modem is power-cycled.

  Workaround: Reload the router.

- 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.

- CSCtc19036

  Symptoms: Getting traceback from function k_rttMonEchoAdminEntry_ready while performing an SNMP operation.

  Conditions: This symptom is observed when using SNMP to create an IP SLA jitter probe that includes a codec option.

  Workaround: There is no workaround.

- CSCtc23003

  Symptoms: A Cisco device running Cisco IOS Software may unexpectedly reload with a STACKLOW message.

  Conditions: This symptom is observed when the **logging buffered xml** *xml-buffer-size* command is entered to enable system message logging (syslog) and send XML-formatted logging messages to the XML-specific system buffer.

  Workaround: Disable the XML syslog buffer and return the size of the buffer to the default using the **no logging buffered xml** *xml-buffer-size* command.

- CSCtc23374

  ```
  Symptoms: A Cisco router may unexpectedly reload with the following message:
  %SYS-6-STACKLOW: Stack for process BGP Router running low, 0/9000
  ```
  Conditions: This condition is observed when:

  1. BGP is configured
  2. BGP has learned about multiple networks
  3. The **clear ip bgp** *soft* or other **clear ip bgp** commands are entered, or when BGP-related configurations are removed.

  Workaround: There is no workaround.

- CSCtc23465

  Symptoms: A Cisco 881 Integrated Services Router (ISR) may pause indefinitely or reload unexpectedly when a DMVPN tunnel interface is configured.

  Conditions: This symptom is observed when a DMVPN tunnel interface is configured during the same session in which a **shutdown** command precedes the network-id configuration.

  Workaround: Shut down the tunnel after network-id configuration.

  Further Problem Description: A traceback followed by a crash typically occurs when multiple interfaces are configured together with the same configuration, even though the traceback can be seen with a single interface. This does not occur once the configuration is saved and the router is reloaded, as the **shutdown** command is always NVGen'ed after the network-id configuration.

- CSCtc23707

  Symptoms: A Cisco router may either hang or crash with a watchdog timeout.

  Conditions: This symptom is observed when traffic is sent on a router running a pseudo-preemptive process (for example, BFD).

  Workaround: Remove the pseudo-preemptive process (for example, the BFD configuration) from the router.

  Further Problem Description: To compensate for the absence of the BFD configuration on the router, decrease the time interval between hello packets for the associated routing protocol. Note, however, that this may result in decreased performance. This action is specific to BFD and does not apply to other pseudo-preemptive processes.

- CSCtc27454

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

  ```
  %%SYS-3-CPUHOG: Task is running for (xxxxx)msecs, more than (xxxx)msecs (xx/x),process
  = Crypto ACL.
  ```
  Conditions: This symptom is observed when the DMVPN tunnel is shut down.

  Workaround: There is no workaround.

- 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.

- CSCtc33123

  Symptoms: Router may crash when entering the **compress stac** or **compress predictor** command on a PPP-enabled interface.

  Conditions: This symptom is observed when stac or predictor compression is configured, or when switching from stac to predictor or from predictor to stac compression.

  Workaround: There is no workaround.

- CSCtc36703

  Symptoms: Modem calls over BRI are terminated, followed by a channel reset.

  Conditions: This symptom is observed when a BRI VIC is used in conjunction with a Cisco Digital Modem PVDM Module.

  Workaround: There is no workaround.

- CSCtc36826

  Symptoms: Unable to detect SIT and disconnect an FXO call.

  Conditions: The symptom is observed on an FXO port configured with “supervisory sit us immediate-release” or “supervisory sit us”.

  Workaround: Configure “supervisory sit us all-tones”.

- 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.

- CSCtc37697

  Symptoms: A Cisco router pauses indefinitely or reloads unexpectedly.

  Conditions: This symptom is observed when the ATM PVC bundle is removed and reapplied, and when OAM is configured on the bundle.

  Workaround: There is no workaround.

- CSCtc45293

  Symptoms: Ping fails on a back-to-back AIM-IMA bundle when configuring then unconfiguring precedence on a bundle member.

  Conditions: This symptom is observed when a PVC is created using the **atm vc-per- vp** *number* command and the *number* value entered is greater than 255. The PVC does not come up.

  Workaround: There is no workaround.

- CSCtc46540

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed when stress traffic is present with an LWE IPS package.

  Workaround: There is no workaround.

- CSCtc51573

  Symptoms: CME group pickup or pickup features do not work properly.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T1 when a call is placed to the voice-hunt group.

  Workaround: There is no workaround.

- CSCtc55964

  Symptoms: The **xconnect** command is missing.

  Condition: This symptom is observed in Cisco IOS Release 15.0M under the SVI on a Cisco 2900 series router.

  Workaround: There is no workaround.

- CSCtc57940

  Symptoms: A Cisco 2951 ISR G2 may crash when a SIP phone registered to SIP CME parks a call.

  Conditions: This symptom is observed on a Cisco 2951 ISR G2 when the following conditions are present:

  - call-park system application is configured in telephony-service mode
  - a park slot is configured with a timeout limit
  - the SIP phone parks a call.

  Workaround: There is no workaround.

- CSCtc59574

  Symptoms: A Cisco 3945 integrated services router (ISR) may crash with HSRP, SNAT, BFD, EIGRP configured.

  Conditions: This symptom is observed on a Cisco 3945 ISR with NM-1A-OC3-POM or NM-1A-T3/E3 cards installed when IP NAT is removed or added on a BFD-enabled interface.

  Workaround: There is no workaround.

- CSCtc81283

  Symptoms: The following error is displayed when attempting to integrate Cisco Unified CCX 8.0 with Cisco Unified Communications Manager Express (CME):

  ```
  AXL_EXCEPTION:Unknown AXL Exception: Exception=org.xml.sax.SAXParseException: The
  element type "ISExtension" must be terminated by the matching end- tag
  "</ISExtension>".
  ```

  Conditions: This symptom is observed when Cisco Unified CCX 8.0 is integrated with Cisco Unified CME.

  Workaround: There is no workaround.

- CSCtc97687

  Symptoms: A mobile router (MR) cannot roam between two interfaces on the same access router or between two different access routers.

  Conditions: This symptom is observed on an MR with a single roaming interface roaming between two different interfaces on the access router or between two different access routers.

  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.

- CSCtd15454

  Symptoms: A Cisco router may crash while performing online insertion and removal (OIR).

  Conditions: This symptom is observed on a Cisco 7200 NPE-G1 router on PA-GIG in an MPLS environment with traffic.

  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.

- CSCtd82172

  Symptoms: A new China SKU was added to the Cisco ISR family. Currently, there are no MIB definition and codes to access the SysObjectId identifier through SNMP for this new SKU.

  Conditions: When doing “snmp walk” or “snmp get for SysObjectId mib variable” on Cisco1941W-C/K9 router, a SNMP timeout is seen.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.0(1)M

This section describes possibly unexpected behavior by Cisco IOS Release 15.0(1)M. All the caveats listed in this section are open in Cisco IOS Release 15.0(1)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsh90966

  Symptoms: Router with IPv4 MFIB code-based forwarding infrastructure will experience higher CPU usage.

  Conditions: Occurs when moving from legacy v4 Multicast Distributed Fast Switching (MDFS) to Multicast Forwarding Information Base (MFIB). With a large number of multicast groups, CPU usage is increased 30-60%.

  Workaround: There is no workaround.

- CSCsq47730

  Symptoms: Router displays the following error message, then freezes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```
  A reload is required to recover.

Conditions: Occurs on a Cisco 1803 running Cisco IOS Release 12.4(6)T7.

Workaround: There is no workaround.

- CSCsu42583

  Symptoms: Any image or large file is corrupted when copied to disk. The following error message is displayed:

  ```
  Error reading disk2:<filename> (Clusterchain broken on file)
  ```

  Conditions: Happens only when a compact flash card is present.

  Workaround: Replace the compact flash card with another model, one that is supported by Cisco.

- CSCsu49189

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

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: Detach and attach Frame-Relay fragment.

- CSCsu50869

  Symptoms: Calls do not complete because Cisco Unified Border Element (CUBE) does not sent PRACKs to all 1xx messages.

  Conditions: Occurs with h.323 slow start to SIP delayed media call flow.

  Workaround: Enable fast start h.323 with an MTP in CUCM, which allows for SIP early offer. Reliable 1xx messaging can also be disabled to prevent the requirement of provisional acknowledgments.

- CSCsu64365

  Symptoms: The system may experience repeated crash due to I/O memory corruption showing error messages like:

  ```
  %SYS-6-BLKINFO: Corrupted next pointer blk
  ```

  Conditions: The corruption is caused by voice packets encapsulated by GRE/IPSEC (other encapsulations which add to the size of the packet). The router must have voice packets routed through GRE or IPSEC tunnel and if a simultaneous Fax tone is sent, the router will crash.

  Workaround: Move the GRE tunnel from the CME where ever possible.

- CSCsu66197

  Symptoms: Cyclic redundancy check (CRC) errors increment on Cisco 2800 router.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsw28501

  Symptoms: After some time (days to months), all inbound and outbound calls through gateway fail with CCAPI cause 102. Calling party (PSTN or VoIP side) hear fast busy. When failure occurs, all calls, inbound and outbound fail. No R2 signaling is observed on inbound or outbound calls

  Conditions: Observed with Cisco IOS Release 12.4.12c.

  Topology: UCM/IP phones --- ip/h323 --- 5350 --- E1R2

  No changes to network or gateway between incidents.

  Workaround: Reboot gateway resolves issue for some time, issue returns after days or months.

- CSCsw52855

  Symptoms: CRC and frame errors are seen if mark was used as the idle character between packets.

Conditions: This problem occurs when using the following interface cards:

- VWIC2-1MFT-T1/E1
- VWIC2-2MFT-T1/E1
- VWIC2-1MFT-G703
- VWIC2-2MFT-G703

Workaround: Use the following interface cards that are not affected by this problem:

- HWIC-4T1/E1
- HWIC-2CE1T1-PRI
- HWIC-1CE1T1-PRI

- CSCsx26025

  Symptoms: Clients are not able to ping each other after a few minutes.

  Conditions: Occurs on a Unified Communications 520.

  Workaround: There is no workaround.

- CSCsx81957

  Symptoms: Router crashes due to memory corruption in TPLUS process.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- CSCsx94119

  Symptoms: Gateway 12.4(23.15)T5 faces software forced reload intermittently,

  Conditions: Reload occurs intermittently while making hairpin calls continuously

  Workaround: There is no workaround.

- CSCsy34256

  Symptoms: Tracebacks occur after abnormally removing the trustpoint and issuing **no sccp** and **sccp**.

  Conditions: Tracebacks occur after abnormally removing the trustpoint and issuing **no sccp** and **sccp**.

  Workaround: There is no workaround.

- CSCsy49980

  Symptoms: In GETVPN scenarios, on VSA we keep both the SA and the corresponding ACE entry till the SA expires though that ACE entry was removed from the KeyServer. Whereas on S/W they keep the SA but remove the ACE entry.

  Conditions: When an ACE entry from the KS ACL is removed.

  Workaround: Enter **clear crypto gdoi** on the group members to correct the problem.

- CSCsy76260

  Symptoms: Cisco AS5400 may reload on applying **mgcp nas** configuration under a T1 controller.

  Conditions: Controller to be in up state before applying the configurations.

  Workaround: There is no workaround.

- CSCsy85375

  Symptoms: Async interface for V.92 modem in Cisco 1800 router reports in/out errors and CRC errors when connected with ISR rotuer which has PVDM2-ddM modem module using V.44 compression. This issue can cause data packet loss.

  Conditions: This issue only happens when V.92 modem which is built in Cisco 1800 connects to PVDM2-xxDM modems and connected with V.44 compression. If V.44 compression is not negotiated, this issue will not happen.

  Workaround: Disable V.44 compression and configure modems to trainup in V.34 speed using the following modemcap:

  ```
  1800 Modemcap: modemcap edit Si_Lab_V34_no_comp misc &f%c0+ms=v34
  PVDM2-xxDM Modemcap modemcap edit PVDM2DM_V34_no_comp misc &f&d3%c0+ms=11
  ```

- CSCsy89437

  Symptoms: Problem is happening on Cisco AS5400 with the frequency about once in a month.

  Conditions: After some time the memory leak symptoms seen on the GW although normal operations is not affected yet, but after all memory is used GW hangs and only manual reboot of the GW can bring it back to service.

  Workaround: There is no workaround.

- CSCsy98510

  Symptoms: COS value presented at UNI is not mapped to EXP bits.

  Workaround: Set inbound policy map to match on COS and then set MPLS EXP to required value.

- CSCsz38342

  Symptoms: FTP traffic is not policy routed.

  Conditions: Above symptom is seen on Cisco routers configured for local PBR with set IP next-hop clause.

  Workaround: Add a static route to the next-hop network.

- CSCsz39167

  Symptoms: Cisco 888G stops forwarding all traffic when there are two flows through it:

  - ping with normal packet size
  - ping with packet size greater than 1500 bytes

  Conditions: This is being seen on a Cisco 888G running Cisco IOS Release 12.4(24)T.

  Workaround: Disabling CEF solves this.

- CSCsz62850

  Symptoms: Intermittent failure of VRF-aware NAT. After an outside-to-inside translation, the packet is routed based on the global routing table instead of the VRF routing table. Affects only 1-2% of traffic.

  Conditions: Occurs in Cisco IOS Release 12.4(23). May not occur in Cisco IOS Release 12.4(10), but this is not yet confirmed.

  Workaround: There is no workaround.

- CSCsz70049

  Symptoms: VIC2-2BRI port go down suddenly by not detecting the RR command/resposnse from telco side. As a result, this BRI port never send/receive the voice call on this port any more.

  Conditions: Cisco 3825 with VIC2-2BRI running Cisco IOS Release 12.4(19b).

Workaround: Issue **clear interface bri** command to restore this state.

- CSCsz89093

  Symptoms: Cisco 2800 router can drop multicast packets.

  Conditions: Stream sources are connected to NM-16ESW switch module.

  Workaround: Disable IGMP snooping.

- CSCsz89646

  Symptoms: H320 does not provide video.

  Conditions: Cisco 2801 platform.

  Workaround: Use Cisco 2811 or 2821.

- CSCsz89826

  Symptoms: The router starts reloading while testing the OAM management functionality over ATM using the encapsulation “aal5mux ppp” which is done after the “encapsulation aal5snap.”

  Conditions: This is observed after configuring **oam-pvc manage 9** under OAM feature.

  Workaround: There is no workaround.

- CSCsz93306

  Symptoms: Cisco IOS SCEP will always reply with the configured hash and encryption algorithm (the default is md5/des), instead of replying with the hash and encryption algorithms used by the client.

  Conditions: Occurs during normal operation.

  Workaround: Not a work-around per-se, but considering the main concern is that less secure algorithms may be used in the reply than the request, administrators can match the algorithms configured for the clients in the IOS CA. That being said, you can only set the hash algorithm, and not the encryption algorithm. For that there is no work-around.

- CSCta13745

  Symptoms: VM notifications sent from CUE to CME SIp trunk may have no audio.

  Conditions: SIP trunk and VM notifications sent to PSTN over the SIP trunk.

  Workaround: There is no workaround.

- CSCta17774

  Symptoms: Abnormally high interarrival jitter time reported in RTCP from the Cisco AS5400 when using Nextport DSPs.

  Conditions: Occurs with Nextport DSPs when using RTCP to measure interarrival jitter values.

  Workaround: There is no workaround.

- CSCta19719

  Symptoms: Router translates host name even though the host is already locally mapped.

  Conditions: Error occurs when configuring a locally mapped host or pinging a locally mapped host.

  Workaround: Use IP address instead of hostname.

- CSCta20590

  Symptoms: A group member pseudotime gets desynchronised after re-registering or at initial registration.

Conditions: GETVPN with Time Based Anti Replay (TBAR) enabled. After establishing phase I, the GM is supposed to get the KEK and TEKs. If there is packet drop (most of the time, this message is fragmented across multiple frames), then the router is not able to reassemble the packet.

Then IKE will resend this message a bit later but the pseudotime has not been recalculated.

Workaround: Disable TBAR or use a very large window (greater than 30 seconds).

- CSCta21492

  Symptoms: PPP call back case is failing.

  Conditions: When MLP is configured under the dialer.

  Workaround: There is no workaround.

- CSCta30439

  Symptoms: G1 and G2 routers may crash.

  Conditions: Occurs when MLP is configured on CJ-PA and OIR is done.

  Workaround: There is no workaround.

- CSCta32434

  Symptoms: MLP+Bridging is not working on Cisco 7200.

  Conditions: Occurs when MLP is configured on CJ-PA and bridging is enabled on multilink interface.

  Workaround: There is no workaround.

- CSCta36701

  Symptoms: Group member with VSA runs out of memory and starts dropping traffic with continuous traffic for 12 hours.

  Conditions: The packet size of the traffic sent was near MTU so that the packets get fragmented before encryption.

  Workaround: Disable VSA.

- CSCta37063

  Symptoms: NAT fails to translate H323 payload information.

  Conditions: Not yet known.

  Workaround: There is no workaround.

- CSCta38154

  Symptoms: Crash with the following error message while configuring or modifying a ZBFW

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  Conditions: Running Cisco IOS Release 12.4(20)T or 12.4(24)T. The problem should exist on Cisco IOS Release 12.4(22)T but that has not been verified yet.

  Workaround: There is no workaround.

- CSCta42633

  Symptoms: Ping fails to a directly connected router after removing “frame-relay payload-compression.”

  Conditions: Ping fails only if frame-relay payload-compression is removed on both the routers connected back-to-back.

  Workaround: Remove and reapply frame-relay map-class under the interface on both of the routers.

- CSCta50110

  Symptoms: GM does not register.

  Conditions: Crypto map is attached to tunnel interface only.

  Workaround: Apply the crypto map to tunnel source physical interface as well.

- CSCta66499

  Symptoms: MGCP gateway may face software-forced reload while re-enabling MGCP with version 1.0 after testing “fgdos” calls with MGCP version 0.1 with Cisco IOS Release 12.4(20)T4 or later.

  Conditions: Signalling type of ds0-group should be “fgdos.”

  Workaround: There is no workaround.

- CSCta69213

  Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

  Conditions: Cisco router running Cisco IOS with the fix for CSCsv40340 configured for NHRP and DMVPN.

  Workaround: There is no workaround.

- CSCta73342

  Symptoms: Noise caused due to concurrent INVITES to same destination and port.

  Conditions: In and out call works fine with good quality voice. Placing calls on hold and resuming works fine. When I press the transfer key, then the phone on PSTN gets MoH. When I complete the transfer, then we have the strange noise again on both ends -like crushing a piece of cardboard and ongoing. Occurs with Cisco IOS Release 12.4(24).

  Workaround: There is no workaround.

- CSCta73534

  Symptoms: Copying a file to the device using SCP fails, but the SCP server returns a “OK (0)” code.

  Conditions: The SCP server did not receive an EOF marker from the SCP client.

  Workaround: There is no workaround.

- CSCta76251

  Symptoms: VPLS AD is not working after BGP has converged.

  Conditions: Reload all the PE routers at the same time.

  Workaround: Apply **mpls ip** on one of the tunnel interface.

- CSCta76698

  Symptoms: PIM Register tunnel would stay in DOWN state in a VRF under certain conditions.

  Conditions:

  1. When VRF has only subinterfaces and no other type of interfaces.
  2. When the configuration is first applied (potentially during startup).
  3. The underlying physical interfaces becomes operationally up, it might not cause the subinterface to be used in bringing PIM register tunnel to UP state.

  Workaround: Doing a shutdown followed by no shutdown on the subinterface will cause this subinterface to be used in bringing PIM register tunnel to UP state.

- CSCta77785

  Symptoms: MGCP ports may be marked with an incorrect status (idle/busy) on the CUCM. This causes calls to be presented to ports it can't traverse, resulting in a fast-busy or causes calls to be rejected that could be put through.

  Conditions: MGCP CAS/PRI trunks with MLPP.

  Workaround: Perform a **shut/noshut** on the controller to allow the channels to resync.

- CSCta77960

  Symptoms: Customer seeing TCB leak with increasing number of sessions stuck in "CLOSEWAIT".

  Conditions: Voice gateway under normal use.

  Workaround: There is no workaround.

- CSCta78212

  Symptoms: Following Cisco IOS upgrade to 12.4(15)T7 with IPS V5, severe drop in throughput for customer traffic when IPS enabled.

  Conditions: This symptom is observed on a Cisco 1841 that is running Cisco IOS Release 12.4(15)T7 image: c1841-advsecurityk9-mz.124-15.T7 IPS-IOS V5.

  Workaround: Deactivate IPS from interface.

- CSCta94467

  Symptoms: When calls are active, the DSP errors happen then the call disconnects.

  Conditions: Normal operation causes this problem to happen.

  Workaround: There is no workaround.

- CSCta95295

  Symptoms: Cisco 7200 router terminating 100+ VPN tunnels, using CRL checking for the Phase 1 authentication. When the CDPs become unavailable (i.e. the router cannot verify the certificate validity) after few hours of working, the IOMEM depleted leading possibly to all traffic failing through the router.

  Conditions: Cisco 7200/NPE-G2 running Cisco IOS Release 12.4(20)Tx, with CRL checking while CDPs unavailable

  Workaround: Disable CRL checking or use pre-shared keys

- CSCta98321

  Symptoms: Not able to configure AAA server for HTTP authentication on Cisco 861 router

  Conditions: Trying to configure AAA server for HTTP authentication on Cisco router.

  Workaround: There is no workaround.

- CSCta98976

  Symptoms: Router crashes when migrating to CA rollover certificate.

  Conditions: Router configured a certificate server. Rollover CA certificate is existing and about to be installed as active CA cert.

  Workaround: There is no workaround.

- CSCtb01178

  Symptoms: Performance testing reveals that degradation occurs in frames per second (FPS) rates.

  Conditions: Occurs on devices running Cisco IOS Release 15.0(1)M.

Workaround: There is no workaround.

- CSCtb05151

  Symptoms: When comparing specific performance metrics between Cisco IOS Release 12.4T and Cisco IOS Release 15.0(1), throughput degradation is observed on select Cisco ISR routers.

  Conditions: This degradation appears to be related to (but not limited to) tested Network Address Translation (NAT) configurations.

  Workaround: There is no workaround.

- CSCtb05967

  Symptoms: The command **analysis-module** is not replicating packets routed from an IP phone.

  Conditions: The symptom is observed on an IP phone communication set up via router to FXO. Ingress interface contains the **analysis-module monitoring** command.

  Workaround: There is no workaround.

- CSCtb08588

  Symptoms: There is no audio when call is placed on hold and then resumed on Cisco AS5400 configured for MGCP.

  Conditions: Cisco AS5400 with SPE DSPs configured for MGCP may get into a no-audio condition when the active call is placed on hold and resumed.

  When this occurs, the output of **show call active voice brief** will show that the packet tx/rx count is not incrementing on the IP call leg.

  Workaround: This function appears to work correctly in later versions of Cisco IOS Release 12.3(11)T somewhere; for example Cisco IOS Release 12.3(11)T10. This appears to be present only in later 12.4 releases of Cisco IOS. Downgrading Cisco IOS if available as an option would be a workaround. Otherwise, no known workaround exists.

- CSCtb09784

  Symptoms: TDM-IP application running on Cisco ISR routers with Cisco IOS Release 15.0(1)M may experience some performance degradation.

  Conditions: Loss is approximately 6% for Cisco 3845 routers, and more so on lower end platforms.

  Workaround: There is no workaround.

- CSCtb11373

  Symptoms: Enabling IPv6 inspection debugs might lead to router crash when traffic is passing through the box.

  Conditions: Issue seen on Cisco IOS Release 12.4(21) with the following debugs:

  - **debug ipv6 inspect tcp**
  - **debug ipv6 inspect detailed**
  - **debug ipv6 inspect events**

  Workaround: Avoid debugging IPv6 inspection.

- CSCtb13015

  Symptoms: Configure a VPN profile (template) cisco-avpair="template:ip-addr=10.10.10.10 255.255.255.255". Bring up a PPPOE session from Client to LNS, call comes up and the virtual-access2.1 on the LNS fails to get the template IP address 10.10.10.10.

  Conditions: When running **per vrf aaa** script, configured vpn profile(template) cisco-avpair= "template:ip-addr=10.10.10.10 255.255.255.255" is not applied to the virtual-access on the LNS.

Workaround: There is no workaround.

- CSCtb17152

  Symptoms: Big packet drop after FRF.12 is applied.

  Conditions: FRF.12 enable.

  Workaround: There is no workaround.

- CSCtb17856

  Symptoms: H323 calls may fail with cause code 41 intermittently. Depending on traffic, after several days, calls may start failing with cause code 47

  Conditions: This may happen when there is a race condition in setting up H245 session between H323 peers and we end up with two separate H245 session simultaneously.

  Workaround: None for cause code 41. But if you start getting too many cause code 47, reload will help alleviate symptoms.

- CSCtb21428

  Symptoms: Interface is not trying to restart after configuring restart-delay.

  Conditions: When the serial interface is down due to some reasons and if you have configured restart-delay on the serial interface, it should try to restart the interface.

  Workaround: There is no workaround.

- CSCtb22889

  Symptoms: SIP (TLS--SIP CUBE may experience up to 2-3 seconds of post dial delay due to TLS processing. Processing delays of 1000 ms, 600ms, and 200ms are seen between the gateway's TLS response.

  Conditions: A TLS connection to another gateway.

  Workaround: The gateway's TLS aging timer can be increased to lower the frequency of the problem with the aging TLS timer:

  sip-ua timers connection aging tls <*time*>

- CSCtb26396

  Symptoms: HTTPS connections suddenly fail with the following error.

  ```
  Jul 25 12:23:12.442: //-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1 Jul
  25 12:23:12.442: //394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL
  socket_connect failed fd(0)
  ```

  Conditions: CVP Standalone deployment running with HTTPS IOS versions Cisco IOS Release 12.4(22)T1 or 12.4(24)T1.

  Workaround: There is no workaround.

- CSCtb26941

  Symptoms: Intermittent echo on voice calls.

  Conditions: A DSP channel, or set of DSP channels, go into a bad state where they no longer cancel echo. The audio stream coming into the DSP will match exactly what is going out. This can be identified by the symptom that the echo-cancellation tail will vary during a call even when the tail is specified on the voice port. Values from 24ms to 112ms have been observed for a single call which this issue occurs on. The command **show call active voice echo-canceller summary** can be used to observe the echo cancellation tail, and the voice-port command **echo-cancel coverage** can be used to statically set the echo cancellation tail.

Workaround: The DSP can be reset, or the gateway can be reloaded, and the echo canceler will begin functioning.

- CSCtb34814

  Symptoms: The following error message is reported just before the crash:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```
  There may not be any tracebacks given for the crash.

  Conditions: Normal use.

  Workaround: There is no workaround.

- CSCtb36578

  Symptoms: Ping fails with **ip nat inside** configuration.

  Conditions: Issue is seen on GigE interface on Cisco 7200.

  Workaround: There is no workaround.

- CSCtb37145

  Symptoms: PPP fails with async_dialer interface type.

  Conditions: This happens only when the interface type is async_dialer. There is no issue with async_legacy or async_virtual interface types.

  Workaround: There is no workaround.

- CSCtb37756

  Symptoms: Cisco router used as client is not authenticated by NAS using EAP Proxy through BRI lines. Configure legacy dialer on the Client. Configure legacy dial on UUT. Configure UUT to use RADIUS Server. Configure Multilink on Client and UUT. Initiating a call from client to UUT will fail.

  Conditions: This issue is seen in routers running Cisco IOS Release 12.4(24.6)PI11r.

  Workaround: There is no workaround.

- CSCtb38071

  Symptoms: While testing Large Scale Dial Out feature, expected number of links are not seen in the bundle after starting calls in both direction for a single client. The traffic is sent for around 10 minutes. Dialer map is formed for the required address.

  Conditions: This issue is seen in routers running Cisco IOS Release 12.4(24.6)PI11r.

  Workaround: There is no workaround.

- CSCtb39345

  Symptoms: When per-user profile has session-timeout value configured the Session-Timeout is not happening in the expected time.

  Conditions: This issue is seen in Cisco IOS Release 15.0(1). VTY session is not getting teardown within configured session-timeout period.

  Workaround: There is no workaround.

- CSCtb39756

  Symptoms: New GM will not be able to communicate to existing GMs.

  Conditions:

  1. Primary KS reloads
  2. Secondary KS takes over role as primary and removes the old TEK and creates a new TEK2

3. During the period where the existing GMs have both old and new TEK keys, any new GM that registers will only get the new TEK. This new GM will not be able to communicate to the existing GMs until the old TEK expires.

Workaround: There is no workaround.

- CSCtb44031

  Symptoms: LDP session goes down and does not re-establish.

  Conditions: Remove password on the LDP session on both peers with **no mpls ldp neigh x.x.x.x password xxxxxx**

  Workaround: There is no workaround.

- CSCtb44167

  Symptoms: Router reloads while testing EAP fast authentication with RADIUS accounting feature.

  Conditions: The symptom is observed when the Cisco 1841 router is running with Cisco IOS Release 12.4(24.6)PI11q.

  Workaround: There is no workaround.

- CSCtb45718

  Symptoms: Router crashed with traceback leading to checkheap.

  Conditions: Router has “ip nat service enable-sym-port” in configuration.

  Workaround: Remove “ip nat service enable-sym-port”.

- CSCtb47337

  Symptoms: Virtual-reassembly is broken when configured on a L2TP dialer interface and VLAN interface. This causes traffic with a size bigger than 1472 to be dropped.

  Conditions: This issue has been observed on a Cisco 3250 running the Cisco IOS Release 12.4(15)T9.

  Workaround: Remove “ip virutal-reassembly” from the dialer interface and only have it configured on the VLAN interface.

- CSCtb51423

  Symptoms: Memory leak and chunks leaks were detected on editing configurations via **netconf** using XML.

  Workaround: There is no workaround.

- CSCtb52200

  Symptoms: Crash happens at 3 level policy in a typical configuration.

  Conditions: If interface has bandwidth configured of very low value and a class in parent policy has bandwidth less than 1000, then adding child policy with priority or bandwidth remaining perc can cause router to crash.

  Workaround: While attaching child policy with priority or bandwidth remaining percent, make sure parent class bandwidth is >= 1kb/s.

- CSCtb55576

  Symptoms: When a HWIC-3G-GSM Cellular interface goes up or down [%LINK-3-UPDOWN event log generated], traffic traversing other interfaces is delayed for ~160-250ms during the %LINK-3-UPDOWN event.

Conditions: This issue has been observed on a Cisco 2811with HWIC-3G-GSM. Any time the Cellular interface experiences a state change traffic routed through the Cisco 2811 is delayed for ~160-250ms.

Workaround: There is no workaround.

- CSCtb56567

  Symptoms: Cisco Voice Gateway experiences memory leak error on CCSIP SPI CONTROL process. It leads router to crash every 4-5 days

  Conditions: The problem occurs when a router is configured with **sip-ua mwi-server** <*ip*> **transport tcp**, but the server specified is not setup to receive SIP and thus replies with TCP resets. This can be caused by misconfigured SIP MWI.

  Workaround: Reload the device regularly to free the memory.

- CSCtb57237

  Symptoms: After a call is resumed from hold, the gateway sends G.729 although G.711 was negotiated in the H.245 messages.

  Conditions: Issue was found in Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCtb58605

  Symptoms: VSA gets into error state after boot up.

  Conditions: Crypto maps are attached.

  Workaround: There is no workaround.

- CSCtb60330

  Symptoms: SVTI tunnel flaps at phase 1 rekey. Line protocol on tunnel interface going down.

  Conditions: Only SVTI tunnels affected. DPDs enabled.

  Workaround: There is no workaround.

- CSCtb62272

  Symptoms: G2 router may crash or G1 gives align correction on Cisco 7200 router.

  Conditions: Occurs when MLP is configured on CJ-PA and OIR is done.

  Workaround: There is no workaround.

- CSCtb63244

  Symptoms: Group member Cisco 7200G2 with VSA crashed while registering to KS.

  Conditions: Get the PKI certificate from CA server and start registration to key server

  Workaround: There is no workaround.

- CSCtb63993

  Symptoms: When using nested access-control child policies, a memory traceback message may be seen when removing the policy from an interface.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCtb64017

  Symptoms: Router reloaded when removing ACL in class map when traffic flowing.

  Conditions: This is happened on Cisco 7200 router with latest image.

Workaround: There is no workaround.

- CSCtb64686

  Symptoms: When vc-bundle is configured and traffic is passed at high rate, the output packet counters show very large value.

  Conditions: This is only seen in FR pvc counters. The **show interface** shows proper output.

  Workaround: There is no workaround.

- CSCtb64927

  Symptoms: After some time (~ 24 hours and after a rekey), some of the VPN tunnels stop encrypting traffic. The encrypt counter for the IPSEC SA shows “0”, while the decrypt counter shows increasing value.

  Conditions: Cisco 7200 with VSA, a large number of tunnels and SAs, and tunnels terminated on a dynamic crypto map with a match statement.

  Workaround: Reloading the chassis fixes the issue for a while or remove the match statement from the dynamic crypto-map.

- CSCtb65151

  Symptoms: Device might crash with a bus error and %ALIGN-1-FATAL: Illegal access to a low address.

  Conditions: Cisco device running Cisco IOS Release 12.4(24)T1 and might affect other releases.

  Workaround: There is no workaround.

- CSCtb66295

  Symptoms: No IP connectivity due to erroneous ARP table.

  Conditions: Occurs when NAT and HSRP are configured on the same interface.

  Workaround: There is no workaround.

- CSCtb66963

  Symptoms: SIP call from a call-forwarded phone to a Cisco IOS VoIP gateway is rejected when INVITE contains a comma in the Diversion Header.

  Conditions: Example on an inbound SIP invite that contains a Diversion field such as this:

  ```
  ---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
  172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
  <sip:5555555555@172.27.128.130>;party=calling;screen=yes;privacy=off From:
  <sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9-3843c1b221cc-53184879? To:
  <sip:15551111111@10.1.134.116> Date: Sat, 29 Aug 2009 08:06:56 GMT Call-ID:
  e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
  User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK,
  UPDATE, REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact:
  <sip:5555555555@172.27.128.130:5070> Expires: 180 Allow-Events: presence
  Session-Expires: 1800 Diversion: "Smith, John"
  <sip:87007@172.27.128.130>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
  Content-Type: application/sdp Content-Length: 214 ----
  ```

  The Cisco IOS gateway will respond back with a:

  ```
  ---- Sent: SIP/2.0 400 Bad Request - 'Malformed CC-Diversion/Diversion/CC-Redirect
  Header' Reason: Q.850;cause=100 From:
  <sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9-3843c1b221cc-53184879
  Content-Length: 0 To: <sip:15551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
  e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
  172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
  ```

Workaround: Modify the diverting name associated with the redirecting device so that it does not contain a comma.

- CSCtb67800

  Symptoms: Memory leak observed when zone-based firewall policy is configured and unconfigured.

  Conditions This is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCtb67967

  Symptoms: PPP fails at LCP stage with VPDN Dial out calls.

  Conditions: Happens in Cisco IOS Release 12.4(24.6)PI11v image. Occurs only in dial out scenario.

  Workaround: There is no workaround.

- CSCtb70595

  Symptoms: A Cisco router may crash.

  Conditions: This has been experienced on a Cisco 2851 running Cisco IOS Release 12.4(25a).

  Workaround: There is no workaround.

- CSCtb71569

  Symptoms: Packet drops happen on LLQ before crypto when service-policy using Hierarchical Shaping is applied to tunnel interface and crypto hardware is used.

  Conditions: Cisco 7200VXR and Crypto hardware (VPN acceleration Module), and running Cisco IOS Release 12.3(22.7) and later, 12.4(12.15b) and later, or 12.4(13.5)T and later releases.

  Workaround: There is no workaround.

- CSCtb71628

  Symptoms: Cisco router crashes with policy-map when trying to change the ACL.

  Conditions: Occurs when QoS is configured.

  Workaround: There is no workaround.

- CSCtb72664

  Symptoms: 100% ingress packet drop with free IO memory depletion issue.

  Conditions: Cisco 3845 [NM-1A-OC3-POM] <-> [NM-1A-OC3-POM] peer in setup above or similar scenario, stressing OC3 at line rate (~84Mbps) with bi-directional traffic will cause this problem along with free IO memory depletion issue.

  Workaround: Do not stress OC3 at line rate. Stopping/reducing the traffic rate would solve free IO memory depletion issue.

- CSCtb82256

  Symptoms: Router will crash.

  Conditions: If the Cisco Unified CallManager XML configuration files are being downloaded to the router and the router is currently processing the pri-group configurations, and if you do **shut** and **no shut** of voice-port and do no ccm-manager config again, the router will crash .

  Workaround: Do not shut voice port at the time of configuration download.

- CSCtb83578

  Symptoms: Severe memory leak with “CCSIP-REGISTER” process.

  Conditions: Occurs on a CME router.

Workaround: There is no workaround.

- CSCtb89424

  Symptoms: System crash while using IP SLA with the following error:

  ```
  19:25:55 CDT Wed Aug 26 2009: Address Error (load or instruction fetch) exception, CPU
  signal 10, PC = 0x424ECCE4
  ```

  Conditions: System crashes while using IP SLA.

  Workaround: There is no workaround.

- CSCtb90496

  Issue: FXO ports intermittently locks up in FXOLS_REMOTE_RELEASE VPM STATE which are MGCP controlled. This causes incoming and outgoing calls to fail.

  Work Around: The only way to recover them is by doing a shut / no shut.

  Version: 12.4(15)T7

- CSCtb90873

  Symptoms: Counters for **class-default class-map** is not reaching zero.

  Conditions: It is seen Cisco 7200 platform.

  Workaround: There is no workaround.

- CSCtb91992

  Symptoms: When running with IOS IPS, the router may crash with chunk related errors.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- CSCtb98159

  Symptoms: TCP connections made to the IP address of an interface on a Cisco 870 router are dropped when IPSec VPN and protocol inspection is configured for the same interface. TCP connections that are dropped are not made over an IPSec connection.

  Conditions: IPSec VPN is configured for the interface. Inspection is configured for the interface with the **ip inspect** command. TCP drops are triggered by a successful IPSec VPN session establishment and termination to the interface.

  Workaround: Removing the inspection or crypto map under the interface configuration resolves the issue.

- CSCtb98508

  Symptoms: A Cisco router may experience a bus error crash.

  Conditions: This has been experienced on a Cisco 2851 running Cisco IOS Release 12.4(20)T3, and configured for voice.

  Workaround: There is no workaround.

- CSCtc03147

  Symptoms: A Cisco 2811 running Cisco IOS Release 12.4(24)T1 and configured with “ip helper-address” statements may crash with a bus error.

  Conditions: It is believed that “ip helper-address” is a requirement in this crash.

  Workaround: Remove “ip helper-address” if possible.

- CSCtc04016

  Symptoms: Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience issues of high CPU utilization.

  Conditions: Under rare conditions the Cisco IOS gateway may get into a state where the processes associated with SIP (as seen in **show process cpu**) may get into a state where they are running extremely high causing further calls through the router to fail.

  This is due to the gateway and 3rd party device in a SIP "491 Request Pending" and ACK loop. This has been shown to occur in environments with large number of SIP REFER transfers.

  This can be seen in **show sip statistics** command and look for the RequestPending value showing an high and increasing output count.

  Workaround: There is no workaround.

- CSCtc04228

  Symptoms: The **mgcp behavior g729-variants static-pt** command is default and will show up in the configuration. This causes a problem when you save the configuration and downgrade to a lower version of IOS where this behavior is not present. There the CLI will now be enabled, when it was not previously.

  Conditions: Downgrade IOS with lower version will enable the CLI.

  Workaround: After downgrading to a lower version where **mgcp behavior g729-variants static-pt** is not the default, configure **no mgcp behavior g729-variants static-pt** to remove the CLI.

- CSCtc04788

  Symptoms: Hairpin calls via Cisco AS5400 failing intermittently.

  Conditions: Issue has been found in c5400-is-mz.124-25.bin image.

  Workaround: Reloading GW resolves issue for approximately two weeks.

Resolved Caveats—Cisco IOS Release 15.0(1)M

All the caveats listed in this section are resolved in Cisco IOS Release 15.0(1)M. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCef82896

  Symptoms: When the user name in the authentication dialog box is left blank, the router unexpectedly reloads.

  Conditions: The symptom is observed when authenticating via the HTTP server. It is observed only when a valid user name was previously configured:

  ```
  (config)#ip http authentication local
  (config)#username name privilege number password password
  ```

  Workaround: Do not leave the user name blank in the authentication text box, if username authentication is enabled.

- 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.

- CSCsd77560

  Symptoms: SNMPv3 “auth” and “priv” users are lost across reload.

  Conditions: Occurs after a reload.

  Workaround: There is no workaround.

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

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

  This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsi43340

  Symptoms: DSMP is not programming the DSP for supervisory tone while alerting tone is there, which leads to FXO disconnect supervision issue.

  Conditions: Occurs on routers running Cisco IOS Release 12.3(14)T and later releases.

  Workaround: Downgrade to Cisco IOS Release 12.3(11)T.

- CSCsi82425

  Symptoms: When a secondary IP address is removed from an interface, the entire ARP table may be flushed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2((33)SRB.

  Workaround: There is no workaround.

- CSCsj37160

  Symptoms: Cisco Express Forwarding (CEF) adjacency is going incomplete and local users are down. This may result in packet loss.

  Conditions: When the Peak rate on the ATM PVP is changed and “atm route-bridge ip” is configured on subinterface, then adjacency goes to “incomplete” state.

  ```
  Config t
  interface ATM1/0
  atm pvp 11 3000 << change
  sh ip cef vrf Internet det | incl com
  Adj source: IP adj out of ATM1/0.44604, addr x.x.x.x (incomplete)
  ```

  Workaround: Clear adjanency or perform a **shut/no shut** on the ATM interface.

- CSCsk80396

  Symptoms: Router crashes when jitter operation takes place.

  Conditions: This crash is inconsistent and is seen while auto Ethernet operation is configured to carry on jitter operation on an interface configured with **no ethernet cfm enable**.

  Workaround: There is no workaround.

- CSCsl15443

  Symptoms: Console port can lock up after 10-15 minutes. Telnet sessions fail.

  Conditions: Occurs when terminal server is connected to router’s console port.

  Workaround: There is no workaround.

- CSCsl52962

  Symptoms: The RP crashes due to a watchdog timeout of the uRPF stats process.

  Conditions: The symptom is observed when issuing the **interface range port-channel** <*number*> - <*number*> command.

  Workaround: There is no workaround.

- CSCsm87925

  Symptoms: Memory leak occurs in SSGCmdQue

  Conditions: Occurs on routers configured for Service Selection Gateway (SSG) and running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCso05336

  Symptoms: A Cisco 1811 router reloads when trying to connect to irc.freenode.net during the first 36 hours following a reload.

  Conditions: The symptom is observed only in the first 36 hours following a reload.

  Workaround: Do not connect to irc.freenode.net the first 36 hours following a reload.

- CSCso69413

  Symptoms: A Cisco router may reload when Flexible Packet Matching is configured.

  Conditions: This symptom occurs when a class is configured to match on a protocol field when the protocol stack has not been defined. The stack class- map is required for all field references.

  Workaround: Specify the exact bits to be matched with the **match start** command.

- CSCso85618

  Symptoms:

  1. The MOH does not work between CM and CME.
  2. There is no audio on the CME endpoint when the remote CCM party resumes the call on hold, conferences, or transfers with another CCM endpoint (scenario: CME - CUBE - CCM).

  Conditions: Symptom 1 is observed if the phone registered to the CME is put on hold by the CM, then the CME phone does not hear the MOH.

  Symptom 2 is observed if the CCM endpoint does a conference, hold, or transfer.

  Workaround: Use an MTP.

- 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.

- CSCsq31605

  Symptoms: On a Cisco Catalyst 6500 series switch, 802.1X authentication may not complete if an attempt is made to clear the session in the middle of authentication.

  Conditions: The symptom is observed if 802.1X is configured and the **clear authentication session** command is issued while authentication is occurring.

  Workaround: Do not clear the session before the end of authentication.

- CSCsq42671

  Symptoms: LiveRcd softkey label is shown as "???" instead of localized string.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(15)XZ with Japanese locale.

  Workaround: There is no workaround.

- CSCsq58289

  Symptoms: The connected interface prefix that is redistributed to OSPF is not seen as a Type 5 LSA in the OSPF database.

  Conditions: The symptom is observed with the prefix that is initially covered by a “network ...” statement under **router ospf ...** and later removed by doing **no router ospf ...** instead of **no network ...**.

  Workaround: Perform a **shut** then **no shut** on the interface with the prefix that is not being redistributed.

- CSCsq93893

  Symptoms: Router crashes while issuing show policy-map interface.

  Conditions: The above symptom is seen on a Cisco 3800 router running Cisco IOS Release 12.4(19.18)T6.

  Workaround: There is no workaround.

- 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 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.

- 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.

- CSCsr27727

  Symptoms: A Cisco Catalyst 6000 reports the following message and unexpectedly reloads:

  ```
  %SYS-2-ASSERTION_FAILED: Assertion failed: “wccp_acl_item_valid(item,NULL)”
  ```

  Conditions: This symptom is observed on a WS-C6509 that is running Cisco IOS Release 12.2(33)SXH2a.

  A WCCP service is configured with a redirect-list referring to a simple ACL.

Workaround: Use an extended ACL as the WCCP redirect-list.

- CSCsr40935

  Symptoms: Router crashes when service policy is applied while traffic is flowing.

  Conditions: Occurs on a Cisco 7200 after applying policy map on PVC with traffic.

  Workaround: Stop traffic before applying service policy map.

- CSCsr41631

  Symptoms: AnyConnect client is connecting to a Cisco ISR router that is running Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled. Client is unable to reach the inside interface IP address but can communicate with devices behind the router.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled

  Workaround: Disable CEF globally and/or disable hardware encryption.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

  Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr53059

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

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

  Workaround: There is no workaround.

- CSCsr60092

  Symptoms: One-way audio is observed after use of TCL [connection create] command.

  Conditions: Occurs with TCL application playing media in incoming_leg and leg setup without bridging incoming leg [leg setup $dnis callInfo].

  Workaround: There is no workaround.

- CSCsr62645

  Symptoms: Software-forced reload occurs on Cisco 870 router.

  Conditions: Encountered during extended VLAN testing.

  Workaround: There is no workaround.

- CSCsr88705

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

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

  Workaround: Undo and redo the redistribution.

- 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
  ```

- CSCsu02975

  Symptoms: Router crashes due to memory corruption

  Conditions: WAN router crashes when feature combination includes Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC The issue is seen only when frame-relay fragment and service-policy is part of map-class frame-relay configs

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configurations.

- CSCsu05186

  Symptoms: The following command does not work:

  dot1x timeout supp-response dot1x timeout reauth-period

  Conditions: Occurs when configuring wireless on a Cisco 871 router.

  Workaround: There is no workaround.

- CSCsu32452

  Symptoms: Spurious memory access occurs.

  Conditions: Occurs while attempting to unconfigure the EzVPN client configuration on an EzVPN client inbound interface.

  Workaround: There is no workaround.

- CSCsu53603

  Symptoms: Router crashes after removing the VCs. All PPP sessions are torn down.

  Conditions: This is a legacy problem. It happens in all images.

  Workaround: Disable over-subscription for all PPP connection.

  Further Problem Description: PPP session should be UP with the default bandwidth even if over-subscription is disabled.

- CSCsu58763

  Symptoms: Card crashed upon attaching the policy-map to the output interface.

  Conditions: Happening in all types of VCs (PVC/SVC) when the service policy is defined with **shape** command.

Workaround: There is no workaround.

- CSCsu65401

  Symptoms: Commands run using the **tclsh exec command** fail with the error:

  Command authorization failed.

  Conditions: This occurs in Cisco IOS Release 12.4(20)T if the following is configured on the device:

  aaa authorization commands 15 default group tacacs+

  Workaround: The username being passed to the AAA server is an empty string. If there is a default profile on the AAA server that allows all commands to be run, then the **tclsh** exec commands will work. Otherwise there is no workaround.

- CSCsu78975

  Symptoms: Crash seen @adj_switch_ipv4_generic_les on a Cisco 38xx 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.

- CSCsu79754

  Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

  Conditions: Unknown at this time.

  Workaround: Create an ACL to drop PIM packets to such interfaces.

- CSCsu92300

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

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

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

- CSCsu92724

  Symptoms: The following errors are logged:

  ```
  Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
  ../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
  -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
  0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT:
  INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99 Sep 21 05:07:25: %SYS-2-QCOUNT:
  Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback=
  0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:25:
  %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99
  Sep 21 05:07:25: %SYS-2-QCOUNT: Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl=
  4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238
  0x600B220C Sep 21 05:07:25: %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at
  ../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNT: Bad dequeue 62D74734 count
  -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C
  0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:28: %ISDN-4-ISDN_UNEXPECTED_EVENT:
  INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99 Sep 21 05:07:28: %SYS-2-QCOUNT:
  Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl= 4, pid= 162 -Traceback=
  0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238 0x600B220C Sep 21 05:07:28:
  %ISDN-4-ISDN_UNEXPECTED_EVENT: INVALID INPUT: Occurred at ../isdn/isdnif_modem.c:99
  Sep 21 05:07:28: %SYS-2-QCOUNT: Bad dequeue 62D74734 count -1 -Process= "ISDN", ipl=
  4, pid= 162 -Traceback= 0x6046769C 0x605B2E64 0x60158F0C 0x600B2204 0x600B2238
  0x600B220C
  ```

  Conditions: Occurs when ISDN is enabled.

Workaround: There is no workaround.

- CSCsu96684

  Symptoms: Inband to RTP-NTE is failing for a slow start to slow start call.

  Conditions: The symptom is observed when inband DTMF is configured in the incoming leg and RTP-NTE is configured in the outgoing leg of CUBE.

  Workaround: Configure RTP-NTE on both legs of CUBE.

  Further Problem Description: In the set up SIP Ph1-CUCM1-CUBE-CUCM2-SIP Ph2, there is no DTMF tone heard on SIP Ph2 when pressing digits on SIP Ph1. If pressing digits on SIP Ph1, CUCM is sending RTP-NTE and CUBE is not sending this to other leg. This is because CUBE is sending RTP-NTE in the TCS towards CUCM1, which it should not do.

- CSCsv09180

  Symptoms: Router will crash upon removing service policy and DLCI associated with a frame-relay interface.

  Conditions: The router if the following steps are performed in the order given:

  1. Configure frame-relay encapsulation on serial interface and assign IP address.
  2. Configure header compression on it through policy-map using the **service-policy output** command.
  3. Associate the interface with DLCI using the **frame-relay interface-dlci** command.
  4. Configure the remote router in a similar fashion and ensure both interfaces ping each other.
  5. Remove the policy-map on local router using the **no service-policy output** command.
  6. Remove the DLCI associated using the **no frame-relay interface-dlci** command. This causes the router to crash.

  Workaround: There is no workaround.

- CSCsv13392

  Symptoms: If an hierarchical QoS policy-map with priority action is applied to an interface that has encryption enabled, queuing should be enabled on the crypto engine, but it is not.

  Conditions: The symptom is observed with Cisco IOS Releases from 12.4(20)T onwards.

  Workaround: There is no workaround.

  Further Problem Description: Flat QoS policies enable crypto engine queuing as expected.

- CSCsv17698

  Symptoms: Packets may be incorrectly classified under child and parent classes.

  Conditions: The symptom is observed when a two or three-level policy is configured/reconfigured coupled with the command **clear counters**. The symptom also occurs if a second level policy-map is detached and then re-attached to a grandparent policy. Some of the packets go through the intended parent (or grandparent) class and incorrectly go through the default class or no class at all of the child policy.

  The issue is seen with a Cisco 7200 series router that is running Cisco IOS Release 12.4(20)T2, 12.4(22)T2 or 12.4(24)T.

  Workaround: Reload the router. In some cases, unconfiguring and reconfiguring the policies will work.

- 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.

- CSCsv28451

  Symptoms: A Cisco 7600 PE router fails to redistribute a VRF prefix into BGP after the prefix or path to it flaps. The PE router will indicate the prefix being redistributed into BGP but the prefix will not get installed into the BGP table until the prefix is cleared:

  ```
  PE2#sh ip route vrf foo 10.5.5.5
  Routing Table: foo Routing entry for 10.5.5.5/32 Known via "ospf 1", distance 110,
  metric 20, type extern 2, forward metric 10 Redistributing via bgp 666 Advertised by
  bgp 666 metric 10 match internal external 1 & 2 Last update from 10.45.45.2 on
  Ethernet1/0, 00:00:56 ago Routing Descriptor Blocks: * 10.45.45.2, from 10.5.5.5,
  00:00:56 ago, via Ethernet1/0 Route metric is 20, traffic share count is 1 PE2# PE2#sh
  ip bgp vpnv4 vrf foo 10.5.5.5 % Network not in table PE2#
  ```

  Conditions: The PE router redistributing the given prefix must have a sham-link configured for the given VRF and an alternate path to the prefix must exist once the primary (sham-link) is down.

  Workaround: Use the following command: **clear ip route vrf vrfname** *prefix*.

  Further Problem Description: This problem is seen only in Cisco IOS Release 12.2(33)SRB. Cisco IOS Releases 12.2(33)SRC/SRD, etc. are not affected.

- CSCsv29720

  Symptoms: When Cisco IOS software is secured using the **secure boot-image** command, doing a **fsck** and **format** on the flash removes the secured image.

  Conditions: This symptom occurs when securing Cisco IOS software using the **secure boot-image** command and when the **fsck** followed by **format** commands are executed continuously on the flash.

  Workaround: Do not format flash immediately after the file check and try “dir” before formatting.

- CSCsv40340

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

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(15)T7. The router is configured with NHRP.

  Workaround: There is no workaround.

- CSCsv62323

  Symptoms: The Fast Ethernet driver code may cause several errors. The observed symptoms of this issue include:

  - Cisco Unified Communications 500 series routers (UC520) may crash with an “Unexpected exception to CPU” error.

  - Cisco 1861 router may fail to establish L2TPv3 session with an error message:

  ```
  "%L2TP-3-ILLEGAL: _____:________: ERROR: unsupported transport protocol; defaulting to
  UDP if possible"
  ```

  Conditions: The symptoms are observed with the following hardware platforms: UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS and Cisco 1861 routers. In addition, the following conditions exist:

  – The UC520 must be configured with a BVI interface. For example:

    interface BVI1 ip address 192.168.0.1 255.255.255.0

  – The Cisco 1861 router is configured with L2TPv3. For example:

  ```
  pseudowire-class l2tpv3 encapsulation l2tpv3 ip local interface Loopback0 ! interface
  Loopback0 ip address 192.168.10.1 255.255.255.255 ! interface FastEthernet0 no ip
  address xconnect 192.168.0.1 1 pw-class l2tpv3
  ```

  Workaround: There is no workaround.

  Further Problem Description: The issue is caused by an underlying driver vulnerability that exists in the UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS and Cisco 1861 routers. No other model of Cisco routers/switches are known to be affected by this issue. The symptoms can be triggered with specific TCP sequences.

- CSCsv62960

  Symptoms: A session service policy with “police cir percent” configuration in the child calculates an actual “cir” of 0 bps.

  Conditions: This can occur when modifying the policy map while it is attached to a session.

  Workaround: Use fixed rate police “cir” rather than percent.

- CSCsv65867

  Symptoms: NM-CEM-4SER modules installed in Cisco 3845 routers will not use network clock if one is available. Instead, they will use the local oscillator. This can be observed by using the **show cem** *slot/port/0* command.

  Conditions: This behavior is observed on a NM-CEM-4SER module installed in Cisco 3845 routers running Cisco IOS Release 12.4(20)T or later.

  Workaround: Use adaptive clocking to improve clock accuracy.

- CSCsv73754

  Symptoms: A Cisco 10000 series router crashes. Traceback decode points to a function of bgp_vpn_impq_add_vrfs_cfg_changes.

  Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 VRFs or more are unconfigured.

  Workaround: There is no workaround.

- CSCsv79584

  Symptoms: An 0.0.0.0 binding with a 0 minute lease gets created and subsequently removed on the DHCP unnumbered relay.

Conditions: The DHCP client sends a DHCPINFORM with ciaddr set to its address, but giaddr is empty. The relay fills in giaddr with its IP address and the server replies to giaddr. Since the DHCPACK is in response to DHCPINFOM, the lease-time option is absent. Relay receives the DHCPACK and tries to process it normally leading to the route addition.

Workaround: There is no workaround.

Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining “debug ip routing” for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv82317

  Symptoms: WIC-4SHDSL: Inconsistency in train up with m-pair Annex interchange.

  Conditions: With the HWIC-4SHDSL scenario, when we create mpair DSL group link, it may fail to train with default B annex. Sometimes with annex B trains up, but when we interchange to annex A, it fails to train up. Also sometimes when we issue **shut/no shut** on CPE/CO side, it fails to train up.

  Workaround: Swapping the termination mode and reloading both the routers may bring up the line successfully. It can be repeated multiple times if controller line does not train properly in the back-to-back setup. This workaround may not be suitable in a customer environment.

- CSCsv85530

  Symptoms: When accounting is enabled for virtual private dial-up network (VPDN), there might be messages with termination cause “nas-error” and displaying impossible values in Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets.

  This causes accounting to be unreliable.

  Conditions: Occurs with Cisco IOS Release 12.4T and configured for PPTP/L2TP with accounting.

  Workaround: There is no workaround.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsv96409

  Symptoms: Router crashes VFR is enabled and CEF is turned off.

  Workaround: Disable VFR using the **no ip virtual reassembly** command.

  Workaround: There is no workaround.

- CSCsv96630

  Symptoms: Memory leak occurs on ISR transcoder router.

  Conditions: Occurs when the secure option is added to a transcoder configuration in a topology with a Cisco Unified Communication Manager 7.1.

  Workaround: Remove the secure configuration from the transcoder.

- 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.

- CSCsw22791

  Symptoms: The router may crash if Group Domain of Interpretation (GDOI) configurations are removed concurrently with the execution of the **show crypto gdoi** command (that is, they are running on different TTY sessions).

  Conditions: The symptom is observed when the removal of the configurations and the execution of the show command are concurrent.

  Workaround: Avoid removing the configuration and executing the **show crypto gdoi** command concurrently.

- CSCsw23314

  Symptoms: A router reloads when a manually keyed crypto map is removed from an interface after unconfiguring the tunnel source.

  Conditions: The symptom is observed when the manually keyed crypto map is applied on the tunnel interface. The crash happens when the user cuts and pastes several “no” forms of the CLI in order to delete the tunnel source interface as well as removing the crypto from the tunnel and deleting the tunnel interface itself:

  ```
  conf t int tunnel0 no ip addr x.x.x.x x.x.x.x no tunnel source e1/0 no tunnel dest
  y.y.y.y no crypto map ! must be a manually keyed crypto map exit no interface tunnel0
  ```

  The issue occurs only on a Cisco 7200 series router with VSA, a Cisco ASR 1000, or a Cisco Catalyst 6000 Series Switch with VPNSPA.

  Workaround: Enter the commands one at a time, waiting after removing the tunnel source. This will prevent the race condition from occurring, avoiding the crash.

- 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.

- CSCsw29463

  Symptoms: The router, which is configured as a hub in a Dynamic Multipoint VPN (DMVPN), may reload unexpectedly.

  Conditions: The symptom is observed periodically in a scaled configuration when the router is connected to a live network and traffic is passing.

  Workaround: There is no workaround.

- CSCsw29664

  Symptoms: After using the command **process restart** *iprouting.iosproc*, BGP address-family IPv6 members are enabled as BGP address-family IPv4 members.

  Conditions: The symptom is observed after using the **process restart** *iprouting.iosproc* command.

  Workaround: Configure “no bgp default ipv4-unicast”.

- CSCsw31207

  Symptoms: Cisco 1841 crashes on issuing the **show controllers shdsl <>** command.

  Conditions: Setup Used: Cisco 1841 [HWIC-4SHDSL/CO] <-> Cisco 2821 [CPE/HWIC-4SHDSL]

  On the above setup, having the following configurations (not a proper configuration though) and issuing the **show controllers shdsl <>** command, the Cisco 1841 crashes. The problem is observed with back-to-back setup and currently it is not known if this can occur on customer setup.

  CO Side:

```
controller SHDSL 0/0/0
termination co
dsl-group 0 pairs 0, 1, 2, 3 ima
shdsl annex A
```

  CPE Side:

```
controller SHDSL 0/3/0
termination cpe
dsl-group 0 pairs 0
shdsl annex A
!
dsl-group 1 pairs 1, 2, 3 ima
shdsl rate auto
```

  Workaround: There is no workaround.

- CSCsw31242

  Symptoms: A memory allocation failure and IO memory depletion is seen when an IP ICMP packet is sent with an SRC address and destination IP address as same as the PPC's interface address.

  Conditions: The symptom is observed on a Cisco 7200 series router when the IP/ICMP is sent to a BVI interface with the same SRC and destination address.

  Workaround: There is no workaround.

- CSCsw32795

  Symptoms: Key server crashes during configuration.

  Conditions: Occurs when key server is configured with two or more GDOI groups.

  Workaround: There is no workaround.

- CSCsw36397

  Symptoms: VoIP RTP connections may dangle at TGW when a call failure occurs, due to a performance test.

  Conditions: The symptom is observed during performance testing with many calls (more than 600) run for any duration above 5 minutes. The call failure occurs due to a network timeout issue from SIP server (acting as proxy server) causing hung VoIP connections at the TGW.

  Workaround: There is no workaround.

  Further Problem Description: The problem appears when the SIP server in the network delays responding to the messages sent from OGW and TGW due to network delays. The TGW is unable to clear the VoIP RTP sessions causing the hung RTP connections. If the calls run for more than an hour, the memory gets exhausted in the TGW causing it to crash.

- CSCsw37279

  Symptoms: When using PKI for identifying group members, a group member may fail to register with the key server if the certificate is not installed at the time that Group Domain of Interpretation (GDOI) is enabled.

  Conditions: The symptom is observed when SCEP is used for certificate enrolment.

Workaround: Clear the current GDOI registration with the following command: **clear crypto gdoi**.

- CSCsw40203

  Symptoms: A Cisco ASR 1000 may crash with certain malformed IKE packets.

  Conditions: This symptom is observed on a Cisco ASR 1000 that is configured for IPSec VPN with digital certificates.

  Workaround: There is no workaround.

- CSCsw43211

  Symptoms: Following errors are seen:

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

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

  Workaround: There is no workaround.

- CSCsw52277

  Symptoms: The previous primary crashes.

  Conditions: Occurs when a fresh Key Server with higher priority comes up and election is triggered.

  Workaround: There is no workaround.

- CSCsw52416

  Symptoms: Dynamic NAT entries are not timing out properly

  Conditions: Occurs even after timer expired.

  Workaround: There is no workaround.

- CSCsw52855

  Symptoms: CRC and Frame errors are seen if mark was used as the idle character between packets

  Conditions: This problem occurs when using the following interface cards:

  - VWIC2-1MFT-T1/E1
  - VWIC2-2MFT-T1/E1
  - VWIC2-1MFT-G703
  - VWIC2-2MFT-G703

  Workaround: Use the following interface cards that are not affected by this problem:

  - HWIC-4T1/E1
  - HWIC-2CE1T1-PRI
  - HWIC-1CE1T1-PRI

  This caveat is Closed.

- CSCsw52932

  Symptoms: Group members' rekey SAs that have the same IKE SA endpoints (source/destination addresses) are mistakenly deleted when one of the group members has to re-register.

  Conditions: This occurs when one of the group members has to re-register.

  Workaround: Have all the group members re-register at the same time (e.g. reapply the crypto map or use the **clear crypto gdoi** command).

- CSCsw62997

  Symptoms: Traceback is seen while configuring a policy in the virtual-template on LAC.

  Conditions: The symptom is observed when the class-map under the policy has the following filter:

  ```
  match vlan <vlan-id>
  ```
  Workaround: There is no workaround.

- CSCsw63222

  Symptoms: Spurious memory access and tracebacks are seen.

  Conditions: The symptoms are observed while attaching the group to the user in the local radius server configuration.

  Workaround: There is no workaround.

- CSCsw65933

  Symptoms: The CE does not learn the prefix from one of the PEs.

  Conditions: The symptom is observed after configuring (on PE2):

  ```
  router bgp 10 address-family ipv4 vrf test1 no neighbor <peer > route-map setsoo in
  end
  ```
  and then clearing using the following command: **clear ip bgp** *peer vrf test1* **soft out**.

  Workaround: Use the command **clear ip bgp * soft** on the PE after SOO is applied.

  Alternate Workaround: On the CE, the command **clear ip bgp * soft** should not be applied within one minute after applying SOO route map to CE on UUT.

- CSCsw67252

  Symptoms: When RTP-NTE and T.38 are both enabled, the re-invite for T.38 incorrectly includes Session Description Protocol (SDP) with RTP-NTE.

  Conditions: Occurs when both RTP-NTE and T.38 are enabled.

  Workaround: There is no workaround.

- CSCsw68882

  Symptoms: MGCP gateway faces software-forced reload when FGDOS endpoint is configured in Cisco IOS Release 12.4(23.12).

  Conditions: The symptom is observed when FGDOS endpoint is configured and MGCPAPP configured in POTS dial-peer for FGDOS voice-port.

  Workaround: There is no workaround.

- 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
  ```
- CSCsw70204

  Symptoms: WISPr attributes could cause memory leak in ProxyLogon situation.

  Conditions: The symptom is observed when the subscriber logs on using WISPr attributes.

  Workaround: There is no workaround.

- CSCsw73196

  Symptoms: BGP MDT session flaps when a router running Cisco IOS is interoperating with a router running Cisco IOS-XR and when withdrawal messages are sent by IOS to XR of previously advertised MDT prefixes.

  Conditions: MDT prefixes need to be exchanged by IOS and XR routers. If a withdrawal message is exchanged subsequently for any reason then this problem is seen.

  Workaround: There is no workaround.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/subinterface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78879

  Symptoms: The secondary key server crashes when it sends a KEK rekey to the GMs soon after it takes over as the primary key server.

  Conditions: The symptom is seen when the secondary key server switches to primary just before it is time to send the KEK rekeys to the group members. This problem can be seen in any co-operative key server environment.

  Workaround: There is no workaround.

- CSCsw79891

  Symptoms: Cisco 3845 gateway may not detect an H.263 video during a video call.

  Conditions: The symptom is observed with a Cisco 3845 gateway when loaded with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsw80640

  Symptoms: A Cisco router may experience the following errors:

  ```
  %SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 659594E0 -Process= "IP
  Input", ipl= 4, pid= 93, -Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534
  0x612D6A44 0x612D8368 0x612D8780 0x612D883C 0x612D8A84 %SYS-2-SHARED: Attempt to
  return buffer with sharecount 0, ptr= 6649466C -Process= "IP Input", ipl= 4, pid= 93,
  -Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534 0x612D6A44 0x612D8368
  0x612D8780 0x612D883C 0x612D8A84
  ```

  Conditions: This symptom is observed on a Cisco 2801 router that is running Cisco IOS Release 12.4(20)T. The errors appear to be triggered with the forwarding of UDP packets.

  Workaround: There is no workaround. The problem does not appear to be service impacting.

- CSCsw84994

  Symptoms: A Cisco 7301 router may experience a lot of CPU hogs due to the SSGTimeout process:

  ```
  %SYS-3-CPUHOG: Task is running for (2008)msecs, more than (2000)msecs (116/59),process
  = SSGTimeout.
  ```

  Conditions: The symptom is observed on a Cisco 7301 router that is running Cisco IOS Release 12.4(21).

  Workaround: There is no workaround.

- CSCsw85293

  Symptoms: The following CPUHOG messages are seen for Crypto ACL process:

  ```
  %SYS-3-CPUHOG: Task is running for (xxxx)msecs, more than (2000)msecs (9/7),process =
  Crypto ACL.
  ```

  Conditions: This has been seen on Cisco routers that are running Cisco IOS Release 12.4(15)T8 (other versions may be affected as well) with GETVPN configured.

  Workaround: Reducing the size and complexity of the crypto ACLs will often stop these errors.

- CSCsw90340

  Symptoms: Traffic flows with loopback on a Cisco 7200 router.

  Conditions: Occurs when you **shut** the controller, configure loopback, then **no shut** the controller.

  Workaround: There is no workaround.

- 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.

- CSCsw97262

  Symptoms: The command **analysis-module** is not replicating packets routed from an IP Phone.

  Conditions: The symptom is observed on an IP Phone communication set up via router to FXO. Ingress interface contains the **analysis-module monitoring** command.

  Workaround: There is no workaround.

- CSCsw98414

  Symptoms: The **ip nat inside source ... match-in-vrf** command is not working without the **overload** option.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T8.

  Workaround: There is no workaround.

- CSCsw99846

  Symptoms: With mLDP over a P2P tunnel, traffic drops in multiple cases.

  Conditions: The traffic drops when there is a change in path set entries, which can happen when you perform a **shut** and **no shut** the TE tunnel or toggle MPLS traffic-tunnel or use the **clear mpls traffic-eng auto-tunnel** command.

  Workaround: There is no workaround.

- CSCsx03120

  Symptoms: When an ATM interface on a WIC1-ADSL comes back up after a flap, under some undefined circumstances, it may be observed that none of the configured PVCs forward traffic.

  Conditions: Specific conditions are still under investigation.

  Workaround: Perform a **shut/no shut** on the interface or power-cycle the router.

- CSCsx03301

  Symptoms: Crash in TCP.

  Conditions: Happens when clearing a BGP neighbor. The trigger is uncertain and hard to reproduce.

  Workaround: There is no workaround.

- CSCsx05494

  Symptoms: There is a rapid memory leak.

  Conditions: The symptom is observed with a running configuration with Zone-based Firewall (ZBFW) and QOS setup.

  Workaround: There is no workaround.

- CSCsx07423

  Symptoms: The router stays at 100% CPU usage after trying to establish an SSL session with an SSL server when this SSL server is not reachable.

  Conditions: The symptom is observed with any applications on the router that use an SSL client to establish a secure session with the SSL server. At the same time, the secure server is not available for whatever reason.

  Workaround: Make sure the SSL server is reachable by pinging it. Save the configuration as startup-config and reload the router.

- CSCsx08292

  Symptoms: When Service Policy is applied under the PVC, traffic flow across that interface stops.

  Conditions: The ping failure starts only after service-policy configuration.

  Workaround: There is no workaround.

- CSCsx08294

  Symptoms: A Cisco 6500 running Cisco IOS Release 12.2(33)SXH may encounter a bus error due to OSPF processes.

  Conditions: Occurs when the device is configured for OSPF Incremental SPF and Virtual Links.

  Workaround: Do not use Incremental SPF.

- 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.

- CSCsx12596

  Symptoms: A router crashes at list_create.

  Conditions: The symptom is observed when the **show archive config differences** command is applied on the router.

  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.

- CSCsx14637

  Symptoms: Modem pass-through calls failing while handshaking

  Conditions: Problem appeared after upgrade from Cisco IOS Release 12.3(26) to Cisco IOS Release 12.4(23).

  Workaround: There is no workaround.

- CSCsx14806

  Symptoms: If you change the IP address of the local address interface from a non-zero value to another non-zero value (for example: from 10.1.1.1 to 10.2.2.2), detach is called but attach is not, and traffic goes out in clear.

  Conditions: The symptom is observed only with crypto configured with a local address.

  Workarounds:

  1. Before changing the local address on the crypto map, shut the interface and remove the crypto map. Following this, re-add the crypto map to the interface.
  2. If you have to change the local address while the crypto map is applied on the interface, instead of directly changing the IP address of the local-address interface, follow the steps below:
  a. a. gig0/3 - ip 1.1.1.1 b. gig0/3 - no ip add c. gig0/3 - ip add 2.2.2.2
  3. Put an outbound ACL on the physical interface that has the crypto map applied. This will drop any cleartext traffic that should have been encrypted.

- CSCsx15138

  Symptoms: Device crashes upon entering command **sh policy-map interface**.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx15358

  Symptoms: A router may crash after receiving DNS TCP queries.

  Conditions: The symptom is observed on a router with “ip dns server” configured.

  Workaround: There is no workaround.

- CSCsx15841

  Symptoms: The **BGP aggregate-address** command configured on active RP does not auto-sync to the running configuration of the standby RP.

  Conditions: Occurs when BGP is configured on active/standby redundant RP system.

  Workaround: Configure BGP aggregate-address and reboot the system, forcing both active and standby to load from startup configuration.

- 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.

- CSCsx19184

  Symptoms: Router crash due to Address Error:

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

  Conditions: This has been seen on Cisco routers running 12.4T and 12.4 images with SIP traffic.

  Workaround: There is no workaround.

- CSCsx20984

  Symptoms: Router reloads with a bus error and no tracebacks.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx22711

  Symptoms: GLBP IPv6 groups configured on an interface will remain in the Active state and will continue to use packet buffers in an attempt to send GLBP messages to other peers. Buffer exhaustion may occur in configurations involving a number of GLBP groups which can result in an automatic reload of the platform.

  Conditions: The symptom is observed when the GLBP IPv6 groups are configured and running on an operational IPv6 interface, and you subsequently remove or modify the IPv6 interface address without first shutting down the interface.

  Workaround: The interface should be shut down before the IPv6 interface address is removed or modified.

- CSCsx23602

  Symptoms: Catalyst 6000 running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

  Conditions: Occurs when running modular IOS with NAT deployment. Crash only happening in production, and NAT translation is required for crash to occur.

  Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx24996

  Symptoms: Removing tunnel configuration can cause the router to crash.

  Conditions: Occurs when the tunnel is removed while QoS is active on that tunnel.

  Workaround: Stop traffic to the tunnel, remove QoS and then delete the tunnel configuration.

- CSCsx25725

  Symptoms: Router crashes with “ip dns view ezvpn-internal-view” configuration.

  Conditions: The symptom occurs after configuring “no ip dns view ezvpn-internal-view” in CTY and “domain name-server 10.1.1.2" in VTY.

  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.

- 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.

- CSCsx32061

  Symptoms: The fax T38 call setup on an H323-SIP leg fails due to incorrect 200 OK message generation on the SIP side. This causes ACK timeouts on the SIP side.

  Conditions: The symptom is observed after a midcall reinvite for T38. The SIP leg responds with a 100 trying and a 200 OK right away without waiting for H323 negotiation to complete.

  Workaround: Using SIP-SIP instead of H323-SIP.

- CSCsx33622

  Symptoms: Flapping BGP sessions are seen in the network when a Cisco IOS application sends full-length segments along with TCP options.

  Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the non-fixed Cisco IOS device. ICMP unreachables toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

  Workaround: Any value lower than the advertised MSS from the peer should always work.

  Setting the MSS to a slightly lower value (-20 to -40) is sufficient to avoid the issue. This number actually accounts for the length of TCP options present in each segment. The maximum length of TCP option bytes is 40.

  If the customer is using MD5, Timestamp, and SACK, the current MSS should be decreased by 40 bytes. However, if the customer is using only MD5, the current MSS should be decreased by 20 bytes. This should be enough to avoid the problem. For example:

  1. If the current MSS of the session is 1460, New MSS = 1460 - 40 = 1420 (accounts for maximum TCP option bytes; recommended).
  2. If the current MSS of the session is 1460, New MSS = 1460 - 20 = 1440 (accounts for only the MD5 option).

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

  Conditions: The symptom is observed on a Cisco 7200 series router and Cisco 7301 router with an NPEG1 processor.

  Workaround: Change the MDL of operation to PULL using the command **dma enable pull model**.

- CSCsx34703

  Symptoms: In certain corner cases, received BFD packets can fill up the input queue on the incoming interface eventually blocking packet reception on that interface.

  Conditions: The symptom is observed when BFD is enabled and BFD adjacency is established after bootup.

  Workaround: There is no workaround.

- CSCsx36091

  Symptoms: The input-queue size keeps increasing on the router until it hits the default value, after which packets are dropped at the interface.

Conditions: Occurs with the following topology:

IP phones ---- remote-site ---- WAN ---- central-site --- HQ ---- CUCM --- IP phones

This is a single-NAT scenario, where the remote-site has all Application Level Gateway (ALG) enabled. Ten phones using Skinny Call Control Protocol (SCCP) on the remote site are trying to register to the Call Manager. Performing a **shut/no shut** on the WAN interface of the remote router triggers this scenario faster.

Workaround: There is no workaround. Rebooting the router clears the queue.

- CSCsx41496

  Symptoms: When the fastethernet interface is up, the **reload** command takes the card to an empty state. You need to enter **resetcd** from the PXM to bring the card to an active state.

  Conditions: The symptom is observed when the fastethernet interface is connected to a Cisco 3750 router, a 2950 switch and an RPMXF card. The fastethernet interface should be up.

  Workaround: Enter **resetcd** from the PXM.

- CSCsx42261

  Symptoms: Memory leak occurs with “CCSIP_SPI_CONTROL” process.

  Conditions: The error is found on a Cisco 3825 running the c3845-spservicesk9-mz.124-20.T1.bin image and using Skinny Call Control Protocol.

  Workaround: There is no workaround. Reload the router.

- CSCsx42732

  Symptoms: Cannot create an IPSLA probe. The system returns “no available memory” for probes.

  Conditions: The symptom occurs on a Standby RP2.

  Workaround: There is no workaround.

  Further Problem Description: Analysis determined this issue is a 32-bit IOS versus 64-bit LLP.

- CSCsx43644

  Symptoms: Policy-name remains unchanged after renaming.

  Conditions: The symptom is observed only with an ATM interface.

  Workaround: There is no workaround.

- CSCsx44172

  Symptoms: A privilege 15 user being authorized against a TACACS server can issue certain commands containing the arguments “full” or “brief” although these commands are disallowed in the TACACS server. For instance:

  - show running-config brief

  - show running-config full

  Conditions: When running TACACS debugs when the commands are executed, we can see that the privilege level is set to 0 for these commands, although the correct level should be 15. The router is configured with the following:

  - **aaa authorization config-commands**
  - **aaa authorization exec default group tacacs+ if-authenticated**
  - **aaa authorization commands 0 default none**
  - **aaa authorization commands 1 default group tacacs+ if-authenticated**

  - **aaa authorization commands 15 default group tacacs+ if-authenticated**

  Workaround: There is no workaround.

- CSCsx45429

  Symptoms: The GM crashes when trying to display VSA policy detail using the command **show pas vsa policy detail** and when traffic is being sent through the GM.

  Conditions: The symptom is observed when using the command **show pas vsa policy detail**. It may affect all recent software releases.

  Workaround: There is no workaround.

- CSCsx46383

  Symptoms: A Cisco Catalyst 6000 series switch does not respond with any data when using SNMP with VRFs configured and polling for the IP-FORWARD-MIB.

  Conditions: The symptom is observed on a Cisco Catalyst 6000 series switch that is running Cisco IOS Release 12.2(33)SXH.

  Workaround: There is no workaround.

- CSCsx47227

  Symptoms: Incoming traffic on a PBR-configured interface is process switched.

  Conditions: The symptom is observed when traffic ingressing on an interface configured for PBR when using an ipbase, ipvoice, or entbase Cisco IOS images.

  Workaround: Disable PBR on the incoming interface.

- 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.

- CSCsx49573

  Symptoms: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml

  Conditions: See “Additional Information” section in the posted response for further details.

  Workaround: See “Workaround” section in the posted response for further details.

- CSCsx51135

  Symptoms: In GETVPN scenarios on a VSA, both the SA and the corresponding ACE entry is kept until the SA expires, even though the ACE entry has been removed from the keyserver.

  Conditions: The symptom is observed when an ACE entry is removed from the keyserver ACL.

  Workaround: Use the command **clear crypto gdoi** on the group members.

- CSCsx51674

  Symptoms: Agent entry is not seen.

  Conditions: Occurs on a roaming interface that is configured for Collocated Care-of Address (CCoA). The mobile router will not see it as a usable interface.

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

- CSCsx53084

  Symptoms: Some of the OILs are not being fully populated for the groups.

  Conditions: The symptom is observed with an Auto RP configuration.

  Workaround: Use a static RP configuration instead of Auto RP.

- CSCsx54460

  Symptoms: RP unexpectedly restarts upon issuing the command **show crypto ipsec sa identity**.

  Conditions: The symptom is observed with a simple site-to-site configuration and with no traffic.

  Workaround: There is no workaround.

- CSCsx55741

  Symptoms: Transit IPsec traffic is dropped on GM GETVPN. The following message is shown:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=192.168.6.1, prot=50, spi=0xC39A071A(3281651482), srcaddr=192.168.6.2
  ```

  Conditions: The symptoms are observed under the following conditions:

  1. A Cisco 7200 series router in combination with VSA as HW-accelerator.
  2. GDOI policy defined to not perform double encryption.
  3. R1 connects to R2[GM], connects to R3[GM], connects to R4. (R2 and R3 are two group members of a GETVPN networks.) The GDOI policy is: Deny R1=>R4; Deny R4=>R1; Permit any any.

  Workaround: Permit double encryption with the following caveat: If transiting ESP packet are near the IPsec path MTU then, after encapsulation into GETVPN IPSEC, they will be fragmented. The receiving side of the transit IPsec flow (e.g. R1 or R4 in above scenario) will have to reassemble these packets which can lead to high CPU on the receiving end.

  This makes the workaround more or less applicable depending on the transiting traffic pattern.

- CSCsx55861

  Symptoms: On a Cisco 880 router, the UUT crashes when the PVC comes up and when “auto qos voip” is configured.

  Conditions: The symptom is observed when “auto qos voip” is configured under ATM and when the PVC is toggled (due to, for example, a shut/no shut of the ATM interface or a cable being pulled and then restored).

  Workaround: There is no workaround.

- CSCsx56047

  Symptoms: RTP call fails with SRTP configuration.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(23.15)T3.

  Workaround: There is no workaround.

- CSCsx56837

  Symptoms: Intermittent one-way audio occurs during a call.

  Conditions: Calls through a Cisco IOS transcoding device may experience one-way audio when certain signaling RTP payload types are received.

Cisco IOS VoIP gateways utilize named signaling events (NSE) to signal certain transitions to other states for active calls. Modem passthrough is a feature by which two gateways can upspeed to g711 an active RTP session. This is signaled through the use of certain NSE packets between these devices.

Modem passthrough using NSE through a transcoding session is not supported. However, under some situations on a voice call (no modems on the call), it is possible that the modem detection algorithm on the DSP may falsely detect a modem signal. If this occurs, a NSE will be sent out if modem passthrough is configured on the VoIP gateway. If the transcoder session that is bridging the two calls between the VoIP gateways receives this NSE packet, all further processing of RTP packets will stop in that direction.

Workaround: Disable modem passthrough on the end VoIP gateways.

- CSCsx57360

  Symptoms: A Cisco 870 router may fail to write a crashinfo file and will display the following error on the console:

  ```
  File flash:crashinfo_XXXXXXXX-XXXXXX open failed (-1): Not enough space
  ```

  Conditions: The symptom is observed with certain types of memory corruption.

  Workaround: There is no workaround.

- 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.)

- CSCsx58097

  Symptoms: Spurious access/tracebacks and occasionally a crash are seen on the console after an SSO switchover.

  Conditions: The symptom is observed when the router has huge configurations of L2VPN (VPLS) VCs.

  Workaround: There is no workaround.

- CSCsx58889

  Symptoms: Calls fail intermittently with cause “47: no resource available” error.

  Conditions: Occurs when router is under load test.

  Workaround: There is no workaround.

- CSCsx61138

  Symptoms: Bindings are not cleared after the **clear ip mobile binding** *ip address*.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(23.15).

  Workaround: There is no workaround.

- CSCsx63855

  Symptoms: CPU hogs are seen on a Cisco 2430 router when performing a shut/no shut on the ATM interface.

  Conditions: The symptom is observed when configuring 511 PVC subinterfaces on the ATM interface and after performing a shut/no shut on the ATM main interface. (CPU hog messages appear every 2000 msec until 50008 msec.)

  Workaround: There is no workaround.

- CSCsx63982

  Symptoms: A router configured for SNMP might unexpectedly crash with a bus error code.

  Conditions: This issue occurs when you query cSipCfgPeerTable of CISCO-SIP-UA-MIB. To be more specific, cSipCfgPeerPrivacy MIB object.

  Workaround: Do not poll cSipCfgPeerPrivacy MIB object.

- CSCsx65027

  Symptoms: If CEF is enabled, traffic fails to pass.

  Conditions: The symptom is observed on Cisco 2801 and Cisco 2811 routers and with the ipvoicek9-mz.124-23_15_PI10 image.

  Workaround: Disable CEF.

  Alternate Workaround: Perform a shut/no shut on the interface with incomplete adjacency (using the **show adjacency** command).

- CSCsx67084

  Symptoms: Police policy is not working at Multilink interface with MPLS EXP classification.

  Conditions: This symptom is seen with a Cisco 7200 series router after detach a 3 level policy. In a 3 level policy, police is configured at level 3. After detach 3 level policy, attach a single level policy with police class.

  Workaround: There is no workaround.

- CSCsx67255

  Symptoms: An outgoing call from an IP phone to PSTN through ISDN PRI fails on a channel due to a DSP allocation failure (not enough DSPs to support the call). Subsequent calls through that same channel continue to fail with “resource unavailable” cause value equal to 47 even after DSP resources have been made available to handle the call.

  Conditions: The symptom occurs on a router running Cisco IOS Release 12.4(15)T8 or higher. The call must first fail with a legitimate DSP allocation error. Any call made through the same channel as the failed call will also fail.

  DSP allocation failures on gateway can be checked through the use of the exec command **show voice dsp group all**. The last line of the show command output includes a counter for “DSP resource allocation failure”.

  This issue can be seen also in some cases upon bootup. When a gateway is reloaded, system resources will come up with slightly different timing. If, for example, a PRI interface comes up before the DSP resources have fully initialized, there may be a similar failure.

  Workaround:

  1. Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.

2. If this issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the CCO "DSP Calculator" at http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl.
3. If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.

- CSCsx67352

  Symptoms: The following error message is seen:

  ```
  %DSLSAR-3-FAILSETUPVC: Interface ATM0, Failed to setup vc 23 (Cause: VC setup failed)
  ```

  Conditions: The symptom is observed on a Cisco 1801 router when multiple PVCs are configured on the ATM interface. Typically, this issue is seen when multiple PVCs try to re-establish and if the line rate degrades.

  Workaround: There is no workaround.

- CSCsx67931

  Symptoms: The **no l2tp tunnel authentication** command does not work at LNS.

  Conditions: This symptom happens when the VPDN group that is used has a **virtual-template** *x*.

  Workaround: Configure the **no l2tp tunnel authentication** command under virtual template.

- CSCsx68596

  Symptoms: The system may display a %SYS-3-NOELEMENT message, similar to:

  ```
  %SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue -Process=
  "<interrupt level>", ipl= 6
  ```

  after which system behavior can be unpredictable. If the interrupts are rapid enough, the system may become unresponsive (hang), use all available memory to create more buffer elements, or crash due to CSCsj60426.

  Conditions: The message is caused by extremely rapid changes in flow control or modem control lead status on a console port.

  Workaround: Eliminate the source of the rapid lead changes. As modem control and flow control are generally not supported on the console, these changes are usually due to misconfigured devices attached to the console.

- CSCsx68730

  Symptoms: Pseudowire switching configured between ASBR routers does not work and tracebacks are seen.

  Conditions: Occurs when Cisco 7200 router is used as Autonomous System Border Router (ASBR) and pseudowire switching is configured.

  Workaround: There is no workaround.

- CSCsx68809

  Symptoms: When PowerPC processors are reloaded, they hang and are unable to boot. The session to PowerPCs will not work. The **show sami processors** command run on the LCP (processor 0) yields the status of the processor as "ROMMON INITIALIZING (0x00000800)" and they are unable to go beyond this state in the bootup process.

  Conditions: The symptom is observed when the PowerPC processors have been rebooted around 250 times, without reloading the complete SAMI card in the process. (Note: if all six are rebooted, then it can happen in 42 times, 42x6=252).

  Workaround: Reboot the SAMI card.

Further Problem Description: To confirm this issue, session to the LCP (processor 0) of the SAMI from the SUP and execute the **debug sami ppc_download errors** command. Reload any one processor (for example: **reload sami processor 3**).

Then you should see an error saying "Failed to open file". Execute the command **show sami processors**, which should show that the reloaded processor remains in the "ROMMON INITIALIZING (0x00000800)" state. If both of these conditions are satisfied then this confirms that this issue is causing the behavior.

- CSCsx70594

  Symptoms: A router configured for SSL-VPN and with TE tunnels may truncate packets when sending traffic from SSLVPN over the TE tunnel. This does not affect all packets, as some transmit correctly. When the issue is seen, 14 bytes are missing from the tail of the data packet.

  Conditions: The symptom is observed with SSL-VPN traffic that transmits over a TE tunnel.

  Workaround: Disable hardware encryption.

- 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.

- CSCsx73867

  Symptoms: A router that is running Cisco IOS Release 12.4(22)T and that is configured for L2L tunnels may intercept pass-through UDP 4500 packets destined to an internal client. Logged on the fault router is:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=x.x.x.x, prot=50, spi=0xDD8DEB2(232316594), srcaddr=y.y.y.y.
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4(22)T configured for IPSec. Internal IPsec client is natted on the router using NAT-T.

  Workaround: There is no workaround.

- CSCsx74151

  Symptoms: Large packets may be dropped if prefragmentation is enabled with VSA.

  Conditions: The symptom is observed when GETVPN creates some tunnels with time-based anti-replay and others with counter-based anti-replay/no anti-replay.

  Workaround: Use the same replay method for all the SAs in the router.

- CSCsx75004

  Symptoms: In a Carriers Carrier, the CSC-PE router advertises wrong out-label. This causes the end-to-end LSP to be broken in the CSC network, and all traffic is dropped.

  This problem is observed by enabling the **show ip bgp label** command on CSC-CE. See "Out Label" of the route is "imp-null".

  Conditions: This condition is observed in routers that are running Cisco IOS Release 12.0(32)SY6.

  Workaround: Configure **neighbor** {*ip-address* | *peer- group-name*} **next-hop-self** on CSC-PE.

- CSCsx75230

  Symptoms: Traceback is seen with MobileIP configuration.

  Conditions: The symptom is observed with a Cisco 7200 series router.

Workaround: There is no workaround.

- CSCsx75353

  Symptoms: High CPU usage is observed on a Cisco 2821 router. An increase of almost 10 percent in CPU utilization is observed with every voice call.

  Conditions: This symptom is observed when an AIM compression card is present on the motherboard (specifically AIM-COMPR2-V2).

  Workaround: Remove the AIM compression card from the motherboard.

- 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.

- CSCsx80605

  Symptoms: Zone Based Firewall starts dropping all the packets.

  Conditions: The symptom is observed when you configure and unconfigure the zone-pairs in a particular sequence.

  Workaround: Delete the zone-pairs completely then attach the zone-pairs again.

- CSCsx80629

  Symptoms: Router with QoS configuration crashes after removing bandwidth from the policy-map.

  Conditions: The symptom is observed when the policy-map is attached to the router interface.

  Workaround: Remove the policy-map from the interface and then remove bandwidth from the policy-map.

- CSCsx82690

  Symptoms: A voice gateway placing ISDN calls will exhibit a memory leak. The effects of this memory leak can be seen with the **show process memory** command. It shows that the amount of memory the ISDN process is holding continues to increase without being released.

  Conditions: The symptom is observed on a voice gateway that is processing ISDN calls on a PRI interface. Switchtype is set to be primary-QSIG and the calls that leak memory are QSIG-GF (connection-oriented calls) and not regular voice calls. Such calls are typically used when implementing supplementary services such as MWI.

  Workaround: There is no workaround.

- CSCsx83443

  Symptoms: ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vty’s even though **debug crypto condition peer ipv4 x.x.x.x** is set.

  Conditions: Use peer IP-based debug condition.

  Workaround: There is no workaround.

- CSCsx94324

  Symptoms: Packets with certain packet sizes get dropped when being CEF-switched on a router.

  Conditions: The symptom is observed when CEF is enabled and when the outbound interface is an HWIC-4SHDSL DSL interface. It is observed when the packet undergoes fragmentation.

  Workaround: Disabling CEF is a workaround.

- CSCsx94349

  Symptoms: Router software force crash.

  Conditions: The symptom is observed when “IPv6 firewall” is configured and the maximum TCP half-open threshold is exceeded.

  Workaround: Increase the maximum TCP incomplete session threshold with the following command **ipv6 inspect tcp max-incomplete host**.

- CSCsx95906

  Symptoms: Call fails when Nortel endpoint is at remote end.

  Conditions: Nortel endpoint sends a long contact header field value, which exceeds the maximum limit of the Cisco device. This remote contact overwrites memory for the from header and results in a dialog mismatch from the new message generated by the gateway.

  Workaround: There is no workaround.

- CSCsx96381

  Symptoms: A video conference device makes a video call to a TDM Conference Station through an H320 gateway. When the call is placed, only the primary channel goes up and the H320 gateway does not proceed with secondary channels.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsx98284

  Symptoms: A router may crash with a bus error and with a corrupted program counter:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0x66988B14 , ra=0x66988AFC ,
  sp=0x66A594D0
  ```

  Conditions: The symptom is observed on a Cisco IOS Voice over IP (VOIP) gateway configured for IPIPGW (CUBE) as well as Cisco Unified Communications Manager (CUCM) controlled MTP on the same gateway. Under situations where a call loop is present (same call routing back-forth through the same gateway), the system may reload if an MTP is also present in the loop.

  Workaround: Find and break the source of the call loop. Be careful of default destination-pattern/route-patterns that may kick in under some conditions.

  Alternate workaround: Separate the MTP functionality from the gateway.

- CSCsx99097

  Symptoms: The router crashes.

  Conditions: The symptoms is observed when the command **no iphc-profile** is done in global configuration mode and when the same map-class is configured on a frame relay interface.

  Workaround: Remove “iphc profile” from the map-class before deleting in global mode.

- CSCsy01360

  Symptoms: Router crashes when configuring GETVPN.

  Conditions: The symptom occurs when configuring GETVPN on a frame-relay serial interface with EIGRP, OSPF, LLQ and PIM Sparse mode.

  Workaround: There is no workaround.

- CSCsy01760

  Symptoms: There is a system crash.

  Conditions: The symptom is observed when the interface for COOP and GM is shut down.

Workaround: There is no workaround.

- 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.

- CSCsy03568

  Symptoms: Spoke-to-spoke TCP applications fail over a GRE/IPSec tunnel on a hub and spoke scenario, when traffic flows through the hub.

  Conditions: The symptom is observed with the following conditions:

  – GRE/IPSec configured with crypto maps.

  – Hub has “ip tcp adjust-mss” configured under the tunnel interface that is facing the spoke from where traffic is coming.

  Workaround: Use tunnel protection instead of crypto maps.

  Alternate workaround: Disable CEF globally on hub (this may impact performance, so should be used with care).

- CSCsy05111

  Symptoms: A router crashes after enabling and disabling NBAR on an interface if a class-map with match protocol is configured first (“match protocol rtp audio”).

  Conditions: The symptom is observed if the “match protocol rtp audio” statement is found in the class-map configuration. RTP uses a label heuristic which quickly reproduces the bug.

  Workaround: Do a config/no-config on one interface while keeping NBAR configured on any other interface.

- CSCsy05298

  Symptoms: The IOSD-crash is seen and is affecting the main functionality.

  Conditions: This symptom is observed when a large number of groups (i.e. 50) is configured. The IOSD-crash is seen when we give the **show crypto gdoi** command after applying the general configuration and after checking the ping between all the PIM neighbors.

  Workaround: Use the **show crypto gdoi group** *group- name* to display a specific group’s information.

- CSCsy06128

  Symptoms: When a router is about to renew a certificate, the following syslog message is seen

  ```
  "%PKI-6-CERTRENEWAUTO: Renewing the router certificate for trustpoint xxx".
  ```

  However, no certificate is received until a few hours later.

  Conditions: The issue only happens on a Cisco 871 running Cisco IOS Release 12.4(15)T8 and 12.4(22)T1 or earlier releases. This issue is only seen with a very short certificate lifetime, such as 1 hour.

  Workaround: Increase the certificate lifetime to a few days or more.

- CSCsy06404

  Symptoms: When testing the inbound route-map for external peer-group members by using a community-list, routes which are set with the community as “no-advertise” in the eBGP peer are being shown in the BGP table of the iBGP neighbor of UUT.

  Conditions: The symptom is observed on a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCsy07369

  Symptoms: An invalid range of IP addresses are accepted at CLI.

  Conditions: The symptom is observed when the following command format is used: **range** *ipaddress1 ipaddress2* where the range of the IP addresses is not seen in same network.

  Workaround: Avoid entering wrong ipaddress2.

- CSCsy07953

  Symptoms: Any attempt to copy a file from a router to an FTP server will fail. The FTP error is “No such file or directory”.

  Conditions: This is only a problem with FTP and only when transferring to an FTP server. Transfers from an FTP server work as expected.

  Workaround: Use a different file transfer protocol, such as TFTP.

- CSCsy09101

  Symptoms: Cisco Configuration Professional (CCP) is unable to load signatures from the router. IOS-IPS signatures cannot be viewed or modified using CCP.

  Conditions: The symptom occurs when using CCP to manage IPS5.0 in routers that are running Cisco IOS Release 12.4(20)T2, 12.4(24)T and 12.4(22)T1.

  Workaround: There is no workaround from CCP. Use CLI to view or modify IPS signatures.

- CSCsy09250

  Skinny Client Control Protocol (SCCP) crafted messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sccp.

- CSCsy10653

  Symptoms: Calls on an MGCP gateway negotiating the g729br8 codec may fail to have audio in one or both directions.

  Conditions: This occurs on MGCP gateways with the fix for CSCsu66759 when the g729br8 codec is being negotiated.

  Workaround: Any of the following will be sufficient to get around this issue:

  1. Configure the gateway for static payload type using the following commands on the gateway:

     mgcp behavior g729-variants static-pt

     mgcp behavior dynamically-change-codec-pt disable

  2. Disable g729br8 from being negotiated for this call. If CUCM is involved, this is done with the service parameter "Strip G.729 Annex B (Silence Suppression) from Capabilities".

3. Use a Cisco IOS code on the gateway which does not contain the fix for CSCsu66759 (Cisco IOS Release 12.4(22)T and below).

- 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.

- CSCsy13587

  Symptoms: A Cisco 2430 router shows continuous tracebacks when configuring MTU.

  Conditions: The symptoms are observed when a Cisco 2430 router is configured with 511 PVCs under an ATM interface and MTU is configured to the maximum configurable value.

  Workaround: There is no workaround.

- CSCsy14244

  Symptoms: Video call between two Cisco Unified Video Advantage endpoints results in one-way audio and no video.

  Conditions: Occurs when call passes through Cisco Unified Border Element (CUBE).

  Workaround: There is no workaround.

- CSCsy15098

  Symptoms: Cisco 3845 reloads at cm_destroy_connection while changing mode ATM AIM 0 to CAS.

  Conditions: Occurs while switching a Cisco 3845 with an existing connection.

  Workaround: There is no workaround.

- CSCsy15468

  Symptoms: Crash keyserver reloads.

  Conditions: The symptom is observed if test case 1 in TBAR sanity regression on the VSA is configured and then unconfigured. When configuring the second one, the keyserver crashes.

  Workaround: There is no workaround.

- CSCsy16078

  Symptoms: A GETVPN group member might reload when removing “crypto map” from the interface, if that crypto map also contains a dynamic-map set together with the GDOI set.

  Conditions: The symptom only occurs when a dynamic-map set is added to a crypto map that is already applied to an interface and then the whole crypto map is removed, added and removed again. It is on the second removal that the reload occurs.

  Workaround: Execute the command **clear crypto gdoi** before removing the crypto map from the interface.

- 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.

- CSCsy16177

  Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.

  Conditions: Occurs on a Cisco 2811 with flash type file system.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsy19659

  Symptoms: When using Point-to-Point Tunnelling Protocol (PPTP) with RADIUS Accounting, there may be several “nas-error” and “lost-carrier” listed in accounting as the Acct-Terminate-Cause.

  Conditions: The symptom is observed when using Cisco IOS Release 12.4T (Releases 12.4(15)T-12.4(22)T confirmed) and using PPTP with RADIUS Accounting in place.

  Workaround: There is no workaround.

- 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.

- CSCsy20488

  Symptoms: IPSsec/GRE traffic does not go over an ATM interface.

  Conditions: The symptoms are observed when using a VSA encryption card and when the ATM interface is using PVC bundles.

  Workaround: Do not use PVC bundles.

  Alternate workaround: Disable the VSA encryption and use software encryption (not recommended for a high load of encryption).

- 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.

- CSCsy22311

  Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.

  Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.

  Workaround: There is no workaround.

- CSCsy22825

  Symptoms: Chunk leak is seen whenever one PPPoE session is cleared.

  Conditions: Occurs only when one session is cleared.

  Workaround: There is no workaround.

- CSCsy22826

  Symptoms: The VG224 endpoint does not connect to the callback destination, once the callback destination is idle.

  Conditions: The symptom is observed with a multi-node cluster and when a VG224 endpoint is registered with a node other than the first node in the cluster.

  Workaround: Have VG224 endpoints registered with the first node.

  Further Problem Description: The activation of the callback is successful. The failure is when the callback destination becomes idle again and the VG224 endpoint gets notified (ring). After the VG224 endpoint goes offhook, the system should automatically connect to the callback destination. This does not happen and VG224 endpoint gets silence.

- CSCsy22920

  Symptoms: A router crashes at mripv6_mode_entry when the authentication key is configured to be equal to 64 bytes.

  Conditions: The symptom is observed on a router that is running the c7200-adventerprisek9-mz.124-24.6.T image.

  Workaround: Configure an authentication key of less than 64 bytes.

- CSCsy24266

  Symptoms: A call from a night hunt forwarded to BACD dial by an extension to an ephone (call forwarding no answer) to voicemail goes to the night hunt number and not the last redirected number.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsy24676

  Symptoms: On occasion, a false positive is returned on a file system failure. File operation is deemed successful when, in fact, it has failed.

  Conditions: This problem occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converted to a success code. This problem is likely to show up if there is a device error during the write. The device error may be due to bad media or an OIR (although it is very unlikely during an OIR).

  Workaround: There is no workaround.

Further Problem Description: This is possible during any file system operation where a file system device is unable to complete the operation and an error is returned. This error is not passed down to the file system stack but is converted to a success code. Other clients which are dependent on previous file system operations fail on successive file system calls and possibly result in a crash.

- CSCsy26448

  Symptoms: Router configured with DNS crashes when deleting a trust-point.

  Conditions: The symptom is observed on a Cisco 7200 series and Cisco 3845 router that is running Cisco IOS Release 12.4(24.6)T.

  Workaround: There is no workaround.

- CSCsy26526

  Symptoms: Router may reload under excessive **netconf** configuration.

  Conditions: The following configuration commands, when configured repeatedly within a short period of time may cause the device to reload.

  - **netconf ssh**
  - **netconf beep listener**

  Workaround: There is no workaround.

- CSCsy27394

  Symptoms: Users who can execute a **show ip interface** command can see that an LI tap is in progress.

  Conditions: No specific conditions are necessary to trigger this problem.

  Workaround: There is no workaround.

- CSCsy28758

  Symptoms: HLog softkey stops working.

  Conditions: The symptom is observed under the following conditions:

  1. When logging into an EM profile where the user was logged out from the hunt group.
  2. This is to be done on a phone where an EM profile was previously logged in, which was also logged into the huntgroup.

  Workaround: Log in with the EM profile on the phone that was used to log out the huntgroup.

- CSCsy29533

  Symptoms: A T38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP controlled T38 fax relay call and when the gateway is configured for CA control T38. The output of the command **debug voip vtsp all** will give fax relay as “DISABLED”.

  Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCsy29828

  Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

  Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

  Workaround: Enter the following commands:

  - **no ip nat service sip tcp port 5060**
  - **no ip nat service sip udp port 5060**

  Or

  - **ip nat translation timeout never**

- CSCsy29940

  Symptoms: Unable to configure inspect for any protocol in self zone.

  Conditions: Occurs when configuring class-map with match protocol and trying to attach to self-zone pair.

  Workaround: The issue is not seen when **match access-group** is used.

- CSCsy31365

  Symptoms: Memory leak of 24-bytes can occur when a transcoding call is disconnected.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24.6)T and is seen while shutting down the DSPfarm profile when the transcoding call is active in IPIPGW.

  Workaround: There is no workaround.

- CSCsy31552

  Symptoms: A Cisco 1841 router equipped with xDSL WIC will suddenly stop forwarding packets. The packets will appear as output drops on the ATM interface statistics. Under the PVC level, there are no drops. The DSL line is not flapping but the ATM interface(s) report output drops.

  Conditions: The symptom is observed when using a Cisco 1800 and 2800 series router equipped with the same ADSL-WIC module. The ATM interface(s) need to be bridge-group configured. The bridge-group is in forwarding mode.

  Workaround: Reload the router.

- CSCsy32000

  Symptoms: Router crashes when BGP-IPv6 directly connected IBGP neighbors receives route with Link-local Nexthop.

  Conditions: BGP sends IPv6 link-local address in following cases:

  1. Directly connected eBGP neighbors
  2. BGP Ipv6 neighbors connected using Link-local address

  In case of this defect, testing device is advertising link-local nexthop for directly connected neighbor using global IPv6 address. Cisco router will never advertise link-Local nexthop.

  Workaround: There is no workaround.

- 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).

- CSCsy33068

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

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

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

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

- CSCsy34231

  Symptoms: A Cisco 3845 router may reload while try to unconfigure “crypto map” from the VRF interface or configure the IP address for the VRF interface after an associate/disassociate.

  Conditions: The symptom is observed with an EzVPN configured VRF network and when running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsy37573

  Symptoms: The IOS Transcoder responds with two ORC Ack for one ORC, in a special testing scenario.

  Conditions: The symptom is observed when CUCM mistakenly requests a regular Cisco IOS transcoder for transcoding non-G.711 to non-G.711.

  Workaround: There is no workaround.

- CSCsy38625

  Symptoms: A Cisco router may unexpectedly reload during normal operation.

  Conditions: This issue is specific to the usage of DLSw+ on a Cisco router, together with the command **dlsw circuit-keepalive**.

  Workaround: Remove the **dlsw circuit-keepalive** command from the router.

  Further Problem Description: When adding or removing the **dlsw circuit-keepalive** command you must restart all DLSw circuits for the command to take immediate effect.

  This command is used under normal conditions when a Cisco router has DLSw peers to one or more non-Cisco routers. If there are only Cisco routers having DLSw peers to each other than the routers by default will send periodic DLSw peer keepalive messages to test the integrity of the DLSw peer. The **dlsw circuit-keepalive** command should only be used when Cisco routers have established DLSw peers to non-Cisco routers.

- CSCsy39667

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

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

Workaround:

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

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

- CSCsy40285

  Symptoms: Cisco 3845 crashes during end point registration.

  Conditions: Occurs on a router running the c3845-adventerprisek9-mz.124-24.T.bin image.

  Workaround: Increase **tcp idle-timeout** to 7200 seconds.

- CSCsy40745

  Symptoms: After disabling SSH, an alternate SSH port is still enabled on the router.

  Conditions: Occurs on routers that have been configured to use a port other than Port 22 for SSH.

  Workaround: Do not configure alternate SSH ports.

- CSCsy41573

  Symptoms: If a serial interface is configured for MFR, traffic stops flowing through the MFR interface if you flap the serial interface.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24.6)T.

  Workaround: There is no workaround.

- CSCsy41648

  Symptoms: The following issues with the End User License Agreement (“EULA”) display can be seen:

  1. Gatekeeper EULA cannot be displayed on another unit from which a telnet session is initiated through an Ethernet connection.
  2. Ctrl-C cannot abort the EULA acceptance confirmation.
  3. After the EULA is rejected, the warning message cannot be displayed after another configuration CLI is issued.

  Conditions: The symptoms are observed with the EULA display.

  Workaround:

  1. For issue 1, Telnet into console instead of through an Ethernet connection.
  2. For issue 2, type “no” to deny EULA acceptance explicitly.
  3. For issue 3, exit from gatekeeper mode to see the warning.

- CSCsy42401

  Symptoms: User group class matching fails when NAT is turned on.

  Conditions: The symptom is observed with IOS FW user group inter-operated with NAT.

  Workaround: There is no workaround.

- 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.

- CSCsy45371

  Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Stop the network traffic while configuring NAT.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** may cause a router to crash.

  Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

  Workaround: There is no workaround.

- CSCsy48838

  Symptoms: A router may crash with the following (or similar) message:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  ```

  Conditions: The symptom is observed when IOS firewall/ip inspect on H323 traffic is configured (“ip inspect name MY_INSPECT h323”).

  Workaround: Do not inspect H323.

- CSCsy49796

  Symptoms: HTTP redirect intermittently uses IP address instead of FQDN, even though an FQDN is configured in the WebVPN gateway.

  Conditions: The symptom is observed when the WebVPN gateway generates an HTTP redirect with an IP address when the HTTP Request from the client is not complete or split over multiple TCP packets.

  Workaround: There is no workaround.

- CSCsy50066

  Symptoms: Router reloads while deleting the certificate revocation list.

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4(24.6)T2. The router reloads while deleting the certificate revocation list after getting the certificates from the CA server.

  Workaround: There is no workaround.

- 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.

- CSCsy54095

  Symptoms: The append operation does not list the USB flash device file system for both unpartitioned and partitioned USB flash devices. The following error message is shown:

  ```
  % Appending is not supported in this file system
  ```
  Conditions: The symptom is observed with Cisco IOS Release 12.4T.

  Workaround: Append to other available filesystems.

- CSCsy54137

  Symptoms: Some calls are shown as active after a WAN link outage between the gateway and Call Manager.

  Conditions: The symptom is observed if a WAN outage happens when more than 40 calls are in progress. Some random calls are then shown to be as active when using the command **show call active voice compact** with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCsy54233

  Symptoms: exception_reserve_memory is invalid in UNIX image.

  Conditions: UNIX images do not support exception_reserve_memory.

  Workaround: There is no workaround.

- CSCsy54361

  Symptoms: Device hangs. There is no output on the console port.

  Conditions: The symptom is observed on a Cisco 7301 router that is running Cisco IOS Release 12.4(24)T. NAT NVI translation is configured between a VRF and the native routing instance, for example:

  ```
  ip nat pool nvi-pool15 x.x.x.x y.y.y.y netmask z.z.z.z add-route ip nat source list
  nvi pool nvi-pool15 vrf vpnxxx overload ip route vrf vpn104 x.x.x.x y.y.y.y
  GigabitEthernetx z.z.z.z global name nvi
  ```
  (Note: the issue is only occurring when overload is not configured.) The trigger is the packet is arriving to the device and matching the IP routes.

  Workaround: There is no workaround.

- CSCsy55821

  Symptoms: With a VTI tunnel between a Cisco ASR 1000 and another device (non-ASR), the VPN peer of a Cisco ASR 1000 is reporting packets with an invalid SPI.

  Conditions: The symptom is observed in the following scenario:

  - LAN-to-LAN VPN with VTIs.
  - One VPN end point is a Cisco ASR 1002 (RP1) that is running Cisco IOS Release 12.2(33)XNC.
  - The other VPN end point is a Cisco 7206VXR (NPE-G1) that is running Cisco IOS Release 12.4(15)T1 initially, then is upgraded to Cisco IOS Release 12.4(22)T and NPE-G2 plus VSA.

  Workaround: There is no workaround.

  Further Problem Description: At rekey, the Cisco ASR 1000 is sending delete-notify to the Cisco 7200 series router but still keeps using the old SA to encrypt, causing the drops.

- CSCsy56016

  Symptoms: BERT errors and jitter buffer errors reported on AS5xxx when using the **show tech** command.

  Conditions: The symptom is observed on the gateway when the commands **show tech** or **show as5400** are executed.

  Workaround: There is no workaround.

- CSCsy57750

  Symptoms: IPIPGW reloads while making an RSVP-enabled voice call with media statistics configuration.

  Conditions: The symptom is observed with Cisco IOS 12.4(24.6)T2 image.

  Workaround: There is no workaround.

- CSCsy58450

  Symptoms: Zone based firewall drops packets that pass through a VPN tunnel (both forward and reverse traffic). The drops are usually seen for UDP traffic. The following traceback may be seen:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  ```

  Conditions: Occurs when firewall is configured with crypto-map tunnels. Cisco IOS Release 12.4(20)T2 and 12.4(22)T and earlier releases are not affected.

  Workaround: Change the UDP timeout to a reasonably larger value. The default value is 30 seconds, and changing it to something like 300 seconds has been found to make a difference. To do this

  1. Create an "inspect" parameter map with any name if it does not exist, then add the new UDP idle timeout.

  ```
  parameter-map type inspect <param-map-name> udp idle-time 300
  ```

  2. Attach the parameter map to all the inspect actions. **policy-map type inspect** *policy-name* **class type inspect** *class-name* **inspect** *param-map-name* **nbold**

- CSCsy58984

  Symptoms: A device that is running Cisco IOS Release 12.4(24)T reloads when editing ACL with an object group.

  Conditions: The symptom is observed on a Cisco 3845 and 2800 series router that is running Cisco IOS Release 12.4(24)T and 12.4(24.6)T2.

  Workaround: Avoid using "range" in any of the object groups (either direct or nested) and containing a group of objects which use a range of IP addresses.

- CSCsy60668

  Symptoms: On a router in which MPLS Traffic Engineering (TE) is configured, toggling the router-id in the router configuration can cause the router to reload. For example, configuring "router ospf 100 mpls traffic-eng router-id loopback 0" quickly followed by "mpls traffic-eng router-id loopback 1" may trigger this symptom.

  Conditions: It is necessary that "mpls traffic-eng tunnel automesh" is running in the OSPF area of the router, although automesh need not be configured on the affected router.

  Workaround: There is no workaround.

- CSCsy60782

  Symptoms: The **connect** command is not working if "bridging" is configured on the subinterface.

  Conditions: The symptom is observed on a Cisco 7200 series router configured to join two subinterfaces using the **connect** command, with bridging enabled.

Workaround: There is no workaround.

- CSCsy61209

  Symptoms: An IP-to-IP gateway (IPIPGW), also called CUBE, is adding an incorrect token in the H225 connect message.

  Conditions: The symptom is observed on an IPIPGW running Cisco IOS Release 12.4(20)T1, with talking H323 signaling protocol on both sides with security enabled.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsy69542

  Symptoms: Unable to configure a security association for any host using the **ip mobile secure host** command after creating a newly-named extended ACL or modifying an existing-named ACL on Cisco Home Agent.

  Conditions: The symptom is observed on Cisco Home Agent running Cisco IOS Release 12.4(22)YD.

  Workaround: There is no workaround.

- CSCsy69681

  Symptoms: Policy-based routing (PBR) fails to resolve next-hop.

  Conditions: Occurs when PBR is configured on a Cisco 871 to forward traffic to a DHCP-enabled interface.

  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.

- CSCsy70619

  Symptoms: A router may crash when multipath is enabled and when the MR is registered with two or more of its roaming interfaces.

  Conditions: The symptom is observed when using the **no ip mobile router-service roam** command on any one of the MR's roaming interfaces.

  Workaround: There is no workaround.

- CSCsy71006

  Symptoms: When the configured TEK lifetime is greater than 65000, the remaining TEK lifetime on the secondary KS shows zero.

  Conditions: The symptom is observed with a GDOI keyserver and where the TEK lifetime is configured to be greater than 65000.

  Workaround: Use a TEK lifetime of less than 65000.

- CSCsy71258

  Symptoms: Unable to boot a Cisco 850 series router using Cisco IOS Release 12.4(15)T9.

  Conditions: The symptom is observed on a Cisco 850 series router with 64MB of dram. The image requires more dram to boot.

  Workaround: There is no workaround.

- CSCsy73123

  Symptoms: Connected route on port-channel subinterface is not removed when port-channel is down.

  Conditions: Happens when using /22 subnet. Does not happen when using /24 subnet.

  Workaround: There is no workaround.

- CSCsy73838

  Symptoms: Connection for TR-069 is lost to the device after the device reloads.

  Conditions: The symptom is observed under the following conditions:

  1. Enable CWMP in the router. Inform is sent to ACS.
  2. Router is reloaded with CWMP-enabled in the startup configuration.
  3. When the router is reloaded, it sends the Inform request to ACS. In this Inform request, a ConnectionRequestURL value is formed without the ProductClass value.
  4. ACS can not initiate a connection to the router with the ConnectionRequestURL sent in the Inform request.

  Workaround: There is no workaround.

- CSCsy73981

  Symptoms: Cisco AS5400 shows memory leak for DSMP, VTSP, and MGCP processes. Occurs about once a month.

Conditions: After some time, the memory leak symptoms are seen on the gateway, although normal operations are not affected. Eventually all memory is consumed, and the gateway hangs. Only a manual reboot can bring it back to service.

Workaround: There is no workaround.

- CSCsy74329

  Symptoms: The following message appears on the console:

  ```
  [crypto_bitvect_alloc]: bitvect full (size = 8192) -Traceback= 0x4244AB0 0x426875C
  0x426AE60 0x426B330 0x426FAF4 0x4292B7C 0x4293278 0x75429C
  ```

  Conditions: The symptom is observed when the GetVPN rekey is used with a number of Deny ACL entries and with VSA.

  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.

- CSCsy76185

  Symptoms: The following traceback may be seen:

  ```
  Local7.Critical 192.168.133.252 827681: %SYS-2-NOBLOCK: printf with blocking disabled.
  Local7.Critical 192.168.133.252 827682: -Process= "IP Input", ipl= 0, pid= 61
  Local7.Critical 192.168.133.252 827683: -Traceback= 0x11EF3E4 0x1203120 0x180214C
  0x1209F54 0x120A0B8 0x179EF5C 0x19A1F94 0x19A270C 0x19A2930 0x19A2B0C 0x196B6FC
  0x196EC44 0x197115C 0x1972F8C 0x17AC2F4 0x17AC87C
  ```

Conditions: The symptom is observed during basic function.

Workaround: There is no workaround.

- CSCsy77191

  Symptoms: Native GigE interfaces of a Cisco 7200 NPE-G2 router will not acknowledge reception of pause frames and will not stop its transmission in case of media-type RJ45.

  Conditions: The symptom is observed with media-type RJ45 and with SFP with “no neg auto” configured.

  Workaround: There is no workaround.

  Further Problem Description: There are no issues with SFP with a “neg auto” configuration.

- CSCsy77298

  Symptoms: Option 82 is not appended in DHCP NAK packet by DHCP server.

  Conditions: Not any specific condition.

  Workaround: There is no workaround.

- CSCsy78776

  Symptoms: PPPOE session may not come up with CHAP/PAP authentication when call direction call-in is used.

  Conditions: The symptom is observed when the command **ppp authentication chap callin** is used, call direction is not set properly, and both side try to authenticate.

  Workaround: Use the local authentication method list on the client to allow this to operate correctly.

  Further Problem Description: When **ppp authentication chap callin** is used, then call direction is not set properly. The client sends a chap request even though call_direction call-in is set on client side. It works on the server side as call direction is set properly there.

- CSCsy79176

  Symptoms: Need to disable CEF to pass IP traffic. With CEF enabled, traffic fails to pass.

  Conditions: The symptom is observed on a Cisco 2801 and 2811 router that is running the ipvoicek9-mz.124-23_15_PI10 image.

  Workaround: Disable CEF or **shut/no** shut the interface with incomplete adjacency (using the **show adjacency** command).

- CSCsy79955

  Symptoms: Reverse SSH using PVDM2 modems fails. If the **ssh -l <username>:<line #> <ip>** command is entered, modem activation is triggered. The input of “atdt<number>” is making it to the modem, meaning whatever the <number> field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, “at”, “at&f”, “ate1” (and perhaps others) do not appear to be taken.

  Conditions: Seen on routers running Cisco IOS Release 12.4(22)T and 12.4(23). Appears to be issue with all releases. Issue is seen when using both **ssh -l <username>:<line #> <ip>** and by using SSH from a client to a particular line.

  Workaround: There is no workaround.

- CSCsy81339

  Symptoms: A Cisco Router may unexpected reload due to a Bus error exception.

  Conditions: The reload happens when a qos configuration change is made while a packet is in the middle of being processed on the interface the qos is applied.

Workaround:

1. Shutdown the interface before making any qos config changes
2. Remove the service policy from the interface while making the configuration change.

- CSCsy81585

  Symptoms: Spurious memory access.

  Conditions: The symptom is observed while removing the license feature.

  Workaround: Configure “telephony-service”.

- CSCsy84229

  Symptoms: When an HTTP request with payload of greater than 10MB is sent to the HTTP server of the router, the server is not able to process the request and responds back with the message “request entity too large”.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(22)T and 12.4(24)T and when the payload is above 10MB

  Workaround: Updating the signatures from S385 is a potential workaround.

  Further Problem Description: This behavior is only evident while applying S386 and above on devices that do not have any previous signature package. This error does not appear while updating signature from S385 to S386.

- CSCsy84286

  Symptoms: Router crashes while removing “ip dhcp class”.

  Conditions: The symptom occurs with relay agent information and relay-information hex configured.

  Workaround: There is no workaround.

- CSCsy84474

  Symptoms: In an H323 IP-to-IP Gateway (IPIPGW), during call setup when the OLC-ACK is received after the connect message, the call is not completed and the return OLC-ACK is not forwarded by the IPIPGW. The issue is sporadic and does not occur all the time.

  Conditions: This has been observed on a IPIPGW running Cisco IOS Release 12.4(20)T1-ES, having an H323 on both sides of the gateway. This only happens when the connect message is received before OLC-ACK exchange between the parties is complete.

  Workaround: There is no workaround.

- CSCsy86078

  Symptoms: Router crashes with memory corruption.

  Conditions: Occurs when BFD is configured on 10GigE interfaces and constant link flaps.

  Workaround: There is no workaround.

- CSCsy86097

  Symptoms: IP local pool addresses do not appear to be released on the Standby even though the Active RP has released them. Eventually, the number of free addresses on the Standby gets down to zero.

  Conditions: The symptom is observed in a scaled scenario (>4000 sessions roughly) on a HA-enabled system with “ip local pool” configured as frequent connections and disconnections of sessions take place.

  Workaround: Reload the Standby card periodically.

- CSCsy87674

  Symptoms: Calls via an MGCP gateway that is registered to a Cisco Unified Communications Manager (CUCM) fail immediately with a codec negotiation error.

  Conditions: This symptom is observed when a CUCM is configured to use the G729 codec for the MGCP gateway.

  Workaround: Use the G729 AnnexB codec between the MGCP gateway and the CUCM.

- CSCsy88640

  Symptoms: A core dump may fail to write, with the following errors seen on the console:

```
current memory block, bp = 0x4B5400A0,
memorypool type is Exception
data check, ptr = 0x4B5400D0
bp->next(0x00000000) not in any mempool
bp_prev(0x00000000) not in any mempool
writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z
[Failed]
writing compressed ftp://10.0.0.1/testiomem.Z
[Failed]
writing compressed ftp://10.0.0.1/test.Z
[Failed]
%No memory available
```

  Conditions: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.

  Workaround: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.

- CSCsy89234

  Symptoms: Stateful Fail-over of Network Address Translation (SNAT) in primary/backup mode does not converge.

  Conditions: Occurs after a **no shut interface** following a router reload, and then configure SNAT on the primary router.

  Workaround: Perform a **shut/no shut** of the SNAT interface on the primary router.

- 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.

- CSCsy91748

  Symptoms: An NM-CEM-4SER module crashes.

  Conditions: The symptom is observed with an NM-CEM-4SER module when its payload size is changed on a CEM port which is part of a multiplexed group that is created using the **attach <port>** command.

Workaround: Reload the router after using the **write config** command.

- CSCsy93054

  Symptoms: WebVPN portal is not displayed. The router closes the SSL negotiation as soon as it sends an SSL “Server Hello” message by sending a TCP FIN.

  Conditions: The symptom is observed when a trustpoint uses a certificate chain of larger than 4096 bytes.

  Workaround:

  1. Use a smaller certificate chain.
  2. Use self-signed certificates.

- CSCsy94618

  Symptoms: Occasionally, WSMA sessions reject a valid user in the Web Services Security Header (WSSE).

  Conditions: The symptom is observed with WSMA agents using the “wsse” configuration option.

  Workaround: Reconfigure the encapsulations.

- CSCsy95484

  Symptoms: Ping fails from gen to ref.

  Conditions: The symptom is observed when the router is loaded with Cisco IOS Release 12.4(24.6)T5.

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

- CSCsy97506

  Symptoms:

  Case 1: All NAT multicast data packets are processed by software.

  Case 2. Spurious memory access occurs.

  Conditions:

  Case 1. NAT with static port entry, or dynamic overload configuration.

  Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

  Workaround:

  Case 1: Configure NAT as static entry without port, or dynamic non-overload.

  Case 2: Configure with defined pool.

- CSCsy97775

  Symptoms: A router crashes.

  Conditions: The symptom is observed when the maximum allowed NBAR custom protocols are configured and protocol discovery is enabled.

  Workaround: There is no workaround.

- CSCsy97820

  Symptoms: False positives are seen in matching object groups with variable masks.

  Conditions: The symptom is observed when non-matching traffic is sent.

  Workaround: Do not use variable masks and contiguous masks, such as 255.0.255.255. Use only contiguous masks.

- CSCsz00890

  Symptoms: Cisco 7200 router crashes.

  Conditions: Occurs when Distributed LFI over ATM (dLFIoATM) is configured on a Cisco 7200 and a QoS policy is attached.

  Workaround: There is no workaround.

- CSCsz02000

  Symptoms: Router reloads at “atm_update_bundle_counters”.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsz02943

  Symptoms: Stateful fail-over of network address translation (SNAT) in primary/backup mode does not converge when TCP connect is shut down and then turned back on.

  Conditions: It is seen with SNAT in primary/backup mode. Before the following conditions, both primary/backup routers is fully converged once.

  1. Shudown the SNAT interface of primary router and reload the primary router. Perform a **shutdown** on the SNAT interface of the primary router.
  2. Shutdown the interface of the switch between SNAT routers. After 5 minutes, the SNAT peer is down. Enter **no shutdown** on the interface of the switch.

  Workaround: Perform **shut/no shut** on the SNAT interface of the primary router.

- CSCsz03260

  Symptoms: A gateway may take an exception when receiving an inbound H320 call when the call is placed via ISDN overlap sending.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T1.

  Workaround: There is no workaround.

- CSCsz05783

  Symptoms: Voice/SIP (ef) packets are not marking in the ingress/egress when NAT is enabled on the interface.

  Conditions: Occurs when NAT is enabled.

  Workaround: Remove NAT from the configuration.

- 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.

- CSCsz11877

  Symptoms: MPLS-TE tunnel label reallocation on midpoint router occurs while RSVP is gracefully restarting due to CPU switchover.

  Conditions: Occurs on a Cisco 7600 that is configured as the midpoint router when the upstream node is a Cisco IOS-XR router. This does not happen if the upstream node is also a Cisco IOS router. Because of this label re-allocation, traffic downtime is ~100 msec

Workaround: There is no workaround.

- 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.

- CSCsz13800

  Symptoms: An alignment error is seen on an IPv6 DHCP server every few minutes.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T. The router may face an alignment error when running as a DHCP server.

  Workaround: There is no workaround.

- CSCsz14236

  Symptoms: LLC stops forwarding I frames, but continues to respond to poll frames.

  Conditions: The symptom is detected when the output from **show llc** shows that frames are queued up for transmission in the Tx Queue. If DLSw is transporting the LLC frames, the associated DLSw circuit will show that the link is in a max congestion state.

  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.

- CSCsz16277

  Symptoms: A router crashes.

  Conditions: The symptom is observed when many (10 or more) SSLVPN clients are connected and router is under load (CPU>30%).

  Workaround: There is no workaround.

  Further Problem Description: Before the crash, typically the IO memory gets depleted. This can be verified with the **show memory statistics history** command.

- 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.

- CSCsz16635

  Symptoms: One-way audio may be experienced on a call which traverses a transcoder hosted on an ISR platform (e.g.: Cisco 2800, 3800 etc) after a hold, resume, or transfer.

  Conditions: When the call is held or resumed, there is a significant change in the RTP Sequence Numbers but the SSRC does not change. This behavior may cause the receiving device to assume that the RTP packets are out of sequence (i.e.: late, early, or lost) and therefore the receiving device may drop them.

Workaround:

1. A hold/resume from the phone receiving the out-of-sequence RTP audio packets will restore normal reception of audio.
2. If possible, use a Communications Media Module (CMM) module for transcoding while ensuring that the Cisco IOS Release used on the CMM module has the fix for CSCsi27767.
3. If possible, eliminate the need for a transcoder in the audio path for affected call flows.
4. This problem does not affect Cisco IOS Software Media Termination Points (MTPs) nor SW MTPs hosted on a Cisco Unified Communications Manager (CUCM) server. So, if like-to-like capabilities (i.e.: codec and packetization) are being used, then using a SW MTP via IOS or CUCM may be an option.

Further Problem Description: This issue looks very similar to CSCsi27767 which was opened and resolved against the Catalyst 6000's CMM. The fix for CSCsi27767 is, however, only intended for the CMM platform.

IOS DSPFarm services and voice gateways will now avoid generating discontiguous RTP sequence numbers with the same SSRC, by using a new SSRC and setting the marker bit of the first RTP packet for the new SSRC whenever its DSP restarts the RTP sequence number due to call features such as call transfer, hold, resume, etc.

- CSCsz16941

  Symptoms: A TR-069 Agent becomes disabled on the router and the device is unreachable from the ACS server.

  Conditions: The symptom is observed when a TR-069 Agent is enabled and running on a router and the default WAN interface is configured and has a DHCP-assigned IP address. When the configurations are saved and the router is reloaded the issue is seen.

  Workaround: If possible, do not save the configurations on the router when the WAN interface gets a DHCP-assigned IP address.

  Alternate workaround: Use the **write erase** command and remove all the configurations just before every router reload.

- CSCsz18018

  Symptoms: When a router sends the CRL request via HTTP, the CA might respond with 404 HTTP error, even when the URL is configured properly. The PKI debugs show extra trailing characters added to the URL.

  Conditions: The symptom is observed when a router sends the CRL request via HTTP.

  Workaround: Try using LDAP-based CRL check or disable CRL checking temporarily under the trustpoint configuration.

- CSCsz20496

  Symptoms: A Cisco VG224 voice gateway displays the wrong secondary dial tone to the customer if "cptone CN" is configured under the voice-port.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(24)T, 12.4(20)T1, and 12.4(9)T7.

  Workaround: Upgrade to the latest IOS version (see bug CSCsk28301) and change the dial_tone2 to make it same as the dial tone by using the command **test voice tone cn 2nd_dialtone**:

```
event manager applet setCNsecondDialtone event syslog occurs 1 pattern
".*%SYS-5-RESTART: System restarted --.*" action 1.0 syslog msg "Setting DIAL_TONE2
for cptone CN" action 2.0 cli command "enable" action 3.0 cli command "test voice tone
CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0" action 4.0 syslog
msg "DIAL_TONE2 for cptone CN has been set"
```

Copy the script to the running-configuration and then save it to NVRAM. If the router reloads, the setting “test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0" will automatically be re-asserted. If you want the command set immediately without a reload then cut and paste the command directly at the EXEC prompt.

- CSCsz21577

  Symptoms: SIP-NAT SBC does not properly preserve the Contact Header for outside-to-inside translations.

  Outside Packet:

  ```
  Contact: "EMTAlinea1"<sip:1188800099@192.168.15.10:1032;transport=udp>;expires=1674
  ```

  Inside Packet:

  ```
  Contact: "EMTAlinea1"<sip:118880099@10.0.2.101:5060;expires=60
  ```

  Conditions: Only seen on outside-to-inside translations when using the registration-throttle feature.

  Workaround: There is no workaround.

- CSCsz23730

  Symptoms: The ATM/IMA virtual interface is always down on a Cisco 3845 router.

  Conditions: The symptom is observed on a back-to-back E1/T1 ATM-IMA setup (E1/T1 with ATM-AIM card). When “ima-group” is configured under the ATM interface, the ATM link goes down and does not come up. The E1/T1 controllers will be up, but the ATM/IMA link will be down.

  Workaround: There is no workaround.

- CSCsz23976

  Symptoms: A Cisco 7200 series router that is running Cisco IOS Release 12.4(15)T7 may experience an unexpected reset while forwarding traffic with a Cisco 7200 VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router running with a Cisco 7200 VSA installed on Cisco IOS 12.4(15)T code.

  Workaround: There is no workaround.

- 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.

- CSCsz24971

  Symptoms: A router crashes with multiple uses of the **vc-group** command.

  Conditions: The symptom is observed when deleting a VC-group from a VTY while configuring the same VC-group in the TTY.

  Workaround: Do not do a multiple user operation in the VC-group at the same time.

- 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%.

- CSCsz29320

  Symptoms: A Cisco 3845 running Cisco IOS Release 12.4.(20)T2 reloaded due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process MGCP Application running low, 0/12000
  %Software-forced reload
  ```

  Conditions: The crash suggests that the issue is just one of inefficient stack usage.

  Workaround: There is no workaround.

- CSCsz29542

  Symptoms: In the current implementation, “cwmp agent” identifies the WAN uplink if it has “cwmp wan default” configured on it. The WAN uplink interface differs, based on the router type used as a CPE. For the Cisco 871 router, WAN interface is FastEthernet 4 and for a Cisco 2811 router it is Fast Ethernet 0/0. This creates a problem in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Conditions: The symptom is observed in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Workaround: There is no work around.

- CSCsz29815

  Symptoms: TTY sessions not accessible after reverse SSH session to the same TTY port results in failed authentication.

  Conditions: Occurred on a router running Cisco IOS Release 12.4(24)T and configured with TTY lines accessed using reverse SSH Version 2. Issue also affects SSH version 1 and affects VTY lines.

  Workaround: Reload the router.

- CSCsz30204

  Symptoms: A router reloads after “dot1q vlan range” is unconfigured under the dot11 interface.

  Conditions: The symptom is observed under the following conditions:

  1. A router acting in non-root mode is associated to a parent AP.
  2. “dot1q vlan range” has been configured and unconfigured.
  3. Dot11 radio interface is configured to receive an IP address from DHCP.

  Workaround: There is no workaround.

- CSCsz31940

  Symptoms: Active secure NAT (SNAT) continuously prints the following tracebacks and the router is not operational while tracebacks are printed:

```
%SYS-2-INSCHED: suspend within scheduler -Process= "<interrupt level>", ipl= 1,
-Traceback= 0x41732A78 0x4009B8AC 0x42DF1EC8 0x41F780E4 0x41F9E790 0x41F53274
0x41F7D830 0x400ECDD8 0x40069574 0x439BE7A8 0x439BC010 0x40047734 0x4000FCC0
```

Conditions: The symptom is observed when flow switching and SNAT are configured on the router interface and SNAT traffic passes through the router.

Workaround: Stop the SNAT traffic and wait for the tracebacks to clear.

- CSCsz32366

  Symptoms: A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

  Conditions: This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

  Workaround: Do not use SSH. Disable SSH on the router by removing the RSA keys “crypto key zeroize rsa”

  Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

- CSCsz34920

  Symptoms: Router continuously reboots.

  Conditions: The symptom is observed when an NME-502 is installed in the router.

  Workaround: Replace or take out the NME-502.

- CSCsz35204

  Symptoms: A Cisco 2821 router reloads sporadically, after enabling WebVPN using clientless web proxy method and extended access.

  Conditions: The symptom is observed with a Cisco 1841 router and a Cisco 2800 series router that is running Cisco IOS Release 12.4(24)T under moderate to heavy traffic.

  Workaround: There is no workaround.

- CSCsz36002

  Symptoms: GETVPN traffic stops. Upon entering **show crypto engine accelerator statistic**, you will see the “ppq full” counter going up.

  Conditions: Occurs on a Cisco 3800 running Cisco IOS Release 12.4(22)T or 12.4(24)T.

  Workaround: Either reload the router or enter the following sequence of commands:

  ```
  configure terminal
  no crypto engine accelerator
  crypto engine accelerator
  ```

- CSCsz43987

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip.

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

- CSCsz44220

  Symptoms: Passive FTP flows are not classified by NBAR if they are translated by NAT.

  Conditions: The symptom is observed under the following conditions:

  1. It is seen in both directions: input and output.
  2. It is verified with fast Ethernet, ATM PVC, serial and dialer interface only.
  3. It is observed with Cisco IOS T train releases only.

  Workaround: Use Cisco IOS mainline code.

- CSCsz45286

  Symptoms: A Cisco 2800 series router crashes upon configuring VRRP under a Dot11 radio interface.

  Conditions: The symptom is observed when the router is associated and operating in non-root mode.

  Workaround: There is no workaround.

- CSCsz45539

  Symptoms: Unable to attach the frame relay DLCI to the serial subinterface. The following error is received:

  ```
  %PVC already assigned to interface Serial3/0
  ```

  Conditions: The symptom occurs with a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-ldp.

- CSCsz45855

  Symptoms: Cisco Unified Border Element (CUBE) ignores reINVITEs from Cisco Customer Voice Portal (CVP).

  Conditions: While call transfer is in progress and CUBE is waiting for NOTIFY (with 200 or any final response code) after receiving NOTIFY (with 100), it receives INVITE.

  Workaround: There is no workaround.

- CSCsz48086

  Symptoms: Default violate-action is missing from three color policy.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsz48392

  Symptoms: Doing reverse SSH to a TTY line, which is busy, causes the terminal server to crash.

  Conditions: This issue is encountered in a Cisco 3845 router that is running Cisco IOS Release 12.4(23).

  Workaround: There is no workaround.

- CSCsz48614

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-cucme.

- CSCsz48680

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sip.

- CSCsz48914

  Symptoms: Next Hop Resolution Protocol (NHRP) registration and tunnels are not up between first- and second-level hubs.

  Conditions: Occurs in hierarchical topology.

  Workaround: There is no workaround.

- CSCsz49741

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-cucme.

- CSCsz50091

  Symptoms: A hub router acting as the RP in a DMVPN environment with tunnel setup between hub and spoke and with VRF forwarding, does not form the (*,G) entry in the multicast routing table when hosts connected to the spoke join a multicast group using the **ip igmp join-group** command.

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsz50275

  Symptoms: The firewall is configured to reset if an invalid command goes through the unit under test. But the reset action does not happen, and this functionality issue observed all inspected application traffic, such as IM, SIP, and P2P.

  Conditions: This problem occurs both when Cisco Common Classification Policy Language (C3PL) is used, and when it is not used.

  Workaround: There is no workaround.

- CSCsz50362

  Symptoms: “DHCPRELEASE” messages are not received in server routers.

  Conditions: This issue is seen in routers loaded with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsz52576

  Symptoms: The vlan.dat file gets deleted after the second reload of the router, and the VLAN definition and names are lost (not the interfaces and IP addresses). It has been observed that when the vlan.dat is lost, in “sh vtp status” the VTP Domain Name is blank (and was properly configured before).

  Conditions: This behavior is observed in a Cisco 3270 router that is running Cisco IOS Release 12.4(24)T. It is also observed with Cisco 1800 ISR with switch modules in Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround. Customer needs to reconfigure them again after reboot. This problem is not observed in Cisco IOS Release 12.4(15)T.

  Further Problem Information: When a customer is running an image that does not store the VTP and VLAN information in the start-up configuration or the normal output of show running-config, the vlan.dat file gets overridden to the default vlan.dat approximately 2 minutes after reboot. The current VLANs and VTP information remains operational until the router is rebooted.

  A reboot causes the VLANs and VTP information to disappear because the start-up configuration does not contain any VLAN or VTP information, nor does the vlan.dat file in flash.

The operating VTP information appears in the output of show running-config all (which shows non-default and default values), indicating that the router considers the VTP information to be at default values even when there is a VTP domain name configured. This allows the VLANs and VTP to remain operational until the router is rebooted.

- CSCsz52815

  Symptoms: If number of hours for statistics is increased to 10 or more after the probe is initially run and then restarted, system crashes with memory corruption

  Conditions: Occurs when the probe is started with the hours of statistics less than 10 and then re-started with the hours of statistics greater than 9.

  Workaround: There is no workaround.

- CSCsz53177

  Symptoms: When running Network Load-balancing (IGMP-mode) in VLANs with PIM enabled and static ARP entries for unicast IP to layer-2 multicast address, packet duplication will occur.

  Conditions: This symptom occurs when sending unicast (non-multicast) IP packets with multicast layer-2 destinations.

  Workaround: Use non-IGMP NLB modes (unicast or multicast with static macs) or use IGMP snooping querier instead of PIM on NLB SVIs.

- 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.

- CSCsz56805

  Symptoms: Different IPs are seen on the same session between Active and Standby PRE cards and the number of in-use IP addresses on Standby is more than that on the Active.

  Conditions: The symptom is observed with the frequent connect/disconnect of sessions and when IP addresses are allocated from the local pool.

Workaround: Reload the Standby card frequently.

- CSCsz58813

  Symptoms: Cisco UC500 console displays the following log(s) constantly:

  `%PQII_PRO_FE-4-QUEUE_FULL: Ethernet Switch Module transmit queue is full.`
  Phones and hosts connected to the UC can not retrieve IP addresses via DHCP.

  Conditions: This problem occurs shortly after a reload of the Cisco UC500 (on the CME side). This problem is observed after upgrading from Cisco IOS Release 12.4(20)T2 to Cisco IOS Release 12.4(20)T3.

  Workaround: There is no workaround.

- CSCsz60659

  Symptoms: The cooperative GDOI keyserver starts printing `%GDOI-5-COOP_KS_REACH` and/or `%GDOI-5-COOP_KS_UNREACH` syslog messages.

  Conditions: The symptom is observed if two or more ISAKMP connection attempts fail, which might be normal in production networks.

  Workaround: There is no workaround.

  Further Problem Description: In fixed versions, the logic of the reachability test was changed to avoid this problem.

- CSCsz61665

  Symptoms: The “icmp-echo timeout” value is lost upon a system reload.

  Conditions: The issue occurs upon a reload if the timeout value is less than the default threshold value of 5000.

  Workaround: Increase the timeout value to be greater than or equal to 5000.

- CSCsz62974

  Symptoms: Router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: Occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- 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.

- CSCsz66965

  Symptoms: After the activation of the HW encryption modules (VSA), the following message is logged by Cisco 7200:

  `%VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Unknown Error`
  There is a traffic impact towards the destination mentioned in the error.

  Conditions: This symptom occurs when VSA hardware encryption is used on a Cisco 7200 with Time-based anti-replay (TBAR) enabled.

  Workaround: Disable Time-based anti-replay (TBAR).

  Further Problem Description: This happens when VSA receives a very small UDP fragment that is less than 26 bytes.

- CSCsz68373

  Symptoms: After configuring NAT, traffic fails to hit the policy-map of the frame-relay serial interface.

  Conditions: This issue is seen with NM-1T3/E3 of a Cisco 3845 router only when NAT is configured.

  Workaround: Remove and re-apply the frame-relay map-class under serial interface after NAT is configured.

- CSCsz70486

  Symptoms: On a Cisco 7200 series router with a VPN Services Adapter (VSA) installed, the outbound interface Access Control List (ACL) is not checked if a crypto map is applied to the interface and Cisco Express Forwarding (CEF) is enabled globally.

  Conditions:

  1. Egress ACL configured on the interface.
  2. A crypto map is applied to the same interface.
  3. VSA is installed in the chassis.
  4. CEF is enabled.

  Workaround: Remove the VSA or the crypto map, or disable CEF.

- CSCsz71392

  Symptoms: WCCP stops functioning when GDOI SA is accelerated by VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T with VSA (FPD 0.23). It is seen when **ip wccp** *61* **redirect out** and **ip wccp** *62* **redirect in** are applied to the inside interface, and traffic gets WCCP GRE redirected to WAE. When GDOI crypto-map (currently in inbound-only state) is applied to the outside interface, traffic is returned from WAE via WCCP and GRE gets dropped within UUT.

  Workaround: Disabling VSA with **no crypto engine slot 0** restores connectivity to normal.

- 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.

- CSCsz74629

  Symptoms: There is a delay in the propagation of interface link down state. Link failure is detected with a huge delay once the other end of the link gets disconnected.

  Conditions: The symptom is observed on a Cisco 1861 router that is running Cisco IOS Release 12.4(24)T.

  Workaround: The default keepalive period is 10 seconds and the periodic function which updates the link state change runs on the order of keepalive time, hence it takes long time to detect the link down state. If keepalive is set to 1 or 2 seconds, the time taken to detect link down is normal.

- CSCsz74859

  Symptoms: NHRP cache entry is not getting created for certain spoke nodes.

Conditions: This symptom occurs when two spokes A and B advertise the same subnet with varying masks (anything other than /8 or /16 or /24). A third spoke upon receiving such routes (from the hub), in order to send traffic to such subnets, can form a dynamic tunnel with either A or B but not both at the same time.

Workaround: There is no workaround.

Further problem description: There is no hindrance to traffic since it continues to flow via the hub. When tunnel with spoke A is formed, there is no problem with traffic to subnet behind spoke A. But, traffic to subnet behind spoke B takes the spoke A - hub - spokeB path. This can be easily noted by traceroute.

- CSCsz75186

  Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-tcp.

- 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.

- 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. Enable blank_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.

- CSCsz79001

  Symptoms: A Cisco 87x router may hang or crash after displaying “Now reloading” during ROMmon upgrade when using the **upgrade rom-monitor file flash:** command.

  Conditions: This occurs when a router running ROMmon release 12.3(8r)YI4 or an older ROMmon from alternate space is upgraded to YI5 or a newer ROMmon version

  Workaround: Power cycle the router to recover from this hang state. The router will then boot with the upgraded ROMmon.

- CSCsz79901

  Symptoms: Firmware file download using the TR-069 Agent on a router fails.

  Conditions: The symptom is observed when doing a firmware upgrade using the TR-069 Agent on a router and when the URL is given as “http://{ip address}/dir/filename.bin?{name}={value}”. This issue is noticed only with the TR-069/CWMP Agent.

  Workaround: Firmware download works if the URL is given as “http://{ip address}/dir/filename.bin”.

- CSCsz79943

  Symptoms: A router may issue the following errors:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level, -Traceback=
  0x40095578z 0x42AF8DA0z 0x41EF2CB4z 0x41EFA250z 0x41647960z 0x4164930Cz 0x41649908z
  0x41649974z 0x42503B44z 0x425049CCz 0x423C78BCz 0x423B2B28z 0x4244C1F4z 0x4244C378z
  0x411CE1ECz 0x411CF234z
  %SYS-2-MALLOCFAIL: Memory allocation of 212 bytes failed from 0x41F023EC, alignment 0
  Pool: Processor Free: 120987132 Cause: Interrupt level allocation Alternate Pool: None
  Free: 0 Cause: Interrupt level allocation -Process= "<interrupt level>", ipl= 1, pid=
  111, -Traceback= 0x4007D714z 0x400955A8z 0x42AF8DA0z 0x41EF2CB4z 0x41EFA250z
  0x41647960z 0x4164930Cz 0x41649908z 0x41649974z 0x42503B44z 0x425049CCz 0x423C78BCz
  0x423B2B28z 0x4244C1F4z 0x4244C378z 0x411CE1ECz
  ```

  Conditions: The symptoms are observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(24)T with EZVPN configured.

  Workaround: There is no workaround.

- CSCsz81308

  Symptoms: Using “send break” causes router to display “TLB Miss exception” error and hang indefinitely.

  Conditions: Occurs on a Cisco 800 router running Cisco IOS Release 12.4(24.6)T9.

  Workaround: There is no workaround.

- CSCsz82825

  Symptoms: When relaying to multiple servers, from an unnumbered interface, the Cisco IOS DHCP relay sends packets to all servers, even for packets where the client in a RENEWING state unicasting to attempt to reach a single server.

  ARP entries are retained for all OFFERed addresses, even if the client ultimately is using a different address. These extra ARP entries persist for several hours.

  Conditions:

  1. When relaying a DHCP packet on an unnumbered interface, and the DHCP client is in a renewing state (as determined by the fact), send it to the DHCP server that allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions.
  2. When the client is in any other state, or if we do not get a response from the DHCP server, send to all helper-addresses.

  Workaround: There is no workaround.

  Further Problem Description: Only retain an ARP entry for the address that the DHCP client acknowledges. Do not retain addresses offered by DHCP servers that the client did not use in the ARP table.

- CSCsz85919

  Symptoms: A router reloads with a SegV exception.

Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.4(20)T2 with both NAT and output ACLs configured. It occurs when the packet size changes due to NAT (this can happen with SIP/H.323 etc).

Workaround: There is no workaround.

- CSCsz89904

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-sip.

- CSCsz92137

  Symptoms: A router crashes upon configuring **tunnel protection ipsec profile** from a given tunnel interface.

  Conditions: The symptom is observed using the following steps

  1. Unconfiguring tunnel protection.
  2. Shutting down the tunnel interface.

  Workaround: There is no workaround.

- CSCsz92463

  Symptoms: GetVPN Key Servers no longer function in cooperative mode. The Key Servers (KSs) will fail to communicate with each other, and each will assume it is the primary. GMs registering to different KSs will not be able to communicate with GMs registered to a different KS.

  Conditions: This symptom occurs when using GetVPN Key Servers in cooperative mode.

  Workaround: There is no workaround.

- CSCsz92924

  Symptoms: CPU HOG in Crypto ACL is seen on the GM. The GM may crash some milliseconds later after printing the hog.

  Conditions: This symptom is observed on a large ACL on the KS (greater than 70 lines) with or without large ACL locally on the GM.

  Workaround: Limit the ACL length drastically.

- CSCsz93207

  Symptoms: In an EZVPN scenario, the traffic to the internet is not getting NATed.

  Conditions: The symptom is observed in an EZVPN scenario with “identical addressing” and “split tunnel” configured.

  Workaround: Use Cisco IOS Release 12.4(15)T3.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCsz97833

  Symptoms: HTTP-based certificate revocation list (CRL) checking fails.

  Conditions: Occurs due to an extra character appended to the URL.

  Workaround: Disable CRL checking.

- CSCta02089

  Symptoms: There is a crash on a Cisco AS5400 due to CPU signal 10.

  Conditions: The symptom is observed on a Cisco router due to expiration of freed receive_digit timer in SIP

  Workaround: There is no workaround.

- CSCta02460

  Symptoms: On a router that has a PRI trunk towards the PSTN, you may hear dead air when calling any ISDN device that returns cause code 0x8484 in a PROGRESS message that also contains a progress_ind with value 8.

  Conditions: The symptom is seen when using the primary-4ess (PRI 4ESS) and primary-5ess (PRI 5ESS) switch type.

  Workaround: There is no workaround.

  Further Problem Description: The problem was discovered when a user attempted to call a cell phone on a wireless network that was switched off. The user did not have voicemail, and the wireless network played a message in the band to alert that the phone was off. It is this message that should be heard - but it is not, due to this bug.

  The issue is due to an invalid cause value sent from the provider for an outgoing to call to a mobile phone which is switched off. The cause value of 4 is not supported by PRI 4ESS switches. Hence ISDN will send a STATUS message reporting invalid information element contents and the provider disconnects the call.

- CSCta04123

  Symptoms: A router may crash with a “STACKLOW” message or memory corruption.

  Conditions: The symptom is observed when the router is configured for IP inspect (only a basic IP inspect configuration is necessary).

  Workaround: Disable IP inspect.

- 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.

- CSCta05809

  Symptoms: A group member on a GETVPN network may stop passing encrypted traffic.

  Conditions: A GETVPN group member (GM) may accept and process an old or duplicate rekey message from the designated key server (KS). If the rekey message includes a TEK which was previously used to encrypt data, but which has already expired, the GM may become unable to send and receive encrypted traffic.

  Workaround: There is no workaround.

- CSCta07228

  Symptoms: IAD images do not boot.

  Conditions: The symptom is observed when booting up IAD2430 images with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCta07484

  Symptoms: A crash may occur on a CME when doing a web query on an ephone.

  Conditions: The symptom is observed when doing a web query on an ephone and maximum SIP phones are not configured on the CME under “voice register global”.

  Workaround: Configure maximum supported SIP phones under “voice register global”.

- CSCta10569

  Symptoms: After decryption, unicast traffic with a frame size of 1447 or above drops on a Cisco 7200 series router.

  Conditions: The symptom is observed with unicast traffic after it gets decrypted and only if the frame size is greater than or equal to 1447.

  Workaround: There is no workaround.

  Further Problem Description: Only unicast traffic gets dropped after decryption. Multicast traffic does not drop even if the frame size is greater than or equal to 1447.

- 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.

- CSCta12296

  Symptoms: Group member router crashed.

  Conditions: Occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: There is no workaround.

- CSCta13035

  Symptoms: Incoming calls start failing over a certain PRI channels after 2-3 days of normal operation. The following message is seen:

  ```
  ISDN Se0/0:15 Q931: TX -> DISCONNECT pd = 8 callref = 0x8640 Cause i = 0x80AF -
  Resource unavailable, unspecified
  ```

  Conditions: The symptom is observed on a Cisco AS5400XM Universal Gateway.

  Workaround: Reload the Cisco AS5400.

- CSCta18454

  Symptoms: CN is unable to ping MN due to a tunnel failure on the HA.

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

  Workaround: There is no workaround.

- CSCta19962

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

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-h323.

- CSCta20040

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip.

  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://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

  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

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

- CSCta21892

  Symptoms: VPN client with certificates will fail IKE negotiations and show the following messages:

  ```
  Sev=Warning/2IKE/0xE300009B Failed to validate the payloads (MsgHandler:105)
  Sev=Warning/2IKE/0xE300009B Failed to process MM Msg 6 (NavigatorMM:570
  ```

  Conditions: The symptoms are observed with the following conditions:

  1. VPN client connects to a router with certificates.
  2. The router must be running Cisco IOS Release 12.4(24)T or later, or a version with the fix for CSCsv04325.

  Workaround: Use a Cisco IOS Release prior to 12.4(24)T.

  Further Problem Description: This issue is due to a change in Cisco IOS Release 12.4(24)T where the router will send the IKE phase 1 lifetime notification in MM6 (main mode 6th packet) and the client will reject it.

- CSCta22939

  Symptoms: Even if the EzVPN is down, NAT is calling EzVPN API to check if the EzVPN is interested in the packet to NAT.

  Conditions: The symptom is observed if external NAT is configured.

  Workaround: There is no workaround.

- CSCta24037

  ```
  Symptoms: A Cisco router may reload due to a bus error and show the following
  messages:
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  TLB (store) exception, CPU signal 10, PC = 0x415A2630
  ```
  Conditions: The symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCta25832

  Symptoms: Intermittent call failures occur through a Cisco AS5350XM or AS5400XM gateway.

  Conditions: The gateway is configured as an ISDN gateway. The **show voice call summary** command will show b-channels stuck as shown below:

  ```
  #show voice call summary  PORT CODEC VAD VTSP STATE VPM STATE
  ============== ========= === ==================== ======================
  3/6:D.13 g711ulaw n S_CONNECT S_TSP_WAIT_RELEASE
  ```
  This is usually seen after the gateway has processed a very high number of calls (~200,000 calls or more).

  Workaround: There is no workaround.

- CSCta26029

  Symptoms: Path attribute memory leak is found when there is some path attribute churn in the network.

  Conditions: The symptom is seen only when there are idle peers on the router.

  Workaround: Unconfigure the idle peers.

- CSCta26717

  Symptoms: IP phones do not register when an IOS firewall is configured in the gateway.

  Conditions: The symptom is observed when using a gateway with an IOS firewall configured. After an upgrade, the IP phones connected to the gateway do not register with CallManager. This problem occurs with nested class maps and match access groups, such as:

  ```
  class-map type inspect match-any  protocols
    *****some protocols applied as filters*****
  class-map type inspect match-all traffic
   match class-map protocols
   match access group
  ```

  The problem will only be seen if the protocols to be matched require pin-holes in the ACL. That means whenever there is deep packet inspection involved, the data traffic fails.

  Workaround: Remove the ACLs or allow the data traffic on the relevant ports to pass through the ACL.

- 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.

- CSCta28068

  Symptoms: The Citrix server (XenApp 5.0) cannot be accessed through WebVPN when using IE. The following message is shown:

  Cookies required

  This web site uses cookies in order to provide you with access to your published resources. You must configure your browser to accept cookies. Contact your system administrator for assistance.

  Conditions: The symptom is observed when using IE and XenApp 5.0.

  Workaround: Use Firefox.

- CSCta30440

  Symptoms: Tracebacks are seen on router console when trying to ping a DMZ address space from a Pagent with the datagram size more than 10K bytes. If the repeat count is set to more than five, then tracebacks are thrown on console repeatedly and, after some time, the router hangs and it becomes unresponsive until it is reloaded.

  Conditions: The symptoms are observed with a datagram size of more than 10K bytes and repeat count of more than five with timeout as eight seconds.

  Workaround: Use smaller datagram sizes.

- CSCta35393

  Symptoms: CPE WAN Management Protocol (CWMP) agent on a Cisco Unified CallManager Express (CME) causes CPU to spike to 96%.

  Conditions: The symptom is observed when configuring the CWMP agent and placing a phone call.

  Workaround: Disable the CWMP agent.

- CSCta35496

  Symptoms: G.729b variant calls fail from MGCP controlled VG2XX to SIP trunk-side VG2XX.

  Conditions: The symptom is observed when sRTP is enabled on MGCP and SIP gateways. It is seen when the gateways are registered to CUCM and inter-region codec is set to G.729b.

  Workaround: Set to “TRUE” the CUCM Service parameter “Strip G.729 Annex B (Silence Suppression) from Capabilities Required Field”.

- CSCta39579

  Symptoms: VPN routing/forwarding (VRF) Network Address Translation (NAT) is not translating UDP traffic at all. The inside local IP is still used after NAT. If the inside local IPs are not routeable on the NAT outside side of the network this breaks all applications relying on UDP. ICMP and TCP traffic are not impacted

  Conditions: Occurs when NAT is inside a VRF. nat is in vrf

  Workaround: Make sure the inside local is known on the NAT outside side of the network.

- CSCta39763

  Symptoms: A Cisco router may experience a memory leak in the "ISDN Call Tabl" process, as seen in the output below:

  Router# **show memory all totals**

  Allocator PC Summary for: Processor Displayed first 2048 Allocator PCs only

  PC Total Count Name 0x6010B9E8 9891336 513 ISDN Call Tabl

  Conditions: This has been experienced on a Cisco 3845 router running Cisco IOS Release 12.4(22)T with ISDN configured.

  Workaround: There is no workaround.

- 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.

- CSCta43033

  Symptoms: Cisco Unified Border Element (CUBE) gives OLC reject during transfer despite correct codec negotiation. The cause code is 57.

  Conditions: Occurs under reasonable load and with many call transfers (such as CVP or IPCC environment).

  Workaround: There is no workaround.

- CSCta45116

  Symptoms: EAP-FAST authentication fails between router and client (PC or laptop running ADU).

  Conditions: The symptom is observed when the wireless client is running "ADUv2.x" and the router is running with Cisco IOS Release 12.4(15)T8.

  Workaround: Upgrade the wireless client ADU to version 3.x or 4.x.

- CSCta45845

  Symptoms: All show commands under crypto are showing blank outputs. For example **show crypto pki certificates** shows a blank output, even though there may be some crypto certificates on the device.

  Conditions: This happens only when using web interface to a Cisco IOS device. The commands are:

  ```
  certificates: Show certificates
  counters: Show PKI Counters
  crls: Show Certificate Revocation Lists
  server: Show Certificate Server
  session: Show PKI Session Data
  timers: Show PKI Timers
  token: Show PKI Token(s)
  trustpoints: Show trustpoints
  ```

  Workaround: There is no workaround.

  Further Problem Description: CCA uses HTTP(s) service to get the output. Even when the certificate is shown using telnet/SSH, CCA GUI shows as unconfigured.

- CSCta46486

  Symptoms: CPU hogging in IKE and traceback seen on headend router terminating large amount of DVTIs.

  Conditions: The symptom is observed with any kind of outage on the remote site or clearing large amount of tunnels with the headend router actively participating in the routing and re-distributing the routes learned via the tunnel to the central site.

  Workaround: There is no workaround.

- CSCta46650

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

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

  Workaround: There is no workaround.

- CSCta54049

  Symptoms: When removing the remote loopback under controller T1, a Cisco IAD2435-8FXS may reload.

  Conditions: The symptom is observed after executing the **loopback remote** command under controller T1. The Cisco IAD2435-8FXS may reload when removing the remote loopback by executing the command **no loopback**.

  Workaround: There is no workaround.

- CSCta56762

  Symptoms: A Cisco router acting as an IP SLA Responder may leak memory in the chunk manager.

  Conditions: The symptom is seen when the router is responding to VoIP RTP probes.

  Workaround: Stop the probes.

- 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**.

- CSCta63555

  Symptoms: A router crashes if running with Cisco IOS Release 12.4(24)T or later.

  Conditions: The symptom is observed if the SNR number change menu is selected from an extension mobility phone. The router crashes after submitting the change.

Workaround: Configure an SNR under the user-profile or logout-profile with which the extension mobility phone is provisioned.

- CSCta66915

  Symptoms: Ping fails.

  Conditions: The symptom is observed when you perform a shut/no shut on the interface.

  Workaround: Reload the router.

- CSCta67965

  Symptoms: A Cisco 7200 NPE-G1 may crash.

  Conditions: The symptom is observed when “ip pim sparse-mode” is added to the port-channel configuration and an OIR is performed on the FA-PA.

  Workaround: There is no workaround.

- CSCta68917

  Symptoms: Cisco IOS allows duplicate installation of the same SSL VPN Client (SVC) packages with different sequence numbers.

  Conditions: Because of this defect, uninstallation of the SVC package causes an error when the same package has been installed more than once.

  Workaround: Install a SVC package only once on the router with the required sequence number.

- 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.

- 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.

- CSCta75271

  Symptoms: When we change a policy-map from a pure precedence policy (only match precedence classes) to a pure DSCP policy (only match DSCP classes), it causes a crash.

  Conditions: When we remove the last precedence/DSCP class from a pure policy and replace it with DSCP/QoS_group, it causes a crash. Occurs in Cisco IOS Release 12.4(20)T and 12.4(24)T throttles.

  Workaround: Remove the service-policy from the interface, then make the change to the policy-map and reapply the service-policy on the interface again.

- CSCta77678

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

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

  Workaround: There is no workaround.

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

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

  Workaround: Clear VPDN again or reload the router.

- CSCta83318

  Symptoms: Tracebacks seen when attaching a service policy-map in an ATM PVC interface.

  Conditions: The symptom is observed when attaching a service policy-map in an ATM PVC interface.

  Workaround: There is no workaround.

  Further Problem Description: There is no impact on the router's operation.

- CSCta85026

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

```
Router(dhcp-config)#option 60 ascii Cisco AP c1240
% Invalid input detected at '^' marker.
Router(dhcp-config)#
```

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

  Workaround: There is no workaround.

- CSCta91556

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

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

  Workaround: There is no workaround.

- CSCta91735

  Symptoms: Contact and Via ports are rewritten to 0.

  Conditions: The symptom is observed under the following conditions:

  1. INVITE is sent from outside to inside.
  2. Contact and Via headers in the SIP packet have a different port than the one specified as the outside port the configuration.

  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.

- CSCta94296

  Symptoms: Some voice commands go missing, the router freezes on bootup, or there may be a crash on bootup with the following message:

  %ALIGN-1-FATAL: Illegal access to a low address.

  This is possibly seen with "Unable to save the data for mode. Too many saves" being printed on bootup.

Conditions: The symptom is observed when many global voice or CME commands are configured.

Workaround: Remove some global voice or CME feature commands.

- 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”.

- CSCta95621

  Symptoms: Firewall performance degradation is seen for HTTP traffic.

  Conditions: The symptom is observed when configuring a Zone Based Firewall to match HTTP traffic.

  Workaround: There is no workaround.

- CSCta96311

  Symptoms: Decrypted IPSec packets are not forwarded to the IVRF.

  Conditions: The symptom is observed with dual ISPs. It is seen when the primary default route is via a higher numbered interface and when crypto map is applied to both interfaces which go to the different ISPs.

  Workaround: Use the command **no ip route-cache cef** on the ingress interface of the incoming IPSec packet.

- 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.

- CSCtb03905

  Symptoms: The entPhysicalContainedIn value of HWIC-1GE-SFP ports is incorrect.

  Conditions: The symptom is observed with HWIC-1GE-SFP ports.

  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.

- CSCtb08032

  Symptoms: Unknown unicast packets are forwarded after bridging configuration is removed.

Conditions: The symptom is observed after bridging is unconfigured on the l2 ports of the router.

Workaround: There is no workaround.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (a.k.a. tunnel switching). The router may infrequently crash due to a bus error.

  This crash is limited to cases where at least one of the following VPDN group commands are configured:

  ip pmtu ip tos reflect

  Workaround: Disable the above mentioned commands. However the consequences of this on user traffic must be evaluated first.

- CSCtb16459

  Symptoms: Unable to export traffic from interfaces (other than Ethernet) using RITE.

  Conditions: The symptom occurs when trying to configure “inteface integrated-service-engine 1/0” under “ip traffic-export profile test”.

  Workaround: There is no workaround.

- 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.

- CSCtb23350

  Symptoms: With Time-Based Anti-Replay enabled when using GETVPN, the receiver may not detect and drop replayed packets even though the TBAR time threshold has been reached.

  Conditions: The symptom is observed with Time Based Anti-Replay enabled.

  Workaround: There is no workaround.

- CSCtb24514

  Symptoms: Spurious memory access observed when loading a configuration with frame-relay traffic shaping, frame-relay payload-compression and egress policy.

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCtb26955

  Symptoms: The following error message is seen:

  %CRYPTO-4-GM_REGSTER_IF_DOWN: Can't start GDOI registration as interface FastEthernet1.2 is down

  Problem: The interface is not actually down. The registration should go through.

  Conditions:

  1. Manually clear the rekey SA (**clear cry isakmp** *connid*).
  2. Wait for the re-registration to start.

  Workaround: Use the **clear cry gdoi** *group* command or remove and add the crytpo map. The manual deleting of rekey SAs is not a valid option.

  Further Problem Description: An incomplete check in the code interprets this as "the associated interface is down". The registration fails with the GM_REGSTER_IF_DOWN error message.

- CSCtb29256

  Symptoms: A router crashes after entering the **sh isdn history** command.

  Conditions: This issue is seen in a Cisco 7206VXR (NPE-G2) that is running Cisco IOS Release 12.4(15)T9.

  Workaround: Avoid using the **sh isdn history** command and use the **sh isdn active** command.

- CSCtb29640

  Symptoms: GETVPN GMs keep re-registering in multicast rekey mode.

  Conditions: The symptom is observed when multicast rekey mode is configured.

  Workaround: Switch to unicast rekey.

- CSCtb34358

  Symptoms: Tunnel sources get mixed up when tunnel interfaces are configured with serial subinterfaces as sources and the router is reloaded.

  Conditions: The symptom occurs only after a reload or when a saved configuration is applied to the running configuration.

  Workaround: There is no workaround.

- CSCtb34920

  Symptoms: Calls may intermittently be dropped or disconnected.

  The debug output for "debug isdn q931" will reveal that the gateway is sending a Q.931 INFORMATION message similar to the following:

  ```
  Aug 11 13:51:20.137 EST: ISDN Se0/2/1:23 Q931: TX -> INFORMATION pd = 8 callref =
  0x80AE
  ```

  The connected service provider switch may respond with a Q.931 STATUS message similar to the following:

  ```
  Aug 11 13:51:20.197 EST: ISDN Se0/2/1:23 Q931: RX <- STATUS pd = 8 callref = 0x00AE
  Cause i = 0x81E17B - Message type not implemented Call State i = 0x0A
  ```

  The connected service provider switch may also respond with a Q.931 DISCONNECT message similar to the following:

  ```
  Aug 11 13:51:20.297 EST: ISDN Se0/2/1:23 Q931: RX <- DISCONNECT pd = 8 callref =
  0x00AE Cause i = 0x81E4 - Invalid information element contents
  ```

  Conditions: This problem may occur when an ISDN PRI is configured to use "switch-type primary-4ess" or "switch-type primary-5ess."

This problem may occur when an IP phone user blind transfers a call to another destination (another IP phone, IVR, IPCC queue, etc). The transfer request triggers the Cisco Unified Communications Manager (CUCM) server to send an H.225 INFORMATION message with a Signal IE to the Cisco IOS H.323 gateway indicating to start/stop playing ringback tone toward the PSTN. The Cisco IOS H.323 gateway should generate the ringback tone, but it should NOT send the Q.931 INFORMATION message toward the connected service provider switch.

The 4ess spec indicates that the INFORMATION message is NOT supported per AT&T TR 41459 section 3.1.8. Also the Lucent AT&T 235-900-342 5ess spec does not even mention the INFORMATION message in section 4.2 which covers all other supported Q.931 message types.

Workaround: Another similar defect CSCsr38561 was previously opened for this same type of problem with “switch-type primary-ni” and has now been resolved.

If you are running a version of Cisco IOS, which has the fix for CSCsr3856, it “may” be possible to reconfigure the Cisco IOS gateway user side of the PRI to use “switch-type primary-ni” even though the connected service provider switch may be provisioned for 4ess or 5ess. This should only be used as a temporary workaround because it could expose other interworking errors due to switch-type mismatch configuration.

- CSCtb36384

  Symptoms: Memory corruption.

  Conditions: The symptom is observed with an unaligned IP packet in an interrupted switch path.

  Workaround: There is no workaround.

  Further Problem Description: This is very old code running across all the releases. The conditions which cause the issue are rare.

- 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 "
  " 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 "
  " action 002 if $line eq "" goto 004 action 003 end action 004 puts "Made it here"
  ```

- CSCtb38432

  Symptoms: EZVPN gets hung on a Cisco 871 router that is running Cisco IOS Release 12.4(24)T.

  Conditions: The symptom is observed when PPPoE renews the IP address and hangs at the “More” prompt.

  Workaround: Reconfigure the EZVPN command.

- CSCtb43009

  Symptoms: A Cisco 3845 router crashes when key server is removed from the list.

  Conditions: The symptom is observed with the following configuration on a GM router:

  ```
  conf t
  crypto gdoi group GetvpnScale1 identity number 1111
  no server address ipv4 10.10.1.4
  ```
  When a unicast rekey is received, the router crashes.

  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.

- CSCtb48852

  Symptoms: Multilink Frame Relay (MFR) bundle in HW mode.

  Conditions: Occurs when different PA members are added to MFR on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCtb48984

  Symptoms: SSLVPN Login Page is not being properly displayed on mobile devices. Also, there is no support for iPhone and iPod safari browsers.

  Conditions: The symptom is observed on an access page using Windows Mobile, or on an iPhone or iPod.

  Workaround: Page will be displayed but quality will be poor.

- 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 **show user** 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.

- CSCtb58160

  Symptoms: A router crashes upon bootup.

  Conditions: The symptom is observed when reloading a router with the NAM module configured.

  Workaround: There is no workaround.

- CSCtb58724

  Symptoms: The symptoms are:

  1. Incomplete rekey/ANN seqnum checking. This may cause inaccuracy in detecting seqnum errors in Co-operative key server (COOP KS) split/merge corner cases.
  2. After using the command **clear cry gdoi** on the GM, the GM may not register successfully due to a PST difference between the key server and the GM.

  Conditions: The symptom is observed in corner cases of COOP KS split/merge scenarios.

  Workaround: There is no workaround.

- CSCtb66273

  Symptoms: EzVPN traffic is getting dropped at the DVTI interface on the server.

  Conditions: The symptom is observed with an EzVPN DVTI server configured with split tunneling.

  Workaround: Removing the split tunnel configuration.

- CSCtb68229

  Symptoms: The box crashes within "cns config notify code".

  Conditions: This symptom is observed in the corner case when someone removes "cns config notify diff" from the config while adding other CLIs to the running config by using the method "config replace". The box can crash.

  Workaround: Do not remove "cns config notify diff" using "config replace".

- CSCtb68539

  Symptoms: There may be problems with downloading large packages from remote server to local server.

  Conditions: The symptom is observed when the package size is approximately greater than 4KB.

  Workaround: Use small packages.

- 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.

- CSCtb71889

  Symptoms: DNS A-answer from IPv4 DNS server (which is supposed to be forwarded to IPv6 side as AAAA-answer) is dropped on NAT-PT routers.

  Conditions: The symptom is observed when DNS NAT-ALG is enabled.

  Workaround: There is no workaround.

- CSCtb72653

  Symptoms: The router crashes when unconfiguring a policymap from a virtual interface.

  Conditions: This issue is seen only when the interface is a virtual interface and the configuration is changed after the interface flaps.

  Workaround: There is no workaround.

- 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.

- CSCtb79211

  Symptoms: A Cisco AS5400XM may process switch all traffic through interfaces. Other platforms may be affected.

  Conditions: The symptom is observed if you are running Cisco IOS Release 12.4(20)T or later and the interface is configured for netflow with one of the following feature sets:

  - c5400-ik9s-mz
  - c5400-ik9su2-mz
  - c5400-jk9su2_ivs-mz

  Workaround: Disable netflow.

- CSCtb86279

  Symptoms: Cisco IOS crashes at bootup.

  Conditions: The symptom is observed on a Cisco 1941 with 512MB of on-board memory.

  Workaround: There is no workaround.

- CSCtb87856

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

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

  Workaround: There is no workaround.

- CSCtb89819

  Symptoms: A single ping packet with size that is greater than or equal to 1501 bytes will cause a router with an ATM interface to crash.

  Conditions: The symptom is observed only when NAT or “ip virtual-reassembly” is configured on an ATM interface.

  Workaround: There is no workaround.

- CSCtb90751

  Symptoms: FTP and HTTP protocols are not supported for the remote download of FPM packages.

  Conditions: The symptom is observed with the remote download of FPM packages.

  Workaround: Use TFTP, SCP, or HTTPS.

- 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.

- CSCtb98080

  Symptoms: When you attempt to browse to a WebVPN portal you only see a blank page. The router does not send the browser a certificate and the portal login page is not displayed. The command **debug webvpn sdps** logs the following error message:

  ```
  WV-SDPS: Sev 4:sslvpn_tcp_read_notify(),line 1569:No to notify read: already queued[1]
  004549:
  ```

  Conditions: The symptom is observed when the SSLVPN process is waiting for an HTTP REQUEST from a client on the port configured using the **http-redirect <port no>** command but the process does not wake up. This can happen because of an unexpected IPC message to the SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect** from the WebVPN gateway and reload the device.

- CSCtc13085

  Symptoms: The keys used in the PI11 code for encrypting and decrypting FPM filters in eTCDF are dummy keys, used for internal testing. Those keys need to be replaced with actual keys for encrypting and decrypting filters.

  Conditions: The symptom is observed with the keys used in the PI11 code for encrypting and decrypting FPM.

  Workaround: There is no workaround.

- CSCtc21389

  Symptoms: IMA subinterfaces do not come up.

  Conditions: Occurs if the number of PVCs exceeds 255.

Workaround: Do not create more than 255 PVCs.