Release Notes for Cisco IOS Release 12.4(24)GC5

Current Release:
12.4(24)GC5 - November 19, 2012

Previous Release:
12.4(24)GC4
12.4(24)GC3
12.4(24)GC2
12.4(24)CG

The following release notes support Cisco IOS Release 12.4(24)GC5. They are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and how to obtain support and documentation.

Contents

This publication consists of the following sections:

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

Image and Documentation Information

These images are bug compatible with Cisco IOS release 12.4(24)GC5.

The following Cisco IOS images are part of this release:

- c1861-adventerprisek9-mz
- c1861-advipservicesk9-mz
- c2800nm-adventerprisek9-mz
- c2800nm-advipservicesk9-mz
- c2801-adventerprisek9-mz
- c2801-advipservicesk9-mz
- c3250-adventerprisek9-mz
- c3270-adventerprisek9-mz
- c3825-adventerprisek9-mz
- c3825-advipservicesk9-mz
- c3845-adventerprisek9-mz
- c3845-advipservicesk9-mz

Note You must have a Cisco.com account to download the software.

The following documentation is available for use:

- *Mobile Ad Hoc Networks for Router-to-Radio Communications* (OL-19437-02)

New Features

New Features for Cisco IOS Release 12.4(24)GC5

No new features have been added to this release.

New Features for Cisco IOS Release 12.4(24)GC4

No new features have been added to this release.

New Features for Cisco IOS Release 12.4(24)GC3

No new features have been added to this release.

New Features for Cisco IOS Release 12.4(24)GC2

The following features have been added to this release:

- Support for QoS (MQC)

Limitations

The following limitations exist in this release:

- The QoS policy can only be applied to one outgoing interface the PPPoE session is traversing.

  A QoS output policy can be applied to the Virtual Template or the VMI, but not at the same time. If a policy is attached, the outgoing physical interfaces (ie. physical-interface FastEthernet0/0) should not have output policy applied. It is recommended that the policy be attached to the Virtual Template. The other option is to apply the policy to the VMI but not to the Virtual Template or Ethernet interface.
- When a service policy is applied to the VMI and packets are dropped on the VA due to credit starvation, the **show policy-map int** VMI command will not show these dropped packets. There is no backpressure between the interfaces in this configuration. The VMI does not know that packets were dropped by the VA or the Ethernet physical interfaces.
- RFC 5578 credits do not tie into QoS formulas. Credits only indicate to QoS the ability to transmit a packet or not. If there are enough credits a packet will be transmitted from the highest priority queue. When there are not enough credits, packets will be queued.
- Software Release 12.4(24)GC4 may have OSPFv3 incompatibility issues with software versions 12.4(22)GC1 or older. To avoid any issues, ensure that all routers run the same version of Cisco IOS.

Troubleshooting

Use the following command to collect data when reporting router issues:

- **show tech**

Use the following command to collect data to confirm neighbor establishment:

- **show vmi neighbor**

Use the following command to display active PPPoE sessions:

- **show pppoe session**

Use the following command to examine QoS issues:

- **show policy-map interface virtual-access** *interface-number*

Use the following commands to debug vmi issues:

- **debug vmi error**
- **debug vmi pppoe**

Use the following commands to verify PPPoE and VMI interface operation related to credit information:

- **show vmi neighbor detail**
- **show pppoe session all**

Use the following command to debug PPPoE issues:

- **debug pppoe error**

Use the following command to display OSPFv3 traffic data including LSA counts:

- **show ipv6 ospf traffic**

Use the following command to display EIGRP traffic data:

- **show ip eigrp traffic** [*as-number]*

The following command is not supported, but may be useful in debugging EIGRP MANET metric issues:

- **debug eigrp neighbor**

Use the following command to collect data when reporting ROMMON issues:

- **showmon**

Complete the following procedure to collect data if a router reboot to rommon occurs:

1. **dir flash:** - Use to locate the Route Processor (crashinfo*) or Network Processor (pxf_crashinfo*) exception file.
2. E-mail the exception file with a write up to the Cisco Beta support email address.

Recommended Configuration Settings

Use the following configuration guidelines when enabling class-based weighted fair-queuing:

- Enter the following command to turn off creation of virtual-template subinterfaces:

```
no virtual-template subinterface
```

- Enter the following commands to create a policy map with class-based weighted fair-queuing and apply the newly created policy-map to the virtual template:

```
 class-map match-any chat
  match  dscp af11
 class-map match-any voice
  match  dscp ef

 policy-map mypolicy
  class chat
   bandwidth percent 40
  class voice
   bandwidth percent 40

interface virtual-template number
service-policy output mypolicy
```

- No additional configuration is supported on the policy-map.

Use the following configuration guidelines when disabling PPP keepalives:

- You can turn off the PPP keepalive messages to decrease overhead when the radio alerts the router with a PADT message that the layer-2 RF connection is no longer available. Turning off the PPP keepalive messages may also avoid the potential for the router to terminate the connection based on missed PPP keepalives over a poor RF link.

- To turn off the PPP keepalive messagess, enter the following command for the virtual-template.

```
interface virtual-template number
no keepalive
```

Use the following configuration guidelines for setting the recommended OSPF values of radio link metrics:

- You may have to dampen the amount of changes in order to reduce network-wide churn because cost components may change rapidly.
- The following recommended values are intended as a starting point for optimizing a OSPFv3 network and are based on network simulations that may reduce the rate of network changes. Each network may have unique characteristics that require different settings to optimize actual network performance.

  You must configure these values for both OSPFv3 IPv4 and IPv6

  S1 = ipv6 ospf dynamic weight throughout
  Recommended value = 0
  Default=100
  S2 = ipv6 ospf dynamic weight resources
  Recommended value = 29
  Default = 100
  S3 = ipv6 ospf dynamic weight latency
  Recommended value = 29
  Default = 100
  S4 = ipv6 ospf dynamic weight L2 factor
  Recommended value = 29
  Default = 100

  The following is an example configuration for a VMI interface or on the virtual template when running bypass mode:

  ```
  interface vmi1
  …
  ipv6 ospf cost dynamic weight throughput 0
  ipv6 ospf cost dynamic weight resources 29
  ipv6 ospf cost dynamic weight latency 29
  ipv6 ospf cost dynamic weight L2-factor 29
  …
  ospfv3 instance 64 cost dynamic weight throughput 0
  ospfv3 instance 64 cost dynamic weight resources 29
  ospfv3 instance 64 cost dynamic weight latency 29
  ospfv3 instance 64 cost dynamic weight L2-factor 29
  ```

For more information on OSPF commands, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_book.html

Use the following configuration guidelines for disabling split horizon in EIGRP:

- By default split horizon is enabled in EIGRP. You can disable split horizon by entering the **no ip split-horizon eigrp** command for the respective autonomous system number.

  ```
  interface vmi number
  no ip split-horizon eigrp as-number
  ```

- Enter the following command to disable the ip redirects on the vmi interface when you are configuring the vmi interface for EIGRP.

  ```
  interface vmi number
  no ip redirects
  ```

Use the following configuration guidelines for setting EIGRP values of radio link metrics:

- EIGRP monitors the following metrics on an interface allowing the tuning of the EIGRP metric calculations; use the metric weights router configuration command:

  ```
  metric weights tos k1 k2 k3 k4 k5
  ```

  where `tos` denotes type of service (currently, it must always be zero) and use the following default values for weights:

  k1 - 1

  k2 - 0

  k3 - 1

  k4 - 0

  k5 - 0

  Note The **no metric weights** command restores the K-values to the above listed defaults:

- Most configurations use the Delay and Bandwidth metrics with Bandwidth taking precedence.
- You must set the weights identically on all routers in an autonomous system.

  Note If you wish to use the default k-values you do not need to enter the **metric weights** command.

- To set the metric dampening value for EIGRP, enter the following commands for either change-based or interval-based dampening of metric updates received through VMI:
  - Change Based Dampening:

    ```
    ip50-1(config)#int vmi 4
      ip50-1(config-if)#eigrp 100 interface dampening-change 40
    ```

    Default Value for Change Based Dampening: 50%

    To enable change-based dampening using the default Value, enter the following command:

    ```
    eigrp 100 interface dampening-change
    ```

    To disable change-based dampening, enter the following command:

    ```
    no eigrp 100 interface dampening-change
    ```

  - Interval-based Dampening:

    ```
    ip50-1(config)#int vmi 4
    ip50-1(config-if)#eigrp 100 interface dampening-interval 20
    ```

    Default Timer value for Interval-based Dampening: 30 seconds

    To enable interval-based dampening using the default Value, enter the following command:

    ```
    eigrp 100 interface dampening-interval
    ```

    To disable interval-based dampening, enter the following command:

    ```
    no eigrp 100 interface dampening-interval
    ```

- The following exceptions will result in an immediate update:
  - a down interface
  - a down route
  - any change in a metric triggered outside the scope of the VMI metric update.

Note No recommended values other than default are currently available.

For more information on EIGRP commands, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_book.html

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

This section lists caveats in the Cisco IOS Release 12.4(24) images:

Open Caveats for Cisco IOS Release 12.4(24)GC5

Cisco IOS Release 12.4(24)GC5 has no open caveats.

Closed Caveats for Cisco IOS Release 12.4(24)GC5

This section lists closed caveats in the Cisco IOS Release 12.4(24)GC5:

- CSCua68693

  When the composite link cost changes due to changes reported by the Cisco 3250 MAR radio, OSPFv3 sends out LSA updates with the changed cost even though the cost is still within the defined hysteresis threshold.

  Workaround: There is no workaround.

- CSCtc42278

  The following error message is seen for incoming ISDN calls:
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error

  This symptom is observed on a Cisco AS5400XM with ISDN configured. This issue also occurs on Cisco IOS Releases 12.4T, 15.0M&T, 15.1M&T.

  Workaround: There is no workaround.

- CSCta33320

  This only happens after a reload of the router. Once the router is reloaded, do an SNMP query of:

  .1.3.6.1.4.1.9.9.44.1.1.1.1 (ciscoICsuDsuStaticConfigEntry) in CISCO-ICSUDSU-MIB,

  the following will be seen in the **show log** command output:

  *Jun 23 14:29:31.863: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x405A6664, -Traceback= 0x4175EC50 0x41781B94 0x417A7A30 0x405A6664 0x405A3CB4 0x405A2DA8 0x42D88260 0x42D8D5B0 0x42D7B7DC 0x42DA9838 0x42F8292C 0x42F82910

  *Jun 23 14:29:31.867: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= 0x405A6670, -Traceback= 0x4175EC50 0x41781B94 0x417A78BC 0x405A6670 0x405A3CB4 0x405A2DA8 0x42D88260 0x42D8D5B0 0x42D7B7DC 0x42DA9838 0x42F8292C 0x42F82910

  Subsequent SNMP queries will not see the above traceback until another reload.

  The issue is seen on Cisco 2821 with VWIC2-1MFT-G703 and HWIC-1CE1T1-PRI running 12.4(20)T1 and 12.4(22)T1 and the latest 12.4(24)T. Other models and IOS versions may also be affected.

  Workaround: There is no workaround.

- CSCte41827

  Device configured with SSLVPN crashes. Device configured with SSLVPN and the **functions svc-enabled** or **functions svc-required** commands, and has an outbound ACL on one of the devices interface.

  This vulnerability has only been observed when the outbound ACL is tied to either a NAT or ZBFW interface in the outbound direction and is not the interface that the SSLVPN session is terminated against.

  This vulnerability has only been observed when the SSLVPN sessions terminate over PPP over ATM interface.

  This vulnerability was not able to be reproduced over SSLVPN sessions terminating over Ethernet or Serial interfaces.

  Workaround: Remove outbound ACL.

- 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

  There are no workarounds that mitigate these vulnerabilities.

  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

- 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
- CSCtj09179

  Cisco IOS Software memory usage may grow over time. Session Initiation Protocol (SIP) trunks are configured and in use and the device running Cisco IOS Software receives a crafted SIP message during an existing subscription.

  Workaround: If SIP operation is not needed then disabling SIP functionality will prevent this issue.
- 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
- 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
- CSCtj48387

  After a few days of operation, a Cisco ASR router running as an LNS box, crashes with DHCP related errors. This symptom occurs when DHCP enabled and sessions get DHCP information from a RADIUS server.

  Workaround: There is no workaround.

- 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

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  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-20120926-dhcpv6

- CSCto72927

  Configuring an event manager policy may cause a Cisco Router to stop responding. This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCto80566

  Device will crash and reload when trying to configure an IPv6 CGA modifier with a 4096-bit RSA keypair. When trying to configure an IPv6 CGA modified by using the **ipv6 cga modifier** command, the device will crash and reload if the referenced RSA keypair is 4096 bits. No other special conditions required.

  Workaround: There is no workaround.

- 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

  There are no workarounds that mitigate these vulnerabilities.

  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

- 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

- 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

- CSCtr86328

  A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.Cisco IOS device configured for clientless SSL VPN.

  Workaround: There is no workaround.

- 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

- 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

- 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

Open Caveats for Cisco IOS Release 12.4(24)GC4

This section lists open caveats in the Cisco IOS Release 12.4(24)GC4:

- CSCua68693

  When the composite link cost changes due to changes reported by the radio on a Cisco 3250 MAR, OSPFv3 sends out LSA updates with the changed cost even though the cost is still within the defined hysteresis threshold.

  Workaround: There is no workaround.

Closed Caveats for Cisco IOS Release 12.4(24)GC4

This section lists closed caveats in the Cisco IOS Release 12.4(24)GC4:

- CSCtb29889

  OSPFv3 may get stuck in the Database Exchange state, which prevents routing updates from being propagated. The problem will only occur with large OSPFv3 LSA databases.

  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://www.cisco.com/warp/public/707/cisco-sa-20110928-sip.shtml.

- 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://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6.shtml.

- CSCth43582
- QoS policy may be dropped on an interface when it receives an invalid CDR value.

  Workaround: There is no workaround.
- CSCti56177
- A Cisco 3250 router running the c3250-adventerprisek9-mz.124-24.GC2 image has a parser error for all IPv6 commands.

  Workaround: Do not use the ?. enter the complete command.
- CSCtk57597

  If 40 OSPF MANET modes all attempt to come up at the same time, the router runs out of memory and may cause a crash in PPPoE.

  Workaround: There is no workaround.
- CSCtl20508

  A Cisco 3270 router may fail to decrypt a packet coming through a tunnel interface with a crypto IPSEC profile. and display the following system message for all received packets:

  ```
  %sys-2-IPSEC(epa_des_crypt): decrypted packet failed SA identity check.
  ```

  Workaround: There is no workaround.
- CSCto23334

  A Cisco device running Cisco IOS may reload due to a software-forced reload that occurs after the following system message: `%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "PPPoE Flow Control Background"`

  Workaround: There is no workaround.

Open Caveats for Cisco IOS Release 12.4(24)GC3

This section lists open caveats in the Cisco IOS Release 12.4(24)GC3:

- CSCtb29889

  OSPFv3 may get stuck in the Database Exchange state, which prevents routing updates from being propagated. The problem will only occur with large OSPFv3 LSA databases.

  Workaround: There is no workaround.
- CSCth43582
- QoS policy may be dropped on an interface when it receives an invalid CDR value.

  Workaround: There is no workaround.
- CSCti56177
- A Cisco 3250 router running the c3250-adventerprisek9-mz.124-24.GC2 image has a parser error for all IPv6 commands.

  Workaround: Do not use the ?. enter the complete command.
- CSCtk57597

  If 40 OSPF MANET modes all attempt to come up at the same time, the router runs out of memory and may cause a crash in PPPoE.

  Workaround: There is no workaround.

- CSCtl20508

  A Cisco 3270 router may fail to decrypt a packet coming through a tunnel interface with a crypto IPSEC profile. and display the following system message for all received packets: `%sys-2-IPSEC(epa_des_crypt): decrypted packet failed SA identity check.`

  Workaround: There is no workaround.

- CSCto23334

  A Cisco device running Cisco IOS may reload due to a software-forced reload that occurs after the following system message: `%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "PPPoE Flow Control Background"`

  Workaround: There is no workaround.

- CSCua68693

  When the composite link cost changes due to changes reported by the Cisco 3250 MAR radio, OSPFv3 sends out LSA updates with the changed cost even though the cost is still within the defined hysteresis threshold.

  Workaround: There is no workaround.

Closed Caveats for Cisco IOS Release 12.4(24)GC3

This section lists closed caveats in the Cisco IOS Release 12.4(24)GC3:

- CSCtb36964

  Use of the **show ospfv3 neighbor manet** or **show ipv6 ospf neighbor manet** commands may cause the router to suffer an unexpected system reload.

  If the **show ospfv3 neighbor manet** or the **show ipv6 ospf neighbor manet** command is entered, with the console at the `--More--` prompt, and a VMI session terminates at the same time, the router will reboot.

  Workaround:

  – Disable the IOS `automore` feature with the following exec-level command to prevent the router reboot from occurring when the above conditions are present:

    ```
    terminal length 0
    ```

Open Caveats for Cisco IOS Release 12.4(24)GC2

This section lists open caveats in the Cisco IOS Release 12.4(24)GC2:

- CSCtb29889

  OSPFv3 may get stuck in the Database Exchange state, which prevents routing updates from being propagated. The problem will only occur with large OSPFv3 LSA databases.

  Workaround: There is no workaround.

- CSCtb36964

  Use of the **show ospfv3 neighbor manet** or **show ipv6 ospf neighbor manet** commands may cause the router to suffer an unexpected system reload.

  If the **show ospfv3 neighbor manet** or the **show ipv6 ospf neighbor manet** command is entered, with the console at the `--More--` prompt, and a VMI session terminates at the same time, the router will reboot.

  Workaround:

  - Disable the IOS `automore` feature with the following exec-level command to prevent the router reboot from occurring when the above conditions are present:

    ```
    terminal length 0
    ```

- CSCth43582

  QoS policy may be dropped on an interface when it receives an invalid CDR value.

  Workaround: There is no workaround.

- CSCti56177

  A Cisco 3250 router running the c3250-adventerprisek9-mz.124-24.GC2 image has a parser error for all IPv6 commands.

  Workaround: Do not use the ?. enter the complete command.

- CSCtk57597

  If 40 OSPF MANET modes all attempt to come up at the same time, the router runs out of memory and may cause a crash in PPPoE.

  Workaround: There is no workaround.

- CSCtl20508

  A Cisco 3270 router may fail to decrypt a packet coming through a tunnel interface with a crypto IPSEC profile. and display the following system message for all received packets:

  ```
  %sys-2-IPSEC(epa_des_crypt): decrypted packet failed SA identity check.
  ```

  Workaround: There is no workaround.

- CSCto23334

  A Cisco device running Cisco IOS may reload due to a software-forced reload that occurs after the following system message: `%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "PPPoE Flow Control Background"`

  Workaround: There is no workaround.

- CSCua68693

  When the composite link cost changes due to changes reported by the Cisco 3250 MAR radio, OSPFv3 sends out LSA updates with the changed cost even though the cost is still within the defined hysteresis threshold.

  Workaround: There is no workaround.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at the following URL:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.