Release Notes for Cisco IOS Release 12.4(24)GC4

Current Release:
12.4(24)GC4 - September 1, 2011

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

The following release notes support Cisco IOS Release 12.4(24)GC4. 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)GC4.

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)GC4

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)GC3, page 8
- Closed Caveats for Cisco IOS Release 12.4(24)GC3, page 9

- Open Caveats for Cisco IOS Release 12.4(24)GC3, page 8
- Closed Caveats for Cisco IOS Release 12.4(24)GC3, page 9

- Open Caveats for Cisco IOS Release 12.4(24)GC2, page 9

Open Caveats for Cisco IOS Release 12.4(24)GC4

Cisco IOS Release 12.4(24)GC4 has no open caveats.

Closed Caveats for Cisco IOS Release 12.4(24)GC4

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

- 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.

- 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 parcer error for all IPv6 commands.

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

- CSCtk57597

  If 40 OSPF MANET nmodes 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 forrowing 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 parcer error for all IPv6 commands.

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

- CSCtk57597

  If 40 OSPF MANET nmodes 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 forrowing system message: `%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "PPPoE Flow Control Background"`

  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 parcer error for all IPv6 commands.

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

  If 40 OSPF MANET nmodes 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 forrowing system message: `%SYS-2-INTSCHED: 'may_suspend' at level 3 -Process= "PPPoE Flow Control Background"`

  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.