Release Notes for Cisco IOS Release 15.1(4)GC and Later

Current Release: 15.1(4)GC1 January 16, 2013
Previous Releases:
15.1(2)GC2 February 9, 2012

The following release notes support Cisco IOS Release 15.1(4)GC. 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 Information and Supported Platforms

These images are bug compatible with Cisco IOS release 15.1(4)M5.

Cisco IOS Release 15.1(4)GC includes the following Cisco IOS images:

- c1861-adventerprisek9-mz
- c1861-advipservicesk9-mz
- c2800nm-adventerprisek9-mz
- c2800nm-advipservicesk9-mz
- c2801-adventerprisek9-mz
- c2801-advipservicesk9-mz
- c2900-universalk9-mz.SPA
- c2951-universalk9-mz.SPA
- c3825-adventerprisek9-mz
- c3825-advipservicesk9-mz
- c3845-adventerprisek9-mz
- c3845-advipservicesk9-mz
- c3900-universalk9-mz.SPA
- c3900e-universalk9-mz.SPA
- c5940-adventerprisek9-mz.SPA

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

Cisco IOS Release 15.1(4)GC is supported on the following platforms:

- Cisco 1861 Integrated Services Router
- Cisco 2801 Integrated Services Router
- Cisco 2811 Integrated Services Router
- Cisco 2901 Integrated Services Router
- Cisco 2911 Integrated Services Router
- Cisco 2921 Integrated Services Router
- Cisco 2951 Integrated Services Router
- Cisco 3825 IP RAN Integrated Services Router
- Cisco 3825 Integrated Services Router
- Cisco 3845 Integrated Services Router
- Cisco 3845 RAN-O Integrated Services Router
- Cisco 3925 Integrated Services Router
- Cisco 3945 Integrated Services Router
- Cisco 5940 Embedded Services Router

Related Documentation

The following documentation is available for use:

- *Software Configuration Guide, Cisco IOS Release 15.1(2)GC* (OL-23478-01)
- *Mobile Ad Hoc Networks for Router-to-Radio Communications* (OL-19437-02)
- Software documentation for Cisco IOS Release 15.1(4)M5

New and Changed Information

This section contains the following information.

New Features for Cisco IOS 15.1(4)GC

: 15.1(4)GC supports all features supported in 15.1(4)M as well as all features supported in 15.1(2)GC. Refer to the following URL for information on the new software features added to Release 15.1M:
http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151-4MNEWF.html

New Hardware Features for Cisco IOS 15.1(2)GC

The following new hardware is supported in 15.1(2)GC:

- Cisco 5940 Embedded Services Router

  For detailed information, refer to the following document:

  Cisco 5940 Embedded Services Router Hardware Technical Reference Guide (OL-23875-01)

New Software Features for Cisco IOS 15.1(2)GC

Cisco IOS Release 15.1(2)GC is based on Cisco IOS Release 15.1T. Refer to the following URL for information on the new software features added to Release 15.1T:
http://www.cisco.com/en/US/docs/ios/15_1/release/notes/15_1m_and_t.html

The following new software feature has been added to this release:

- Router-Radio Control Protocol (R2CP)—R2CP provides a bi-directional, event driven communication channel between the router and the modem. Event driven communication reduces convergence time and decreases the overhead traffic that must be sent to the radio link. R2CP allows real-time link quality metrics on a neighbor-by-neighbor basis. R2CP supports Broadcast Multi-Access (BMA) radios that operate in rapidly changing mobile environments.
- Virtual Multipoint Interfaces (VMI) QoS—VMI QoS provides services that map outgoing packets to the appropriate Point-to-Point Protocol over Ethernet (PPPoE) sessions based on the next-hop forwarding address for that packet. The VMI QoS also provides a broadcast service that emulates a set of point-to-point connections as a point-to-multipoint interface with broadcast ability.

- OSPFv3 CLI changes— The CLI for OSPFv3 IPv4 address families and CLI for OSPFv3 for IPv6 have been changed to a common format. The CLI command format from Cisco IOS Release 12.4(24)GC3 and earlier are still supported.

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 (i.e., 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 back pressure 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.
- QoS policy may drop on an interface when the interface receives an invalid CDR value.

  To prevent dropping QoS policy, the current data rate (CDR) is range checked to a floor value of 80kbps and a ceiling value of 154400kbps. If CDR is below the floor value, the QoS rate shaping is set to the floor value. If CDR is above the ceiling value, the QoS rate shaping is set to the ceiling value.

  In addition to defining floor and ceiling bandwidth values, the class bandwidth percentage must also be 10% or greater. If the class bandwidth is configured to a value less than 10% and the CDR value is less than 80kbps, the QoS policy will be removed. (CSCth43582)
- Software Release 15.1(2)GC2 may have OSPFv3 incompatibility issues with software versions 12.4(24)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 ospfv3 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. Email 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 messages, 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.

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

```
interface vmi1
…
ospfv3 4 cost dynamic weight throughput 0
ospfv3 4 cost dynamic weight resources 29
ospfv3 4 cost dynamic weight latency 29
ospfv3 4 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_ospf/command/reference/iro_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 k4 - 0

  k2 - 0 k5 - 0

  k3 - 1

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_eigrp/command/reference/ire_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 closed (resolved).

Open Caveats for Cisco IOS Release 15.1(4)GC1

Cisco IOS Software Release 15.1(4)GC1 has no opened caveats

Closed Caveats for Cisco IOS Release 15.1(4)GC1

This section lists closed caveats in the Cisco IOS Release 15.1(4)GC1.

- 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

- 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

- CSCub55790

  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

  Affected devices that are configured as Smart Install clients are vulnerable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

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

- CSCud32032

  In Cisco IOS releases 15.1(4)GC and higher, if you configure a Zone-Based Policy Firewall (ZFW), the service policies are not attached to the configuration. The following error message is displayed.

  ```
  % Error: Number of filters in the classmap exceeded the Limit. No Policy will be attached.
  Firewall service-policy attachment failed
  ```

Open Caveats for Cisco IOS Release 15.1(4)GC

Cisco IOS Software Release 15.1(4)GC has no opened caveats.

Closed Caveats for Cisco IOS Release 15.1(4)GC

This section lists closed caveats in the Cisco IOS Release 15.1(4)GC. Cisco IOS Release 15.1(4)GC is bug and PSIRT compatible with Release 15.1(4)M5. For more information on Cisco IOS Release 15.1(4)M1, refer to the following URL:
http://www.cisco.com/en/US/docs/ios/15_1/release/notes/151-4MCAVS.html

- CSCtk81703

  When two interfaces are configured with the same IP and same R2CP port number, but one is in a shutdown state, packets may not be processed correctly for R2CP and the session will not establish. This can only occur when one interface is shutdown as two ethernet interfaces on a single router cannot have the same IP address when they are both in a non-shutdown state.

- CSCt083395

  AGigabit Ethernet receive port stops receiving packets when the data rate exceeds 65%.

Open Caveats for Cisco IOS Release 15.1(2)GC2

This section lists open caveats in the Cisco IOS Release 15.1(2)GC2:

- When two interfaces are configured with the same IP and same R2CP port number, but one is in a shutdown state, packets may not be processed correctly for R2CP and the session will not establish. This can only occur when one interface is shutdown as two ethernet interfaces on a single router cannot have the same IP address when they are both in a non-shutdown state.

  Workaround: Disable R2CP on the shutdown interface or use different ports for each R2CP session. (CSCtk81703)

- AGigabit Ethernet receive port stop receiving packets when the data rate exceeds 65%.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command for the interface to restart traffic. (CSCt083395)

Closed Caveats for Cisco IOS Release 15.1(2)GC2

This section lists closed caveats in the Cisco IOS Release 15.1(2)GC2:

- CSCtd66169

  Multicast traffic drops 100% with zone-based firewall configured.

- CSCtt55925

  Multicast and pim and bsr advertisements fails over unnumbered ppp link

  Router running 15.1(2)T1 will reject bsr advertisements over ip unumbered link while router running 12.4(15)T14 will accept them.

- CSCtn84802

  IPv6 Zone Firewall fails to create inspect session for certain addresses.

- CSCto83395

  5940 stops forwarding traffic when the data rate hits about 65% or more of line rate.

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.