



# Release Notes for Cisco IOS Release 15.1(2)GC

---

**Current Release:**  
**15.1(2)GC - January, 21, 2011**

The following release notes support Cisco IOS Release 15.1(2)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:

- [Image Information and Supported Platforms, page 2](#)
- [Related Documentation, page 3](#)
- [New and Changed Information, page 3](#)
- [Limitations, page 4](#)
- [Troubleshooting, page 4](#)
- [Recommended Configuration Settings, page 5](#)
- [Caveats, page 8](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 8](#)



---

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

© 2011 Cisco Systems, Inc. All rights reserved.

# Image Information and Supported Platforms

These images are bug compatible with Cisco IOS release 15.1(2)T.

Cisco IOS Release 15.1(2)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
- c5940-entbase-mz.SPA

**Note**

---

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

---

Cisco IOS Release 15.1(2) 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(2)T

## New and Changed Information

This section contains the following information.

### New Hardware Features

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

- 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

Cisco IOS Release 15.1(2)GC is based on Cisco IOS Release 15.1 T. 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](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. The floor value is 80kbps. The ceiling value is 154400kbps.  
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)GC 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 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. 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 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](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

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\\_eigrp/command/reference/ire\\_book.html](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 resolved.

## Open Caveats for Cisco IOS Release 15.1(2)GC

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

- When two interfaces are configured with the same IP address 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 only occurs when one interface is shutdown because a router does not support two administratively up Ethernet interfaces with the same IP address.

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

## Closed Caveats for Cisco IOS Release 15.1(2)GC

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

- 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>.

## 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.



---

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2011 Cisco Systems, Inc. All rights reserved.