Release Notes for the *Cisco Broadband Wireless Gateway* for Cisco IOS Release 12.4(15)XL5

Cisco IOS Release 12.4(15)XL5 is a special release that is based on Cisco IOS Release12.4, with the addition of enhancements to the Cisco Broadband Wireless Gateway (BWG) feature. The Cisco IOS Release 12.4(15)XL5 is a release optimized for the Cisco BWG feature on the Cisco 7301 Series router, and the Cisco 6500 Catalyst Switch platform with the Cisco SAMI blade.

Revised: 22 May 2009, OL-14680-01

Contents

These release notes include important information and caveats for the Cisco BWG software feature provided in Cisco IOS 12.4(15)XL5 for the Cisco 7301 series router, and the SAMI card on the Cisco 6500 Catalyst Switch platform and 7600 Series Router platform.

Caveats for Cisco IOS Release 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/tsd_products_support_series_home.html

Release notes for Cisco 6500 Family for Release 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_release_notes_list.html

Release notes for the Cisco 7600 Family for Release 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_release_notes_list.html

Release notes for the Cisco 7300 Family for 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_release_notes_list.html

This release note includes the following topics:

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

Introduction

The Cisco BWG functions in the gateway role in WiMax Access Service Network. WiMAX is a standards-based wireless technology that offers high throughput broadband connections over long distances. WiMAX can be used for a number of applications, including “last mile” broadband connections, hotspots and cellular backhaul, fixed and mobile cellular service, and high-speed enterprise connectivity for business.

The Cisco BWG colocates both the Decision and Enforcement Points (DP and EP), and acts as an interface to the Base-stations in each Access Services Network (ASN).

The BWG is the key to the IP mobility scheme. It provides the termination of the mobility function across base-stations and the foreign agent function. The BWG maps the radio bearer to the IP network. It works with the CSN and the policy servers to control policy on behalf of the user. Additionally, it acts as an IP gateway for the IP host function that is located on the Base Station. The BWG brings together IP functions performed for the access network including end-to-end Quality of Service, Mobility and Security.

- Cisco Catalyst 6500 Series Switch platform with a SAMI blade installed—Please refer to the following URLs for installation and configuration information:

  Switch Chassis Installation

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html

  Switch Chassis Module Installation

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Mod_Install_Note/78_15767.html

  Release Notes

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html

- Cisco 7600 Series Router platform with a SAMI blade installed—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

  - The Supervisor module (Sup720-3BXL, SUP IOS Release 12.2(33)) on the 7600 supports IOS-SLB functionality, and is enhanced to support BWG selection capability.
  - A maximum of 8 blades can be supported per chassis.
  - The BWG can coexist with CSG2 and the HA on co-located blades.

- Cisco 7301 Series Router platform—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_installation_and_configuration_guide_book09186a0080134551.html

Note The Load Balancing and Session Redundancy features are not available for the BWG on the Cisco 7301 Series Router platform.

The Supervisor 720 is supported, both in single and redundant mode. For the Supervisor 720, the 3B and 3BXL versions are supported, with the latter recommended and tested.

The Supervisor 32 is not supported in this release.

System Requirements

The following sections list the BWG system requirements.

Memory Requirements

Table 1 shows the memory requirements for the BWG Software Feature Set that supports the Cisco 7301 Series router, and the SAMI card on the Cisco 6500 Catalyst Switch platform, and the Cisco 7600 Series Router platform.

Note The Supervisor 32 is not supported in this release.

Table 1 Memory Requirements for the Cisco 7301 Router and SAMI on the 6500 Catalyst Switch and 7600 Internet Router

Platform	Software Feature Set	Image Name (BWG, SUP, IOS)	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7301 Router	BWG Software Feature Set	BWG Image: c7301-w1is-mz.124-15.XL4.bin	256 MB	512 MB	RAM
Cisco 6500 Catalyst Switch	BWG Software Feature Set	Sup720-3BXL, SUP IOS Release 12.2(33) BWG Image: c7svcsami-w1is-mz.124-15.XL4.bin	256 MB	2GByte	RAM
Cisco 7600 Internet Router	BWG Software Feature Set	Sup720-3BXL, RSP720-3C-GE, and RSP720-3CXL-GE SUP, IOS Release 12.2(33) BWG Image: c7svcsami-w1is-mz.124-15.XL4.bin	256 MB	2GByte	RAM

- Cisco 7600 Series Router platform with a SAMI blade installed—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

  - The Supervisor module (Sup720-3BXL, SUP IOS Release 12.2(33)) on the 7600 supports IOS-SLB functionality, and is enhanced to support BWG selection capability.
  - A maximum of 8 blades can be supported per chassis.

The BWG can co-exist with CSG2 and the HA on co-located blades.

Hardware Supported

Cisco IOS Release 12.4(15)XL5 is optimized for the Cisco BWG feature on the Cisco 7301 Series router, and the SAMI card on the Cisco 6500 Catalyst Switch platform, and Cisco 7600 Series Router platform.

A Hardware-Software Compatibility Matrix is available on Cisco.com for users with Cisco.com login accounts. This matrix allows users to search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is available at the following URL:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Software Compatibility

Cisco IOS Release 12.4(15)XL5 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(15)XL5 supports the same features that are in Cisco IOS Release 12.4, with the addition of the Cisco BWG feature.

Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version** EXEC command.

New Features in Cisco IOS Release 12.4(15)XL5

- AAA attribute - Service State
- Deregistration Reason TLV in Deregistration Request.
- Delay the Attachment Response from BWG

Features Introduced Before Cisco IOS Release 12.4(15)XL4

The following features were introduced and supported on the BWG prior to Cisco IOS Release 12.4(15)XL4:

- Host Based Accounting,
- Mobile to Mobile Traffic Steering**,**
- CAR/AAA Configuration,
- EAP Authentication
- Security Key Exchange
- IP Address Allocation using DHCP
- Service Flow creation and Management
- Qos Support
- User Group Management
- AAA Accounting Start/Stop/Interim
- Un Predictive Handoff
- KeepAlive Support on R6
- Session Redundancy **(Not supported on the Cisco 7301 Series Router)**
- Load Balancing **(Not supported on the Cisco 7301 Series Router)**
- MIB Support

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco BWG feature in Cisco IOS Release 12.4(15)XL:

- The Load Balancing feature is not supported on the Cisco 7301 Series Router platform.
- The Session Redundancy feature is not supported on the Cisco 7301 Series Router platform.
- To avoid issues with high CPU usage, we recommend the following configurations:
  - To reduce the CPU usage during bootup, disable logging to the console terminal by configuring the **no logging console** global configuration command.
  - To ensure that the HSRP interface does not declare itself active until it is ready to process a peers Hello packets, configure the delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100 interface** configuration command under the HRSP interface.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Caveats for Cisco IOS Releases 12.3 can be found on Cisco.com at http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html

The Open Caveats section lists open caveats that apply to the current release and might also apply to previous releases.

The Resolved Caveats section lists caveats resolved in a particular release, which may have been open in previous releases.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on Cisco.com at **Software Center**: **Cisco IOS Software**: **Cisco Bug Toolkit**: **Cisco Bugtool Navigator II**, or at http://www.cisco.com/support/bugtools.

Open Caveats

The following caveats are unresolved in Cisco IOS Release 12.4(15)XL5:

- CSCsz69597—BWG1.4: Spurious Memory Access Observed at “sock_udp_read_ancillary_data”

  Spurious memory access is seen when the *server-address* used in **dhcp server primary** *server-address* configuration under the user group sub-configuration matches the local interface address on the BWG.

  The general guideline when configuring server addresses for the RADIUS server, DHCP server, etc., is to ensure that the addresses do not conflict with the gateway’s local interface addresses.

  Workaround: In order to avoid spurious memory access, the DHCP server address should not match the local interface address on the BWG.

Unresolved Caveats Prior to 12.4(15)XL5

There are no unresolved caveats in Cisco IOS Release 12.4(15)XL3 or IOS Release 12.4(15)XL4.

Unresolved Caveats Prior to 12.4(15)XL1

The following caveats are unresolved in Cisco IOS Release 12.4(15)XL.

- CSCsk77506—SAMI LCP Hangs With ASNGW SR When a Switchover Happens

  When repeated failovers (around 20 times) have been done in short duration (approximately, 4 hours), a processor in the standby card goes to a hung state.

  The problem is seen in the lab after a high number of forced switchovers (~20) in a very short duration. The problem impacts the processor in the standby card.

  In such a state, the following message might be printed.

  “1w3d: %SVCLC-5-SVCLCNTP: Could not update clock on the module 3, rc is -1”

  Workaround: issue the **hw-module module** *slot-num* **reset** command on the standby card.

Resolved Caveats

There are no new resolved caveats in Cisco IOS Release 12.4(15)XL5:

Resolved Caveats Prior to IOS Release 12.4(15)XL5

The following caveats are resolved in Cisco IOS Release 12.4(15)XL4:

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm97220

  Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at the following link
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml

- CSCsu11522

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XL4

There are no resolved caveats in Cisco IOS Release 12.4(15)XL3.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XL3

The following caveats are resolved in Cisco IOS Release 12.4(15)XL2:

- CSCsi22728—Follow Up Hardware Watchdog Events are Ignored

  A hardware watchdog event following a previous hardware watchdog event is ignored. A runaway process error is not captured a second time.

  This issue occurs under the following conditions:

  a. There should be a serious software bug to cause a hardware watchdog failure.
  b. The first hardware watchdog failure should have happened.

  Workaround: reload the entire card when the first hardware watchdog happens.

  This issue is fixed in SAMI3.0 .

- CSCsk71705—Interface Coming Up Even Though the Vlan on the Sup is not Configured For

  SAMI interface does not come up.

  This condition occurs when the particular vlan is not configured on the supervisor using svclc commands.

  Workaround: when using a vlan on a SAMI processor, it is required to configure the following on the supervisor:

  ```
  svclc multiple-vlan-interfaces
  svclc module <slot#> vlan-group <group #s>
  svclc vlan-group <group #> <vlan #s>
  ```

  The fix for this issue is to provide an error message for this condition.

- CSCsl84868—Submodule Status is ‘Other’ after SSO

  After a Supervisor switchover, the output of the **show module** command shows the SAMI sub-module status as “Other”, and prints the following error message to the console.

Error Message `%CAPI-3-INVALID_SUBMODULE: The submodule type for slot slot num is invalid`

This behavior is seen after a RPR+ or SSO switchover of the Supervisor. Only the sub-module status is incorrectly shown as “Other”. The SAMI card continues to function the way it was before the switchover.

Workaround: Ignore the error message, and the sub module status shown, and use the module status in the output of the **show module** command to determine the status of the SAMI card.

Additional information:

```
Supervisor#show module 8
Mod Ports Card Type                                  Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  8    1  SAMI Module (CSG2)                     WS-SVC-SAMI-BB     SAD10210737

Mod MAC addresses                         Hw    Fw           Sw           Status
--- ------------------------------------ ------ ------------ ------------ -------
  8  0030.f275.b53c to 0030.f275.b543   1.1   8.7(0.5-Eng) 12.4(2008010 Ok <--- Use
this

Mod  Sub-Module                  Model               Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  8  SAMI Daughterboard 1        SAMI-DC-BB         SAD110709U5  0.701  Other<---
Ignore this
  8  SAMI Daughterboard 2        SAMI-DC-BB         SAD110709UE  0.701  Other<---
Ignore this

Mod  Online Diag Status
---- -------------------
  8  Pass
```

- CSCso81854

  Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

  To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml.

  This security advisory is being published simultaneously with announcements from other affected organizations.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XL2

There were no new resolved in Cisco IOS Release 12.4(15)XL.

Related Documentation

Except for feature modules, documentation is available in electronic form. Feature modules are available online on Cisco.com.

Use these release notes with these documents:

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

- *Cisco Broadband Wireless Gateway (BWG) Feature in Cisco IOS Release 12.4(15)XL1 User Guide.*
- *Cisco Broadband Wireless Gateway (BWG) Feature in Cisco IOS Release 12.4(15)XL1 Command Reference.*

Platform-Specific Documents

- Cisco Catalyst 6500 Series Switch platform with a SAMI blade installed—Please refer to the following URLs for installation and configuration information:

  Switch Chassis Installation

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html

  Switch Chassis Module Installation

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Mod_Install_Note/78_15767.html

  Release Notes

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html

- Cisco 7600 Series Router platform with a SAMI blade installed—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

  - The Supervisor module (Sup720-3BXL, SUP IOS Release 12.2(33)) on the 7600 supports IOS-SLB functionality, and is enhanced to support BWG selection capability.
  - A maximum of 8 blades can be supported per chassis.
  - The BWG can coexist with CSG2 and the HA on co-located blades.

- Cisco 7301 Series Router platform—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/products/hw/routers/ps352/products_installation_and_configuration_guide_book09186a0080134551.html

Note The Load Balancing and Session Redundancy features are not available for the BWG on the Cisco 7301 Series Router platform.

The Supervisor 720 is supported, both in single and redundant mode. For the Supervisor 720, the 3B and 3BXL versions are supported, with the latter recommended and tested.

The Supervisor 32 is not supported in this release.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.