



Release Notes for the *Cisco Broadband Wireless Gateway 2.1* for Cisco IOS Release 12.4(24)YG1

Published: December 18, 2009

Revised: December 18, 2009, OL-21495-01

Cisco IOS Release 12.4(24)YG1 is a special release that is based on Cisco IOS Release 12.4, with the addition of enhancements to the Cisco Broadband Wireless Gateway (BWG) feature. The Cisco IOS Release 12.4(24)YG1 is a release optimized for the Cisco 7600 Internet router platform with the Cisco SAMI blade.

Contents

These release notes include important information and caveats for the Cisco BWG 2.1 software feature provided in Cisco IOS Release 12.4(24)YG1 for the SAMI card on the Cisco 7600 Series Router platform.

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/ps6441/prod_release_notes_list.html

This release note includes the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [Memory Requirements, page 3](#)
- [Hardware Supported, page 3](#)
- [Software Compatibility, page 3](#)
- [Features Introduced Before Cisco IOS Release 12.4\(24\)YG1, page 4](#)
- [Limitations and Restrictions, page 5](#)



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

- [Caveats, page 6](#)
 - [Open Caveats, page 6](#)
 - [Resolved Caveats, page 7](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 11](#)

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 7600 Series Router platform with a SAMI blade installed— Refer the following URL for installation and configuration information:

http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.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.

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 also supported in this release.

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

http://www.cisco.com/en/US/products/ps6441/tsd_products_support_series_home.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.

System Requirements

The following sections list the BWG system requirements.

- [Memory Requirements](#)
- [Hardware Supported](#)
- [Software Compatibility](#)

Memory Requirements

Table 1 shows the memory requirements for the BWG Software Feature Set is supported on the Cisco SAMI card on the Cisco 7600 Series Router platform.

Table 1 Memory Requirements for the Cisco SAMI on the 7600 Internet Router

Platform	Software Feature Set	Image Name (BWG, SUP, IOS)	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7600 Internet Router	BWG Software Feature Set	SUP 720 3CXL, Sup720-3BXL, RSP720-3C-GE, and RSP720-3CXL-GE SUP, IOS Release 12.2(33) BWG Image: c7svcsami-w1ik9s-mz.124-24.YG1.bin	256 MB	1GByte per PPC	RAM

Hardware Supported

Cisco IOS Release 12.4(24)YG1 is optimized for the Cisco BWG feature on the SAMI card on the 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/hwswwmatrix.cgi>

Software Compatibility

Cisco IOS Release 12.4(24)YG1 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(24)YG1 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.

SUP Backward Compatibility

The BWG Release 2.1 on the Cisco 7600 hardware platform requires SUP software version SRE. However, BWG Release 2.1 will also work with limited features with an earlier SUP software version SRD.

In order to make BWG 2.1 work with an earlier version of SUP-SRD, configure the following hidden CLI at the global configuration mode:

	Command	Purpose
Step 1	<code>router(config)# wimax agw sup-backward-compatible</code>	Specifies that the BWG will work with the SRD Supervisor image.

With SUP-SRD, BWG Release 2.1 will primarily be used for Cisco-R6, PMIP, and other BWG1.x features.



Note

If you use the SUP-SRD image, the following features in BWG Release 2.1 are not supported:

- SLB Stickiness Support
- NWG R6 in SLB-mode.

Features Introduced Before Cisco IOS Release 12.4(24)YG1

The following features were introduced and supported on the BWG prior to Cisco IOS Release 12.4(24)YG1:

- Support for Proxy Mobile IPv4 (PMIPv4)
- AAA-Based Hot-lining (CoA)
- DSCP Marking
- WiMAX NWG Specification (1.2.2) Compliance
- Accounting Start Response
- SLB Stickiness Support
- AAA Packet of Disconnect Message (PoD)
- AAA-based Static IP Address Provisioning
- Lawful Intercept
- Hitless Software Upgrade
- Redundancy DHCP server
- 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
- Load Balancing
- MIB Support
- EAP and PAP authentication
- Host behind Mobile Subscriber
- Subscriber Session Caching
- Maximum host overflow
- Critical Service Flow
- DHCP Release relay-only
- MS Attachment Response delay
- Multiple SLA support
- De-registration reason in de-registration request
- Static host support
- Maintenance mode for user group
- Support for service state AAA attribute

Limitations and Restrictions

The following limitations and restrictions apply to the Cisco BWG feature in Cisco IOS Release 12.4(24)YG1:

- 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 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/ps6441/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(24)YG1:

- CSCsd34855

The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer-overflow condition. This might result in the execution of arbitrary code. On the 13th September 2006, Phenoelit Group posted an advisory containing the following vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759 — VTP version field DoS
- CSCse40078/CSCse47765 — Integer Wrap in VTP revision
- CSCsd34855/CSCei54611 — Buffer Overflow in VTP VLAN name

An advisory on these vulnerabilities is posted at:

<http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

- CSCsz83159

FP emulation library (libgcc_math.c & libgcc_longlong.h) needs to be removed from shr-ukernel.

- CSCtc96608

On single IP applications, LCP fails to reload a SAMI card if the *show gprs gtp pdp all* command is run when two PPCs have crashed simultaneously.

To work around this issue, reload the card explicitly either from SUP or from LCP.

Resolved Caveats

The following caveats are resolved in BWG 2.1 for Cisco IOS Release 12.4(24)YG1:

- CSCtb80526
To avoid IP address conflicts, BWG should verify the host IP address against the interface IP addresses configured in the BWG.
- CSCtc03432
During a CoA(hotlining) transition, BWG fails to send the Session-Continue attribute.
When BWG receives a CoA, an accounting stop and an accounting start message is sent to the AAA server with the Hotline indication attribute. A Session-Continue attribute (as defined in NWG) is not sent. Therefore, the AAA terminates the session after receiving the accounting stop message.
- CSCtc88357
BWG ignores the results of uplink service flow reservation in the path registration response message(PATH_REG_RSP). Therefore, fails to deregister sessions.
When a base station (BS) sends a service-flow (downlink or uplink) reservation result with errors, for ISF or critical flows, the session should be deregistered. Currently, the BWG checks only the downlink service-flow reservation result for errors. As a result, if the uplink service flow reservation result contains errors, and the downlink service flow reservation result does not contain any error, the session is not deregistered.
- CSCtd13909
BWG fails to disable user-group *Subscriber Multi Host* on an SMX modem in a WiMax setup.
- CSCtb50391
The SR-standby BWG crashes while initiating authenticated calls.
When a user-name vendor specific attributes (VSA) is created on Access-Accept from AAA, the attribute synchronization to SR-standby may cause BWG to crash. However, when the SR-standby BWG re-starts, it successfully synchronizes with the SR- active and becomes operational.
- CSCtb60441
BWG fails to set the correct value for account terminate cause parameter in an accounting stop message to AAA. For example, when a session is terminated by a PoD message (Packet of Disconnect Message) from AAA, BWG should set Acct-Terminate-Cause[49]=user-request in an accounting stop message to AAA.
- CSCtb62797
BWG crashes when a large number of Proxy Mobile IP (PMIP) subscribers are cleared from BWG using the following commands:
 - clear wimax agw subscriber all
 - clear wimax agw subscriber user-group name <name>
 - clear wimax agw path <bs-ip>
 To workaround this issue, avoid clearing large number of PMIP subscribers from BWG, and use the R6 Keepalive mechanism for BWG and BS to stay in sync.

- CSCtb93137
User-group names are not consistently case-sensitive in BWG.
For example, when modifying the user-group configuration, the user-group name is case-insensitive. But, when matching the user-realm and user-group during authentication, the user-group name is case-sensitive.
For BWG 2.1 and later, the user-group name is not case sensitive.
- CSCtd48195
While deploying CoA and hotlining, BWG sends malformed accounting packets to the AAA server when the CoA request does not have the hotline-indication attribute.
- CSCtd48626
BWG 2.0 crashes while processing UDP packets in a WiMax environment when the registration request is replayed when the source base station and the target base station are same.
- CSCtd57335
When the base station sends an error in service-flow reservation result for ISF or critical flows, the session should be de-registered. BWG fails to deregister sessions when the uplink service flow fails.
- CSCsv62323
A vulnerability that exists in the Fast Ethernet driver code of UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS and Cisco 1861 routers may cause unexpected CPU errors. This vulnerability might also stop some of these routers from establishing L2TPv3 sessions.
- CSCsz49741
Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.
Cisco has released free software updates that address these vulnerabilities. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-cucme.shtml>
- CSCta00064
When SIP is enabled, IOS device might crash while processing an incoming SIP message.
- CSCta33973
Recent versions of Cisco IOS Software support RFC4893 ("BGP Support for Four-octet AS Number Space") and contain two remote denial of service (DoS) vulnerabilities when handling specific Border Gateway Protocol (BGP) updates.
These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and with BGP routing configured.
The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments that are made up of more than one thousand autonomous systems.
The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger this issue.
Cisco has released free software updates to address these vulnerabilities. This advisory is posted at: <http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>

- CSCta43662
Cisco IOS software crashes and reloads if the device receives a malformed ICMPv6 neighbor solicitation message, when IPV6 is active on one or more interfaces.
- CSCtd40084
After a dynamic PMIP session is established and then closed, active BWG crashes if *service wimax agw* is configured immediately after unconfiguring it.

The following caveats were resolved in Cisco IOS Release 12.4(24)YG:

- CSCsx07114
A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.
- CSCsy54122
A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.
- CSCsy15227
Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>
- CSCsz38104
The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.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>.
- CSCsq24002
Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml>.
- CSCsx70889
Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml>.

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(24)YG User Guide* at the following URL:
http://www.cisco.com/en/US/docs/ios/12_4/12_4y/12_4_24yg/bwg_2_0/feature_guide/124xl5feat.html
- *Cisco Broadband Wireless Gateway (BWG) Feature in Cisco IOS Release 12.4(24)YG Command Reference* at the following URL:
http://www.cisco.com/en/US/docs/ios/12_4/12_4y/12_4_24yg/bwg_2_0/command_ref/bwg2_0_cr.html

Platform-Specific Documents

- 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.

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 also 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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.