Release Notes for the *Cisco Broadband Wireless Gateway* for Cisco IOS Release 12.4(15)XL4

Cisco IOS Release 12.4(15)XL4 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)XL4 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: 3 March 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)XL4 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:

  www.cisco.com/en/US/docs/routers/7300/install_and_upgrade/7301/7301_install_and_config_guide/5418i.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)XL4 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)XL4 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(15)XL4 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 Software Features in Release *12.4(15)XL4*

The following section describes new features and configuration details for Cisco IOS Release 12.4(15)XL4 that were introduced too late to include in the BWG Feature Guide and Command Reference. The material in this section will be added to the current BWG Feature Guide and Command Reference at a later date.

Session Caching Mechanism

Occasionally, air-link glitches occur between the MS and BS and the hosts behind the CPE/MS are lost. During an air-link glitch, the original BS may or may not send out the R6 de-registration on behalf of the CPE. After an air-link glitch, the CPE may re-connect to the same or a different BS. Previously, in either case, the session in the BWG was deleted and recreated, thus losing the session and host information. The Session Caching Mechanism preserves, or caches, the session across the CPE glitches. This feature involves two scenarios:

- The original BS sends an R6 De-registration Request to the BWG during a CPE glitch. In this case, the session in the BWG is pushed into the CACHED state. The original session, along with its hosts, are preserved when the CPE re-enters into the BWG while the session is in CACHED state.
- The CPE re-enters (through a Pre-Attachment Request) the BWG (through the same or a different BS) when the BWG has its session in ready state. In this case, the session is re-initialized without losing the host information, and re-entry is allowed.

Before entering the CACHED state, the accounting for both flows and host is stopped. When an R6 Pre-Attachment Request is received, the CACHED session is restored along with its previous hosts. Host accounting is re-started at this point. Thereafter, the normal procedure is followed to create the pre-defined service flows for the subscriber.

Note If you clear a session using the BWG CLI, it will not go into a CACHED state.

The value of the session cache timer is specified under the **user-group** sub-configuration mode. It can be specified as following:

- The session cache timeout value between 1 second and 259200sec (3 days).
- The sub-option **follow-dhcp-lease** sets the session cache timeout value to the maximum of DHCP lease remaining across all dynamic hosts. This is the default option.

Session_Cache_timeout = MAX (DHCP lease remaining for Dynamic Host [0],
DHCP lease remaining for Dynamic Host [1],
……..
DHCP lease remaining for Dynamic Host [n])

By default, the session caching feature is enabled with **follow-dhcp-lease** option, as described above. The detailed **show-subscriber** command displays the session's CACHED state.

Session Caching is enabled by default. Perform either of the following tasks to enable or disable the session cache feature using the following **user-group** commands:

	Command	Purpose
Step 1	`router(config-gw-ugl)# [no] timeout cache-session [1-259200]`	Specifies the session cache timer in seconds. The range is 1-259200.

Or this option:

Step 1	`router(config-gw-ugl)# timeout cache-session follow-dhcp-lease`	Sets the session cache timeout value to the maximum of the DHCP lease remaining across all dynamic hosts.

Support for 20 Hosts Per Subscriber support

In Cisco BWG Release 1.3, a CPE can now have up to 20 hosts. However, the total number of hosts for the BWG should not exceed 4 times the total of supported subscribers. For the Cisco 7301 platform, the total number of hosts should be less than 20,000 (4 x 5000 CPEs).

Host Mobility Across CPEs

In BWG Release 1.2, users deployed the BWG in what we termed hot spots. Each hot spot had a WiMAX CPE, and the personal hosts/computers moved around the CPE. These hosts were DHCP hosts. When a host moved away from a CPE, it did not perform DHCP RELEASE. The BWG still maintained information regarding the host despite that it had moved, and that information was not deleted from the BWG until the DHCP lease timer expired. Previously, the DHCP lease was set for 3 days. This caused the BWG to reject new hosts because, from the BWG's perspective, the maximum number of hosts had been reached.

This new feature will address the following scenarios:

- The same DHCP host (based on MAC address) moves from CPE1 to CPE2.

  When this happens, the host may not perform DHCP release through CPE1. Therefore, the BWG still remembers the host associated with CPE1. Previously the host from CPE2 was rejected as long as BWG still remembered the host's association with CPE1.

  In this release, the host's association with CPE1 is removed once the BWG detects the same host is entering the network through another CPE2. The same host can have the same or different IP address when it re-enters the network. Additionally, the same host can re-enter the network with the same or different VRF. Using this approach, the MAC address of the hosts must be unique across the entire network.

  One side effect of this feature is that a spoofed host (with its MAC same as a valid one) through a different CPE can disrupt the normal service of a valid host.

- One host kicks out another host with same VRF and IP address

  In this case, host1 is already in the BWG and associated with a CPE. Host2 (with a different MAC from host1) enters the BWG through the same or different CPE. The network (AAA server through its user-realm => user group => VRF, and DHCP server) assigns host2 with the same VRF and IP address. This should not normally occur because the DHCP server should not re-assign an IP address already in use by host1. However, there may be scenarios where the DHCP server may lose its information (such as a non-graceful restart, or a lease accidentally being deleted through an operator error).

  With this new feature functionality, host1 is deleted to avoid network inconsistency and IP routing confusion. And the deleted host cannot get its service back unless it performs the DHCP procedure again.

Per-Subscriber DHCP Host Overflow Mechanism

Before this feature was implemented, control over the number of DHCP hosts per subscriber was rigid. Once the maximum was reached, any subsequent host coming into the subscriber was rejected. This rigid control was not good for busy hot spots. The problem became even more serious when the DHCP lease time was long and the host left the CPE did not perform DHCP Release.

Now that a new host overflow mechanism based on LRU (Least Recently Used) is used to address the issue that the number of hosts occasionally exceeds a CPE's limit (20). When a new host enters into the subscriber, if its max is reached, an LRU host (with a minimum idle time applied here to avoid trashing) is selected, and this host is deleted from the active list into the overflow list to make room for the new subscriber. A host in the overflow list can be promoted into the active list once uplink data or DHCP messages are received from the host.

You can enable the feature and configure the size of the host overflow list through the CLI, and by default it is set to 50. The newly added host is always appended at the tail of the list. If the overflow list is full, the oldest overflow host, which is at the list head, gets deleted for the new subscriber.

Once an LRU host in the active list is pushed into the overflow, accounting is stopped (if enabled) for the host. The downlink host route is also removed so the overflow host will not be able to receive downlink data. In addition, there is no DHCP timer running against the overflow host.

To save memory, an overflow host only saves the information which is absolutely necessary for its later restoration into the active list. As a comparison, an active host takes about 300 bytes of memory whereas an overflow host uses less than 40 bytes. For the Cisco 7301 platform, the maximum extra memory for all overflow hosts is around 5000*4K = 20MB.

When uplink data or DHCP Renew messages are received for a overflow host, the BWG tries to restore the overflow host into the active list. However, the outcome of this effort depends on two facts:

- If the active list has reached its capacity, or
- If the active list is full, can the BWG find another qualified LRU host from the active list? A qualified LRU host should meet the minimum idle requirement.

If the restoration is successful, the host is removed from the overflow list and added to the active list. The DHCP lease timer is restarted for the host's remaining lifetime as if it has been active all the time. In addition, the host route is restored and host accounting is re-started during this process. If restoration to the active list has failed, the host remains in the cached list.

To summarize, a host is removed from the overflow list under two scenarios:

- Successful restoration into the active list.
- Deleted by another subscriber when it becomes the oldest (at the list head), and the list is full. In this case, DHCP Release is sent to the DHCP server. A host deleted from the cached list can no longer send or receive data unless a DHCP procedure is re-initiated by the host.

In a redundant setup, the overflow host list itself is not synced from the active to standby BWG. However, the information for adding and deleting active hosts is dynamically synced. We expect that this info can be used on the standby side to re-construct its overflow host list. When bulk sync is employed, the standby can no longer re-construct its host overflow list because it has lost the history of how the active hosts got into their position.

The BWG's host overflow feature is not visible to either of the DHCP client or DHCP server. This is a new feature, which allows a CPE to "serve" the number of hosts exceeding its active list.

To make an efficient use of available memory, this feature will be provided on per user group basis. The user-group for hotspot-like CPEs should be explicitly enabled for this feature. By default, this feature is not enabled.

To configure the Per-Subscriber DHCP Host Overflow Mechanism, perform the following tasks:

	Command	Purpose
Step 1	`router(usr-grp)#`**`host-overflow`** [**`size`** *`1-100`*] [**`min-idle`** *`1- 60`*]	Enables the DHCP Host Caching feature and configures the size of the cache list (default 50), and the idle timer (default 5). **min-idle** - establishes the criteria to move a subscriber from the active to the overflow list. The **min-idle** prevents the BWG from frequently moving a host from active host list to overflow list. The **min-idle** value represents minutes.

- Once a data packet is received, since there is no MAC address, the match in the array of records will only be based on IP, and we will not be able to differentiate between dynamic host and spoofing static host. A possible effect would be both actual DHCP host and spoofing host keep on sending traffic with the DHCP host renewing the lease while the spoofing host is “taking advantage”. However, there is no change in the existing behavior and this issue exists today. If the the real IP host is attached to the CPE and the spoofed CPE can start using same address with the same CPE.
- If static IP is allowed, and the record of a DHCP host removed from CPE is also removed from the array (overwritten by some other record), when the DHCP host comes back, the first data packet we intercept is going to result in opening a static host (as per existing code since static IP is allowed). If the host never sends a DHCP renewit will be treated as static, and never deleted unless it gets kicked out. However, this is the user’s choice and existing behavior is exactly same
- If host accounting is enabled, the accounting start/atop for the host can be the overhead.
- The memory requirement is higher per session in cases where hot spot CPE usage is higher in the network.

Perform the following tasks to display the overflow host.

Step 1	`router#` **`show wimax agw subscriber internal`** `router#` **`show wimax agw subscriber msid`** *`msid`* **`overflowed-host`**	Displays the overflow host.

User Group-Based Maintenance Mode, Show, and Clearing

Some customers want to clear all users associated with a particular user group to update an AAA attribute. In doing so, they need a user-group level show and clear command. The maintenance mode allows an operator to block any new CPE from entering a particular user group so that the operator can clear all of the subscribers if needed.

Internally, a user group can keep track of its sessions because it maintains a list of session handles. This handle list is now used for show and clearing.

A user group’s maintenance mode is checked against whenever a session is assigned with the user group. Even though a session can be assigned to only one user group at any time, it can come across more than one user group during its entire life time. This is because a non-EAP session is originally assigned to unauthenticated user group and the AAA response can cause BWG to reassign another user group to the session. In this case, the CPE will be rejected if any one of the user groups it has come across has the maintenance mode on.

By default, maintenance mode is disabled. In non-EAP case, every incoming CPE is initially assigned to the unauthenticated user group. Therefore, no new non-EAP CPE can enter the BWG if the maintenance mode is enabled for the unauthenticated user group.

To enable the Maintenance mode feature, perform the following tasks:

	Command	Purpose
Step 1	`router(config-gw-ugl)# service mode maintenance`	Enables the User Group Maintenance mode feature.

Here is a sample configuration:

```
User group domain name unauthenticated
 User-Group overwritten Counter 0
 Service mode operational
 Sessions 2 associated
 IP-GRE Traffic Sent 0 packets, 0 bytes
 IP-GRE Traffic Received 0 packets, 0 bytes
 Eth-GRE Traffic Sent 18 packets, 6138 bytes
 Eth-GRE Traffic Received 18 packets, 10872 bytes
 Ingress Address filtering 0 packets, 0 bytes
 Traffic Received redirected 0 packets, 0 bytes
 Sessions rejected due to service mode not operational 0   // new line
```

Perform the following tasks to display the sessions associated with a user group:

Step 1	router#**show wimax agw user-group name** *user-group-name* [brief] #**show wimax agw user-group any** [**brief**] #**show wimax agw user-group unauthenticated** [**brief**]	Displays the new sessions rejected for the user-group by the BWG during maintenance mode.

To show sessions associated a user group:

```
router#sh wim agw sub user-group name cisco.com br
MSID           Address         Age       Flows Hosts Pkts-Tx    Pkts-Rx
0003.1238.5678 0.0.0.0         000.07.47 1     0     3          3
0003.123A.5678 11.1.0.5        000.02.32 1     0     2          2
0003.123B.5678 11.1.0.6        000.02.00 1     0     2          2
0003.123C.5678 11.1.0.7        000.01.40 1     0     2          2
0003.123D.5678 11.1.0.8        000.01.40 1     0     2          2
0003.123E.5678 11.1.0.9        000.01.40 1     0     2          2
```

Perform the following tasks to clear the sessions:

Step 1	router#**clear wimax agw subscriber user-group name** *group-name* [**local**] router#**clear wimax agw subscriber user-group any** [**local**] router#**clear wimax agw subscriber user-group unauthenticated** [**local**]	Clears sessions associated with a user group.

CLI-based Keepalive With reset-bs Option

Previously, the BS and BWG were occasionally out of sync in terms of sessions. At that time, it appeared that the only way to correct this was to reload the BWG, because a restarted BWG is able to send a keepalive to reset all BSs. However, reloading BWG is considered a drastic operation, which impacts every BS or CPE.

Now, if the BWG gets out of sync with a BS, this feature allows you to reset that specific BS.

To enable the BWG to resync to a specific BS, perform the following tasks:

	Command	Purpose
Step 1	`router#clear wim agw path 10.10.10.10 [reset-bs]` `router#clear wim agw path 10.10.10.10 local [reset-bs]`	Enables the BWG to reset a specific BS.

In the above configuration, 10.10.10.10 is the BS IP address . The **reset-bs** keyword prompts the BWG to clean up all the sessions belonging to the specified BS (if any), but also to send a keep-alive message (with its current reset time) to that BS to indicate that the BWG restarted so that BS is guaranteed to clear its sessions. This special keep-alive will always be sent even if the periodic keep-alive is disabled. Re-transmission is not applied here, so the command can be issued multiple times if needed.

A path for a BS does not exist if there are no subscriber sessions to the BS on the BWG. If this CLI is triggered in absence of a path for a BS then the BWG will not send KA request to BS.

Brief show CLI to Identify a Static or Dynamic Host.

Hackers tend to use static IP to explore the weakness of the network. This requires the BWG to provide a command to list all hosts with static IP addresses.

This feature leverages the existing **show wimax agw sub brief host** command. At the end of each output line a “D” or “S” is added to indicate if it is dynamic or static host.

Here is an example:

```
Router#sh wim agw sub br host
MSID           Index HostID         Address         DwnLk-SFID Idle Time
1000.2223.0001 1     1000.2223.0002 4.4.0.2         1          00:01:54 D
1000.2223.0001 2     ----.----.---- 4.4.0.3         3          00:00:18 S
```

In the Host Caching feature previously described in this document, the dynamic host is identified with “Idle Time” of “*xxx*”. This is no longer the case as the dynamic host also needs to remember its idle time for the LRU algorithm.

Enable DHCP RELEASE Relay-only

Prior to BWG Release 1.3, the BWG pro-actively performed a DHCP RELEASE to the DHCP server for a subscriber’s DHCP hosts when the subscriber’s session was deleted. With this new feature enabled, the BWG will only handle relayed DHCP RELEASEs from DHCP clients. In other words, the BWG will no longer generate a DHCP RELEASE on behalf of subscriber’s hosts. When the command is not configured, the feature is disabled. In this case, the existing behavior is still preserved.

To enable this feature, perform this task using the following **user group** command:

	Command	Purpose
Step 1	`router(config-gw-ugl)# dhcp release relay-only`	Enables the BWG to handle relay-only DHCP RELEASEs.

Critical Service Flow

Under certain circumstances, one or more secondary flows fail to be created, yet the subscriber session stays up with fewer flows than the subscribers needs. In this situation, the session should be deregistered, so that it can be re-created with all critical flows that the subscriber needs. For example, a customer may want a subscriber to either have all flows (voice, video, and data), or nothing at all. This feature allows a Service Flow(SF) to be marked as critical for the subscriber. The BWG will successfully create subscriber session if and only if every SF marked "Critical" is created.

The BWG allows you to mark a SF as critical while adding it under SLA profile configuration. If the SF is marked critical, then session will fail to open if such critical SF fails to create. The key point is that every critical flow must be created successfully for a session to open. If a SF is not marked to be critical, or if it is ISF, then there is no change in existing behavior.

During Controlled Handover, if the Target-BS fails to include critical flow(s), then the BWG will fail the Handover. The point is to ensure that the "all or none flow(s)" philosophy gets applied to a subscriber all the time.

By default, a SF is not critical, unless specified as "critical" in a SLA-profile.

To configure the BWG to mark service flows as critical, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)#`**`wimax agw sla profile`** *`bronze`* `Router(config-gw-sla)#`**`service-flow pre-defined secondary`** `2` **`profile`** `sec2 critical`	Enables the BWG to mark service flows as "critical" under an SLA profile.

In a SR setup, you must have identical SF-critical configurations on the active and standby BWGs.

The flow details in **show wimax agw subscriber** will indicate if a flow is critical or not.

Here is an example:

```
Router#sh wim agw subs msid <>

MSID 1000.22BA.0001
 CPE is nomadic
 Static IP addresses not permitted
 Subscriber Age 000:00:23
 Base Station ID 0x0A01194B00
....
…
    Flow details Secondary(2)(Critical)
     SF Profile name sec2
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8003(32771)
     Data ID local 0x3(3), remote 0xD(13)
     Data address local 11.1.25.2, remote 10.1.25.75
     Data traffic sent 0 packets, 0 bytes
     Data traffic received 0 packets, 0 bytes
     Accounting disabled
     Idle for inbound 00:00:31, outbound 00:00:31
     Service Flow information Downlink:
      Identifier 5
      Set DSCP (DDS) 30
      QoS information:
       Data-delivery-service real-time-variable-rate
       Minimum traffic-rate-reserved 0, Maximum latency 0
       Unsolicited interval-polling 0, Traffic-priority 0
       Maximum traffic-rate-sustained 0, Request/Transmission-policy 0
       Maximum traffic-burst-rate 0
       Reduced-resources-code 0
```

```
 Media-flow-type 05abcd
Classifier information:
 priority 2
  ethernet permit any 1000.2223.0003 FFFF.FFFF.FFFF any
CS Type information:
 Ethernet CS
```

Support for Jumbo Frames

This feature allows the BWG to support jumbo frames of up to 2000 bytes in payload. Previously, 1500 bytes was the limit beyond which packets are fragmented. The feature raises the Maximum Transfer Unit (MTU) to 2000.

- The mtu has been set for the BWG application to 2000. Configuration in the virtual-template interface allows the change in configuration for mtu, but what is reflected in the virtual-access interfaces is 2000 for BWG.
- The default mtu and ip mtu are respectively 2000 and 1500 in the Virtual-Template interface. So if neither are configured at BWG boot time, the configuration for the virtual-template interface in the running-config will look like the following:

```
Router#sh run | sec Virt
interface Virtual-Template1
 mtu 2000
 ip address 3.3.3.3 255.255.255.0
 ip mtu 1500
 encapsulation agw
```

- Once mtu is configured, ip mtu can be configured to any value less or equal to the mtu and will be reflected dynamically in the virtual-access interface.
- A **no ip mtu** will set **ip mtu** in the virtual-access interface to mtu (2000). Any other desired value for **ip mtu** has to be explicitly configured in the virtual-template interface.

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

There are no unresolved caveats in Cisco IOS Release 12.4(15)XL4:

Unresolved Caveats Prior to 12.4(15)XL4

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

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

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

- CSCsh97579

  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.

- 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

- CSCsq31776

  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.

- 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.

- 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.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.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.

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:

  www.cisco.com/en/US/docs/routers/7300/install_and_upgrade/7301/7301_install_and_config_guide/5418i.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.