Cisco Broadband Wireless Gateway 2.2 Command Reference, IOS Release 12.4(24)YG2

09 April 2010

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level* | **dot1x**} {**default** | *list-name*} [**vrf** *vrf-name*] {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Protocols (NCPs), and AppleTalk Remote Access Protocol (ARAP).
exec	Runs accounting for the EXEC shell session. This keyword returns user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler and disassembler (PAD), and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
dot1x	Provides information about all IEEE 802.1x-related user events.
default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the following accounting methods: • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. • **group tacacs+**—Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command. • **group** *group-name*—Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. VRF is used *only* with system accounting.

start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the accounting server received the "start" accounting notice.
stop-only	Sends a "stop" accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group.

Defaults

AAA accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was introduced on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	The **auth-proxy** keyword was added.
12.2(1)DX	The **vrf** keyword and *vrf-name* argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(15)B	The tunnel and tunnel-link accounting methods were introduced.
12.3(4)T	The tunnel and tunnel-link accounting methods were integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **dot1x** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS release 12.(33)SXH.

Usage Guidelines

General Information

Use the **aaa accounting** command to enable accounting and to create named method lists that define specific accounting methods on a per-line or per-interface basis.

Table 6 contains descriptions of keywords for AAA accounting methods.

Table 6 aaa accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name* argument.

In Table 6, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering values for the *list-name* argument where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and method list keywords to identify the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Note System accounting does not use named accounting lists; you can define the default list only for system accounting.

For minimal accounting, include the **stop-only** keyword to send a “stop” record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a “start” accounting notice at the beginning of the requested process and a “stop” accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

To specify an accounting configuration for a particular VRF, specify a default system accounting method list, and use the **vrf** keyword and *vrf-name* argument. System accounting does not have knowledge of VRF unless specified.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes,

see the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, see the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note This command cannot be used with TACACS or extended TACACS.

Cisco Service Selection Gateway Broadcast Accounting

To configure Cisco Service Selection Gateway (SSG) broadcast accounting, use ssg_broadcast_accounting for the *list-name* argument. For more information about configuring SSG, see the chapter "Configuring Accounting for SSG" in the *Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4.

Layer 2 LAN Switch Port

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of "Update/Watchdog packets from this AAA client" in your RADIUS server Network Configuration tab. Next, enable "CVS RADIUS Accounting" in your RADIUS server System Configuration tab.

You must enable AAA before you can enter the **aaa accounting** command. To enable AAA and 802.1X (port-based authentication), use the following global configuration mode commands:

- **aaa new-model**
- **aaa authentication dot1x default group radius**
- **dot1x system-auth-control**

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a start-stop restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

The following example defines a default system accounting method list, where accounting services are provided by RADIUS security server "server1" with a start-stop restriction. The **aaa accounting** command specifies accounting for vrf "vrf1."

```
aaa accounting system default vrf1 water start-stop group server1
```

The following example defines a default IEEE 802.1x accounting method list, where accounting services are provided by a RADIUS server. The **aaa accounting** command activates IEEE 802.1x accounting.

```
aaa new model
aaa authentication dot1x default group radius
aaa authorization dot1x default group radius
```

```
aaa accounting dot1x default start-stop group radius
```

The following example shows how to enable network accounting and send tunnel and tunnel-link accounting records to the RADIUS server. (Tunnel-Reject and Tunnel-Link-Reject accounting records are automatically sent if either start or stop records are configured.)

```
aaa accounting network tunnel start-stop group radius
aaa accounting network session start-stop group radius
```

The following example shows how to enable IEEE 802.1x accounting:

```
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
dot1x system-auth-control	Enables port-based authentication.
radius-server host	Specifies a RADIUS server host.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting (wimax agw user group-list submode)

To enable various flows on the BWG, use the **aaa accounting** command in wimax user group-list submode. Use the **no** form of this command to disable the various flows.

aaa accounting [start | flow {start [include-framed-ip [*delay*]]} **| host | method-list | update [handover]]**

no aaa accounting [start | flow {start [include-framed-ip [*delay*]]} **| host | method-list | update [handover]]**

Syntax Description

start	Starts accounting for flow and host.
flow	(Optional) Enables user group AAA accounting flow commands
start	Configures accounting start per flow.
include-framed-ip	Includes the Framed-IP-Address to the accounting start record for the flow-accounting.
delay	Enables a delay of one second to 20 seconds before sending an accounting start record. Default value is 3 seconds.
host	(Optional) Enables user group AAA accounting host commands.
update	Enables user group AAA accounting update commands.
handover	Enables the interim accounting updates during handoffs.

Defaults

The accounting update handover is enabled by default. Sending the Framed-IP-Address field in the accounting start record is disabled by default.

Command Modes

Wimax agw user group-list configuration (config-gw-ug)

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL3	The **host** keyword was added.
12.4(24)YG2	The **start include-framed-ip** and **update handover** keywords were added.

Usage Guidelines

Both flow-based and host-based accounting can be enabled or disabled under the user group. Further, both host and flow modes can be enabled simultaneously.

If host accounting is enabled for a user group, and every time a host (default host is known as the CPE, DHCP host behind the CPE is known as a Static Host) gets created on BWG, BWG initiates accounting by sending an Accounting Start request to the RADIUS server. An accounting stop request is sent if the session gets de-registered or the host gets deleted.

Framed-IP is often not included in the accounting start record for flow-accounting. In case of the initial service flow, the accounting start record is sent at the time of flow creation much before the subscriber host is created. From BWG release 2.2, you can delay the sending of the accounting start record until a host is created.

Examples

Here is a configuration and usage example of the **aaa accounting host** command:

```
router(config)#wimax agw user group-list wimax
router(config-gw-ugl)#user-group domain cisco2.com
router(config-gw-ug)#aaa accounting ?
  flow         User group AAA accounting flow commands
  host         User group AAA accounting host commands
  method-list  User group AAA accounting method list configuration commands

router(config-gw-ug)#aaa accounting host ?
  enable  Enable User group AAA accounting per host

router(config-gw-ug)#aaa accounting host enable

user-group domain cisco2.com
  aaa accounting method-list agw
  sla profile-name gold
  ip static-allowed
  security subscriber address-filtering ingress
  subscriber network-behind
  aaa accounting host enable
 !
```

The following example shows how to enable the framed IP delay feature with the default delay of 3 seconds:

```
router(config-gw-ug)#aaa accounting flow start include-framed-ip
```

The following example shows how to enable the framed IP delay feature with the delay of 10 seconds:

```
router(config-gw-ug)#aaa accounting flow start include-framed-ip 10
```

The following example shows how to disable the interim accounting update during handoffs:

```
router(config-gw-ug)#no aaa accounting update handover
```

The following example shows how to include the Framed-IP-Address to the accounting start record:

```
user-group domain eapTls.com
  aaa accounting method-list agw-method_acct_1
  aaa accounting flow start include-framed-ip 20
  aaa accounting host enable
  aaa authentication method-list agw_method_eap-tls_auth_1
  sla profile-name eapTls.com
  dhcp gateway address 20.3.5.50
  dhcp server primary 22.3.5.50
  timeout cache-session 240
  vrf wimax-vrf1
```

aaa accounting start wait-response

To configure the BWG to wait for a response of Accounting Start (both host and flow) from the AAA server, use the **aaa accounting start wait-response** command in User group configuration sub mode. Use the **no** form of the command to disable this feature. If no response is received from the AAA server, the related session is torn down.

aaa accounting start wait-response

no aaa accounting start wait-response

Syntax Description

There are no keyword or arguments for this command.

Defaults

There are no default values.

Command Modes

User group configuration sub mode.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Usage Guidelines

This feature closes a loophole, in that a subscriber will not be able to get a free use of the service when the AAA server is down or not reachable.

Examples

The following example illustrates how to enable the **aaa accounting start wait-response** command:

```
router(config-gw-ug# aaa accounting start wait-response
```

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in global configuration mode. To disable interim accounting updates, use the **no** form of this command.

aaa accounting update [**newinfo**] [**periodic** *number* [**jitter** {**maximum** *max-value*}]]

no aaa accounting update

Syntax Description

newinfo	(Optional) An interim accounting record is sent to the accounting server whenever there is new accounting information to report relating to the user in question.
periodic	(Optional) An interim accounting record is sent to the accounting server periodically, as defined by the *number*.
jitter	(Optional) Allows you to set the maximum jitter value in periodic accounting.
maximum *max-value*	The number of seconds to set for maximum jitter in periodic accounting. The value 0 turns off jitter. Jitter is set to 300 seconds (5 minutes) by default.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	Introduced support for generation of an additional updated interim accounting record that contains all available attributes when a call leg is connected.
12.2(15)T11	The **jitter** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(15)XL	This command was incorporated into Cisco IOS Release 12.4(15)XL.

Usage Guidelines

- When the **aaa accounting update** command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the **newinfo** keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

- When the **gw-accounting aaa** command and the **aaa accounting update newinfo** command and keyword are activated, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators (BCI)) available at the time of call connection are sent through this interim updated accounting record.
- When used with the **periodic** keyword, interim accounting records are sent periodically as defined by the number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.
- When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the number. For example, if you configure the **aaa accounting update newinfo periodic** *number* command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the **newinfo** algorithm.
- Vendor-specific attributes (VSAs) such as h323-connect-time and backward-call-indicator (BCI) are transmitted in the interim update RADIUS message when the **aaa accounting update newinfo** command and keyword are enabled.
- Jitter is used to provide an interval of time between records so that the AAA server does not get overwhelmed by a constant stream of records. If certain applications require that periodic records be sent a exact intervals, you should disable jitter by setting it to 0.

Caution Using the **aaa accounting update periodic** command and keyword can cause heavy congestion when many users are logged into the network.

Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30-minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

The following example sends periodic interim accounting records to the RADIUS server at 30-minute intervals and disables jitter:

```
aaa accounting update newinfo periodic 30 jitter maximum 0
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
gw-accounting aaa	Enables VoIP gateway accounting through the AAA system.

aaa authentication

To specify one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X, use the **aaa authentication dot1x** command in global configuration mode. To disable authentication, use the **no** form of this command

aaa authentication dot1x {**default** | **listname**} *method1* [*method2...*]

no aaa authentication dot1x {**default** | **listname**} *method1* [*method2...*]

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string used to name the list of authentication methods tried when a user logs in.
method1 [*method2...*]	At least one of these keywords: • **enable**—Uses the enable password for authentication. • **group radius**—Uses the list of all RADIUS servers for authentication. • **line**—Uses the line password for authentication. • **local**—Uses the local username database for authentication. • **local-case**—Uses the case-sensitive local username database for authentication. • **none**—Uses no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.

Defaults

No authentication is performed.

Command Types

Global configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet Switch Module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Router support was added for the following platforms: Cisco 1751, Cisco 2610XM – Cisco 2611XM, Cisco 2620XM – Cisco 2621XM, Cisco 2650XM – Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(15)XL	This command was integrated into Cisco IOS Release 12.5(15)YX.

Usage Guidelines

The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly 802.1X-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server. The remaining methods enable AAA to authenticate the client by using locally configured data. For example, the **local** and **local-case** methods use the username and password that are saved in the Cisco IOS configuration file. The **enable** and **line** methods use the **enable** and **line** passwords for authentication.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command. If you are not using a RADIUS server, you can use the **local** or **local-case** methods, which access the local username database to perform authentication. By specifying the **enable** or **line** methods, you can supply the clients with a password to provide access to the switch.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

The **aaa authentication method-list default** indicates if the RADIUS Access Request is to be initiated from the BWG for the unauthenticated group, or not. In the absence of this command under an unauthenticated user group then, the BWG will not send an Access-Request to the AAA and the **proxy realm password**, and **user auto-provisioned** commands will not hold importance.

Examples

The following example shows how to create an authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is allowed access with no authentication:

```
service wimax agw
aaa new-model
!
!
aaa authentication dot1x agw group radius
aaa authorization network default group radius
aaa accounting update periodic 1
aaa accounting network agw start-stop group radius
!
!
aaa session-id unique
clock timezone PST -8
clock calendar-valid
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
identity profile default	Creates an identity profile and enters dot1x profile configuration mode.

Command	Description
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

aaa authentication ppp

To specify one or more authentication, authorization, and accounting (AAA) authentication methods for use on serial interfaces that are running PPP, use the **aaa authentication ppp** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication ppp {**default**}

no aaa authentication ppp {**default**}

Syntax Description

default	Uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.

Defaults

If the **default** list is not set, only the local user database is checked. This has the same effect as that created by the following command:

```
aaa authentication ppp default local
```

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support and **local-case** were added as method keywords. This command was integrated into Cisco IOS Release 12.0(5)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Note The Cisco BWG only supports the **default** setting. If you configure **aaa authentication ppp agw group radius**, the PPP session creation will fail.

The lists that you create with the **aaa authentication ppp** command are used with the **ppp authentication** command. These lists contain up to four authentication methods that are used when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** *list-name method* command, where *list-name* is any character string used to name this list MIS-access. The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 7.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify **none** as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is **none** and no authentication is performed. Use the **more system:running-config** command to display currently configured lists of authentication methods.

Note In Table 7, the **group radius**, **group tacacs+**, and **group** *group-name* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs+-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Table 7 aaa authentication ppp Methods

Keyword	Description
if-needed	Does not authenticate if the user has already been authenticated on a tty line.
krb5	Uses Kerberos 5 for authentication (can be used only for Password Authentication Protocol [PAP] authentication).
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.
cache *group-name*	Uses a cache server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the **aaa group server radius** or **aaa group server tacacs+** command.

Cisco 10000 Series Router

The device supports a maximum of 2,000 AAA method lists. If you configure more than 2,000 AAA method lists, traceback messages appear on the console.

Examples

The following example shows how to create a AAA authentication list called MIS-access for serial lines that use PPP. This authentication first tries to contact a TACACS+ server. If this action returns an error, the user is allowed access with no authentication.

```
aaa authentication ppp MIS-access group tacacs+ none
```

Here is a sample configuration command for PAP authentication on the BWG.

```
!
aaa authentication  ppp default group radius
!
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs+	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
more system:running-config	Displays the contents of the currently running configuration file, the configuration for a specific interface, or map class information.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
tacacs+-server host	Specifies a TACACS host.

aaa pod server

To configure the POD feature on the BWG, use the aaa pod server global configuration command. Use the no form of the command to disable this feature.

aaa pod server [port *port-number*] **[auth-type {any| all | session-key}] server-key** [*encryption-type*] *string*

no aaa pod server [port *port-number*] **[auth-type {any| all | session-key}] server-key** [*encryption-type*] *string*

Syntax Description

port *port-number*	(Optional) The network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700.
auth-type	(Optional) The type of authorization required for disconnecting sessions.
any	Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
all	Only a session that matches all four key attributes is disconnected. All is the default.
session-key	Session with a matching session-key attribute is disconnected. All other attributes are ignored.
server-key	Configures the shared-secret text string.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are **0**, which means that the text immediately following is not encrypted, and **7**, which means that the text is encrypted using an encryption algorithm defined by Cisco.
string	The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Defaults

The default value for the *port-number* is 1700.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

The following example illustrates how to enable the **aaa pod server** command:

```
router(config)# aaa pod server
```

bridge group

To configure a bridge group in the BWG, use the **bridge group** command. Use the **no** form of this command to disable this function.

bridge group [*value*] **{source learning | transparent-vlan [vlan-tag]}**

no bridge group [*value*] **{source learning | transparent-vlan [vlan-tag]}**

Syntax Description

value	Number of the bridge group to which the Wimax user group needs to be added. The range is from 1 to 255.
source learning	Enables source learning.
transparent-vlan	Enables transparent VLAN bridging.
vlan-tag	Enables vlan tagging of the uplink packets from the subscribers associated to the user-group.

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration (config).

Command History

Release	Modification
12.4(24)YG2	This command was introduced.

Usage Guidelines

To enable bridging on a Wimax user group, the user group needs to be added to a bridge group. After the user group is added, a virtual Wimax interface (Wimax<bridge-grp>) is created. This virtual Wimax interface represents the user group in the bridge group. You cannot add Multiple user groups to the same bridge group.

Examples

The following example shows how to configure a bridge group and enable source learning:

```
router(config)#bridge group 23 source learning
```

The following example show how to configure L2-L2 bridging:

```
bridge irb
!
interface Ethernet1/1
  description Interface belong to bridge-group 1
  bridge-group 2
  no bridge-group 2 source-learning
  no ip address
!
bridge 2 protocol ieee
!
wimax agw user group-list wimax
```

```
user-group any
 aaa authentication method-list agw
 aaa accounting method-list agw
 sla profile-name silver
 bridge-group 2
 no bridge-group 2 source-learning
 bridge-group 2 transparent-vlan vlan-tag
```

clear ip slb sticky asn msid

To clear the sticky entry in the BWG sticky database corresponding to the msid specified, use the **clear ip slb sticky asn msid** command in Privileged EXEC mode. Use the no form of the command to disable this function.

clear ip slb sticky asn msid {*macid*}

no clear ip slb sticky asn msid {*macid*}

Syntax Description

macid	Specifies the MSID.

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

The following example illustrates how to enable the **clear ip slb sticky asn msid** command:

```
router# clear ip slb sticky asn msid
```

clear wimax agw path

To clear all the subscribers that belongs to a BS, or to re-sync the sessions with a specific BS, use the **clear wimax agw path** command in privileged EXEC mode. .

clear wimax agw path *bs-ip-addr* [**local**] [**reset-bs**] [**dm-action** [**ms-reset** | **action-code** *0-FFFF*]]

Syntax Description

bs-ip-address	IP address of a specific base station.
local	Clears local sessions on the specified BS.
reset-bs	Prompts the BWG to clean up all the sessions belonging to the specified BS (if any), and 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
dm-action	This option allows the BWG to send a Disconnect-Message action code with subscriber de-registration message.

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL4	The **reset-bs** option was introduced
12.4(24)YG	The **dm-action** option was introduced.

Examples

The following example illustrates how to enable the **clear wimax agw path** command:

```
router#clear wimax agw path 10.10.10.10
router#clear wimax agw path 10.10.10.10 local
router#clear wimax agw path 10.10.10.10 reset-bs
router#clear wimax agw path 10.10.10.10 dm-action ms-reset
router#clear wimax agw path 10.10.10.10 dm-action action-code 0
```

clear wimax agw redundancy statistics

To clear redundancy specific statistics, use the **clear wimax agw redundancy statistics** command in privileged EXEC configuration mode.

clear wimax agw redundancy statistics

Syntax Description

This command has no keywords or arguments.

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

You can use the **clear wimax agw redundancy statistics** command on the standby card without producing a warning message, but the redundancy statistics on the active and standby will not be in sync.

Examples

The following example clears all BWG redundancy statistics:

```
router#clear wimax agw redundancy statistics
```

clear wimax agw statistics

To clear statistics on the BWG, use the **clear wimax agw statistics** command in privileged EXEC configuration mode.

clear wimax agw statistics

Syntax Description

There are no keywords or arguments

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

You can use the **clear wimax agw statistics** command on the standby card without producing a warning message, but the statistics on the active and standby will not be in sync.

Examples

The following example illustrates the clear wimax agw statistics command:

```
router# clear wimax agw statistics
```

clear wimax agw subscriber

To clear the subscriber on the BWG, use the **clear wimax agw subscriber** command in privileged EXEC configuration mode.

clear wimax agw subscriber [msidac-id *mac-id* **] user-group [name** *group-name* **| any | unauthenticated] [local]**

Syntax Description

msid *mac-id*	Specifies the MSID of the subscriber. If the MSID is not specified the entire subscriber list is cleared.
user-group	Clears sessions associated with a user group.
name *group-name*	Specifies the name of the user group.
any	Clears any user group
unauthenticated	Clears only unauthenticated user groups.
local	If the **local** keyword is configured, the subscribers are cleared locally, otherwise de-registration is sent to the base station.

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL4	The **name**, **any**, and **unauthenticated** keywords were added.

Usage Guidelines

Note All **clear wimax** commands are valid only on the SR ACTIVE card.

For example:

```
router#clear wimax agw subscriber all
    This is STANDBY unit. This command must be issued on the ACTIVE unit
```

Examples

The following example clears subscribers locally:

```
clear wimax agw subscriber local
```

cs-type

To specify the cs-type profile under the corresponding direction, use the **cs-type** sub command. The **no** version of the command removes the cs-type information from the corresponding direction. Configuring the command opens a sub configuration mode to configure various cs-type commands.

cs-type {**ethernet-cs** | **ip-cs**}

no cs-type {**ethernet-cs** | **ip-cs**}

Syntax Description

ethernet-cs	Specifies ethernet as the convergence sublayer.
ip-cs	Specifies IP as the convergence sublayer.

Defaults

There are no default values.

Command Modes

Service flow direction configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

Configuring the command opens a sub configuration mode to configure various cs-type commands.

Examples

The following example configures both cs-types:

```
wimax agw service-flow profile isf
 direction downlink
  cs-type ip-cs
   pak-classify-rule isf-classifier-downlink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-downlink
   precedence 2
  qos-info isf-qos-downlink
 !
 direction uplink
  cs-type ip-cs
   pak-classify-rule isf-classifier-uplink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-uplink
   precedence 2
   vlan 2 vrf vrf_1
   vlan range 3 10 vrf vrf_2
   vrf-default vrf_1
  qos-info isf-qos-uplink
```

data-delivery-service

To configure data delivery service associated with certain predefined set of QoS-related service flow parameters, use the **data-delivery-service** command in global configuration mode. Use the **no** form of the command to disable this feature.

data-delivery-service {**unsolicited-grant** | **real-time-variable-rate** | **non-real-time-variable-rate** | **best-effort** | **extended-real-time-variable-rate**}

no data-delivery-service

Syntax Description

unsolicited-grant	Configures the unsolicited grant.
real-time-variable-rate	Cofigures the real time variable rate.
non-real-time-variable-rate	Configures the non-real time variable rate.
best-effort	Configures the best effort.
extended-real-time-variable-rate	Configures the extended real time variable rate.

Defaults

The default setting is **unsolicited-grant**.

Command Modes

Service flow QoS info configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example illustrates how to configure the **data-delivery-service** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
```

```
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

debug aaa pod

To enable POD debugging on the BWG, use the **debug aaa pod** Privileged EXEC command.

debug aaa pod

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

The following example enables POD debugging on the BWG:

```
router# debug aaa pod
```

debug condition

To enable conditional debugging on the BWG, use the **debug condition** command in privileged EXEC mode.

debug condition [**mac-address** *mac-id-of-subscriber*] [**ip** *bs-ip-address*]

Syntax Description

mac-address *mac-id-of-subscriber*]	based on the Subscriber MAC-ID
ip *bs-ip-address*	based on the BS IP address

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

When there is option to branch in the debug CLI, all the options after the **keyword** can be enabled by using the *carriage-return*. For example:

To enable all the WiMAX BWG related debugs, enter:

```
router#debug wimax agw
```

To enable all the WiMAX BWG session related debugs, enter:

```
router#debug wimax agw session
```

Examples

The following example enables conditional debugging on the BWG:

```
Router#debug condition mac-address mac-id-of-subscriber
Rotuer#debug condition ip bs-ip-address
```

debug eap

To display debug output for EAP related events and errors, use the **debug eap** command in privileged EXEC mode. Use the **no** version of command to turn off debug output.

debug eap {**all** | **authenticator** | **errors** | **events** | **packets** | **peer** | **sm**}

no debug eap {**all** | **authenticator** | **errors** | **events** | **packets** | **peer** | **sm**}

Syntax Description

all	Displays all eap debug information.
authenticator	Displays only authenticator errors.
errors	Displays eap errors.
events	Displays eap events.
packets	Displays eap packet information
peer	Displays only peer errors.
sm	Displays EAP state machine errors.

Defaults

No default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample output for the **debug eap events** command:

```
Router#debug eap events
EAP authenticator events debugging is on
EAP peer events debugging is on
Router#
*Feb 22 08:58:46.351: EAP-EVENT: Received context create from lower layer (0x59000003)
*Feb 22 08:58:46.351: EAP-AUTH-EVENT: Received AAA ID 0x00000005 from LL
*Feb 22 08:58:46.351: EAP-AUTH-AAA-EVENT: Assigning AAA ID 0x00000005
*Feb 22 08:58:46.351: EAP-EVENT: Allocated new EAP context (handle = 0xB4000003)
*Feb 22 08:58:46.351: EAP-EVENT: Received event 'EAP_AUTHENTICATOR_START' on handle
0xB4000003
*Feb 22 08:58:46.351: EAP-AUTH-EVENT: Current method = Identity
*Feb 22 08:58:46.351: EAP-AUTH-EVENT: Sending packet to lower layer for context 0xB4000003
*Feb 22 08:58:46.351: EAP-EVENT: Started 'Authenticator ReqId Retransmit' timer (5s) for
EAP sesion handle 0xB4000003
*Feb 22 08:58:46.351: EAP-EVENT: Started EAP tick timer
*Feb 22 08:58:46.351: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0xB4000003
*Feb 22 08:58:46.355: EAP-EVENT: Received event 'EAP_RX_PACKET' on handle 0xB4000003
*Feb 22 08:58:46.355: EAP-AUTH-EVENT: EAP Response received by context
BWG# 0xB4000003
*Feb 22 08:58:46.355: EAP-AUTH-EVENT: EAP Response type = Identity
```

```
*Feb 22 08:58:46.355: EAP-EVENT: Stopping 'Authenticator ReqId Retransmit' timer for EAP
sesion handle 0xB4000003
*Feb 22 08:58:46.355: EAP-AUTH-EVENT: Received peer identity: swimeap@wimax.org
*Feb 22 08:58:46.355: EAP-EVENT: Sending lower layer event 'EAP_GET_AAA_METHOD_LISTS' on
handle 0xB4000003
*Feb 22 08:58:46.355: EAP-EVENT: Sending lower layer event 'EAP_GET_PEER_MAC_ADDRESS' on
handle 0xB4000003
*Feb 22 08:58:46.355: EAP-EVENT: Sending lower layer event 'EAP_CUSTOMIZE_AAA_REQUEST' on
handle 0xB4000003
*Feb 22 08:58:46.355: EAP-AUTH-AAA-EVENT: Request sent successfully
*Feb 22 08:58:46.359: EAP-EVENT: eap_aaa_reply
*Feb 22 08:58:46.359: EAP-AUTH-AAA-EVENT: Server status: GET_CHALLENGE_RESPONSE
*Feb 22 08:58:46.359: EAP-EVENT: Received event 'EAP_AAA_RX_PACKET' on handle 0xB4000003
*Feb 22 08:58:46.359: EAP-AUTH-EVENT: Current method = 13
*Feb 22 08:58:46.359: EAP-AUTH-EVENT: Sending packet to lower layer
for context 0xB4000003
*Feb 22 08:58:46.359: EAP-EVENT: Started 'Authenticator Retransmit' timer (5s) for EAP
sesion handle 0xB4000003
*Feb 22 08:58:46.359: EAP-EVENT: Started EAP tick timer
*Feb 22 08:58:46.359: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0xB4000003
Router#
Router#
*Feb 22 08:58:51.479: EAP-EVENT: 'Authenticator Retransmit' timer expired for EAP sesion
handle 0xB4000003
*Feb 22 08:58:51.479: EAP-AUTH-EVENT: Resending last packet for context 0xB4000003
*Feb 22 08:58:51.479: EAP-AUTH-EVENT: Sending packet to lower layer for context 0xB4000003
*Feb 22 08:58:51.479: EAP-EVENT: Started 'Authenticator Retransmit' timer (5s) for EAP
sesion handle
*Feb 22 08:59:11.959: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0xB4000003
*Feb 22 08:59:11.959: EAP-EVENT: Received event 'EAP_RX_PACKET' on handle 0xB4000003
*Feb 22 08:59:11.959: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0xB4000003
Router#
*Feb 22 08:59:17.079: EAP-EVENT: 'Authenticator Retransmit' timer expired for EAP sesion
handle 0xB4000003
*Feb 22 08:59:17.079: EAP-EVENT: Sending lower layer event 'EAP_TIMEOUT' on handle
0xB4000003
*Feb 22 08:59:17.079: EAP-EVENT: Received free context (0xB4000003) from lower layer
*Feb 22 08:59:17.079: EAP-EVENT: Received event 'EAP_DELETE' on handle 0xB4000003
*Feb 22 08:59:17.079: EAP-AUTH-EVENT: Freed EAP auth context
*Feb 22 08:59:17.079: EAP-EVENT: Freed EAP context
BWG#
*Feb 22 08:59:18.103: EAP-EVENT: Stopped EAP tick timer
```

debug eap authenticator

To display debug output for EAP authenticator related events and errors, use the **debug eap authenticator** command in privileged EXEC mode. Use the **no** version of command to turn off debug output.

debug eap authenticator {**all** | **errors** | **events** | **packets** | **sm**}

no debug eap authenticator {**all** | **errors** | **events** | **packets** | **sm**}

Syntax Description

all	Displays all eap debug information.
errors	Displays eap errors.
events	Displays eap events.
packets	Displays eap packet information
sm	Displays EAP state machine errors.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample output for the **debug eap authenticator errors** command:

```
Router#debug eap authenticator errors
EAP authenticator errors debugging is on
Router#
*Feb 23 07:30:09.546: EAP-AUTH-ERROR: Invalid response id 2 (current id = 3)
```

Here is sample output for the**debug eap authenticator events** command:

```
Router#debug eap authenticator events
EAP authenticator events debugging is on
Router#
*Feb 23 07:36:08.258: EAP-EVENT: Received context create from lower layer (0x67000006)
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: Received AAA ID 0x00000009 from LL
*Feb 23 07:36:08.258: EAP-AUTH-AAA-EVENT: Assigning AAA ID 0x00000009
*Feb 23 07:36:08.258: EAP-EVENT: Allocated new EAP context (handle = 0x27000006)
*Feb 23 07:36:08.258: EAP-EVENT: Received event 'EAP_AUTHENTICATOR_START' on handle
0x27000006
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: Current method = Identity
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: Sending packet to lower layer for context 0x27000006
*Feb 23 07:36:08.258: EAP-EVENT: Started 'Authenticator ReqId Retransmit' timer (5s) for
EAP sesion handle 0x27000006
*Feb 23 07:36:08.258: EAP-EVENT: Started EAP tick timer
*Feb 23 07:36:08.258: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0x27000006
```

```
*Feb 23 07:36:08.258: EAP-EVENT: Received event 'EAP_RX_PACKET' on handle 0x27000006
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: EAP Response received by context
Router# 0x27000006
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: EAP Response type = Identity
*Feb 23 07:36:08.258: EAP-EVENT: Stopping 'Authenticator ReqId Retransmit' timer for EAP
sesion handle 0x27000006
*Feb 23 07:36:08.258: EAP-AUTH-EVENT: Received peer identity: swimeap@wimax.org
*Feb 23 07:36:08.258: EAP-EVENT: Sending lower layer event 'EAP_GET_AAA_METHOD_LISTS' on
handle 0x27000006
*Feb 23 07:36:08.258: EAP-EVENT: Sending lower layer event 'EAP_GET_PEER_MAC_ADDRESS' on
handle 0x27000006
*Feb 23 07:36:08.258: EAP-EVENT: Sending lower layer event 'EAP_CUSTOMIZE_AAA_REQUEST' on
handle 0x27000006
*Feb 23 07:36:08.258: EAP-AUTH-AAA-EVENT: Request sent successfully
*Feb 23 07:36:08.266: EAP-EVENT: eap_aaa_reply
*Feb 23 07:36:08.266: EAP-AUTH-AAA-EVENT: Server status: GET_CHALLENGE_RESPONSE
*Feb 23 07:36:08.266: EAP-EVENT: Received event 'EAP_AAA_RX_PACKET' on handle 0x27000006
*Feb 23 07:36:08.266: EAP-AUTH-EVENT: Current method = 13
*Feb 23 07:36:08.266: EAP-AUTH-EVENT: Sending packet to lower layer for context 0x27000006
*Feb 23 07:36:08.266: EAP-EVENT: Started 'Authenticator Retransmit' timer (5s) for EAP
sesion handle 0x27000006
*Feb 23 07:36:08.266: EAP-EVENT: Started EAP tick timer
*Feb 23 07:36:08.266: EAP-EVENT: Sending lower layer event 'EAP_TX_PACKET' on handle
0x27000006
*Feb 23 07:36:08.274: EAP-EVENT: Received event 'EAP_RX_PACKET' on handle 0x27000006
*Feb 23 07:36:08.274: EAP-AUTH-EVENT: EAP Response received by context 0x27000006
*Feb 23 07:36:08.274: EAP-AUTH-EVENT: EAP Response type = Method (13)
*Feb 23 07:36:08.274: EAP-EVENT: Stopping 'Authenticator Retransmit' timer for EAP sesion
handle 0x27000006
*Feb 23 07:36:08.274: EAP-EVENT: Sending lower layer event 'EAP_GET_AAA_METHOD_LISTS' on
handle 0x27000006
*Feb 23 07:36:08.274: EAP-EVENT: Sending lower layer event 'EAP_CUSTOMIZE_AAA_REQUEST' on
handle 0x27000006
*Feb 23 07:36:08.274: EAP-AUTH-AAA-EVENT: Request sent successfully
*Feb 23 07:36:08.282: EAP-EVENT: eap_aaa_reply
*Feb 23 07:36:08.282: EAP-AUTH-AAA-EVENT: Server status: GET_CHALLENGE_RESPONSE
*Feb 23 07:36:08.282: EAP-EVENT: Received event 'EAP_AAA_RX_PACKET' on handle 0x27000006
*Feb 23 07:36:08.282: EAP-AUTH-EVENT: Current method = 13
```

debug ip packet

To display general IP debugging information and IP security option (IPSO) security transactions, use the **debug ip packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip packet [*access-list-number*] [**detail**] [**dump**]

no debug ip packet [*access-list-number*]

Syntax Description

access-list-number	(Optional) The IP access list number that you can specify. If the datagram is not permitted by that access list, the related debugging output is suppressed. Standard, extended, and expanded access lists are supported. The range of standard and extended access lists is from 1 to 199. The range of expanded access lists is from 1300 to 2699.
detail	(Optional) Displays detailed IP packet debugging information. This information includes the packet types and codes as well as source and destination port numbers.
dump	(Hidden) Displays IP packet debugging information along with raw packet data in hexadecimal and ASCII forms. This keyword can be enabled with individual access lists and also with the **detail** keyword. **Note** The **dump** keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. See the caution notes below, in the usage guidelines, for more specific information.

Command Modes

Privileged EXEC

Usage Guidelines

If a communication session is closing when it should not be, an end-to-end connection problem can be the cause. The **debug ip packet** command is useful for analyzing the messages traveling between the local and remote hosts. IP packet debugging captures the packets that are process switched including received, generated and forwarded packets. IP packets that are switched in the fast path are not captured.

IPSO security transactions include messages that describe the cause of failure each time a datagram fails a security test in the system. This information is also sent to the sending host when the router configuration allows it.

Caution Because the **debug ip packet** command generates a substantial amount of output and uses a substantial amount of system resources, this command should be used with caution in production networks. It should only be enabled when traffic on the IP network is low, so other activity on the system is not adversely affected. Enabling the **detail** and **dump** keywords use the highest level of system resources of the available configuration options for this command, so a high level of caution should be applied when enabling either of these keywords.

Caution The **dump** keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. Because of the risk of using significant CPU utilization, the dump keyword is hidden from the user and cannot be seen using the "?" prompt. The length of the displayed packet information may exceed the actual packet length and include additional padding bytes that do not belong to the IP packet. Also note that the beginning of a packet may start at different locations in the dump output depending on the specific router, interface type, and packet header processing that may have occurred before the output is displayed.

Examples

The following is sample output from the **debug ip packet** command:

```
Router# debug ip packet

IP packet debugging is on

IP: s=172.69.13.44 (Fddi0), d=10.125.254.1 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.6 (Ethernet4), d=255.255.255.255, rcvd 2
IP: s=172.69.1.55 (Ethernet4), d=172.69.2.42 (Fddi0), g=172.69.13.6, forward
IP: s=172.69.89.33 (Ethernet2), d=10.130.2.156 (Serial2), g=172.69.16.2, forward
IP: s=172.69.1.27 (Ethernet4), d=172.69.43.126 (Fddi1), g=172.69.23.5, forward
IP: s=172.69.1.27 (Ethernet4), d=172.69.43.126 (Fddi0), g=172.69.13.6, forward
IP: s=172.69.20.32 (Ethernet2), d=255.255.255.255, rcvd 2
IP: s=172.69.1.57 (Ethernet4), d=10.36.125.2 (Serial2), g=172.69.16.2, access denied
```

The output shows two types of messages that the **debug ip packet** command can produce; the first line of output describes an IP packet that the router forwards, and the third line of output describes a packet that is destined for the router. In the third line of output, rcvd 2 indicates that the router decided to receive the packet.

Table 8 describes the significant fields shown in the display.

Table 8 debug ip packet Field Descriptions

Field	Description
IP:	Indicates that this is an IP packet.
s=172.69.13.44 (Fddi0)	Indicates the source address of the packet and the name of the interface that received the packet.
d=10.125.254.1 (Serial2)	Indicates the destination address of the packet and the name of the interface (in this case, S2) through which the packet is being sent out on the network.
g=172.69.16.2	Indicates the address of the next-hop gateway.
forward	Indicates that the router is forwarding the packet. If a filter denies a packet, "access denied" replaces "forward," as shown in the last line of output.

The following is sample output from the **debug ip packet** command enabled with the **detail** keyword:

```
Router# debug ip packet detail

IP packet debugging is on (detailed)

001556: 19:59:30: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
```

```
001557: 19:59:30: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03
001558: 19:59:30:     TCP src=179, dst=11001, seq=3736598846, ack=2885081910, wH
001559: 20:00:09: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
001560: 20:00:09: IP: s=10.4.9.4 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03
001561: 20:00:09:     TCP src=179, dst=11000, seq=163035693, ack=2948141027, wiH
001562: 20:00:14: CEF: Try to CEF switch 10.4.9.151 from FastEthernet0/0
001563: 20:00:14: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.151 (FastEthernet03
001564: 20:00:14:     ICMP type=8, code=0
001565: 20:00:14: IP: s=10.4.9.151 (local), d=10.4.9.6 (FastEthernet0/0), len 1g
001566: 20:00:14:     ICMP type=0, code=0
```

The format of the output with **detail** keyword provides additional information, such as the packet type, code, some field values, and source and destination port numbers.

Table 9 describes the significant fields shown in the display.

Table 9 debug ip packet detail Field Descriptions

Field	Description
CEF:	Indicates that the IP packet is being processed by CEF.
IP:	Indicates that this is an IP packet.
s=10.4.9.6 (FastEthernet0/0)	Indicates the source address of the packet and the name of the interface that received the packet.
d=10.4.9.151 (FastEthernet03)	Indicates the destination address of the packet and the name of the interface through which the packet is being sent out on the network.
TCP src=	Indicates the source TCP port number.
dst=	Indicates the destination TCP port number.
seq=	Value from the TCP packet sequence number field.
ack=	Value from the TCP packet acknowledgement field.
ICMP type=	Indicates ICMP packet type.
code=	Indicates ICMP return code.

The following is sample output from the **debug ip packet** command enabled with the **dump** keyword:

```
Router# debug ip packet dump

IP packet debugging is on (detailed) (dump)

21:02:42: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.4 (FastEthernet0/0), len 13
07003A00:                        0005 00509C08            ...P..
07003A10: 0007855B 4DC00800 45000064 001E0000  ...[M@..E..d....
07003A20: FE019669 0A040906 0A040904 0800CF7C  ~..i..........O|
07003A30: 0D052678 00000000 0A0B7145 ABCDABCD  ..&x......qE+M+M
07003A40: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
07003A50: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
07003A60: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
07003A70: ABCDABCD ABCDABCD ABCDABCD           +M+M+M+M+M+M
21:02:42: IP: s=10.4.9.4 (local), d=10.4.9.6 (FastEthernet0/0), len 100, sending
07003A00:                        0005 00509C08            ...P..
07003A10: 0007855B 4DC00800 45000064 001E0000  ...[M@..E..d....
07003A20: FF019569 0A040904 0A040906 0000D77C  ...i..........W|
07003A30: 0D052678 00000000 0A0B7145 ABCDABCD  ..&x......qE+M+M
07003A40: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
07003A50: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
07003A60: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
```

```
07003A70: ABCDABCD ABCDABCD ABCDABCD           +M+M+M+M+M+M
21:02:42: CEF: Try to CEF switch 10.4.9.4 from FastEthernet0/0
21:02:42: IP: s=10.4.9.6 (FastEthernet0/0), d=10.4.9.4 (FastEthernet0/0), len 13
07003380:                       0005 00509C08            ...P..
07003390: 0007855B 4DC00800 45000064 001F0000  ...[M@..E..d....
070033A0: FE019668 0A040906 0A040904 0800CF77  ~..h..........Ow
070033B0: 0D062678 00000000 0A0B7149 ABCDABCD  ..&x......qI+M+M
070033C0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
070033D0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
070033E0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
070033F0: ABCDABCD ABCDABCD ABCDABCD           +M+M+M+M+M+M
```

Note The **dump** keyword is not fully supported and should be used only in collaboration with Cisco Technical Support. See the caution in the usage guidelines section of this command reference page for more specific information.

The output from the **debug ip packet** command, when the **dump** keyword is enabled, provides raw packet data in hexadecimal and ASCII forms. This additional output is displayed in addition to the standard output. The **dump** keyword can be used with all of the available configuration options of this command.

Table 10 describes the significant fields shown in the display.

Table 10 debug ip packet dump Field Descriptions

Field	Description
IP:	Indicates that this is an IP packet.
s=10.4.9.6 (FastEthernet0/0)	Indicates the source address of the packet and the name of the interface that received the packet.
d=10.4.9.4 (FastEthernet0/0) len 13	Indicates destination address and length of the packet and the name of the interface through which the packet is being sent out on the network.
sending	Indicates that the router is sending the packet.

The calculation on whether to send a security error message can be somewhat confusing. It depends upon both the security label in the datagram and the label of the incoming interface. First, the label contained in the datagram is examined for anything obviously wrong. If nothing is wrong, assume the datagram to be correct. If something is wrong, the datagram is treated as *unclassified genser*. Then the label is compared with the interface range, and the appropriate action is taken, as Table 11 describes.

Table 11 Security Actions

Classification	Authorities	Action Taken
Too low	Too low	No Response
	Good	No Response
	Too high	No Response
In range	Too low	No Response
	Good	Accept
	Too high	Send Error
Too high	Too low	No Response
	In range	Send Error
	Too high	Send Error

The security code can only generate a few types of Internet Control Message Protocol (ICMP) error messages. The only possible error messages and their meanings follow:

- ICMP Parameter problem, code 0—Error at pointer
- ICMP Parameter problem, code 1—Missing option
- ICMP Parameter problem, code 2—See Note that follows
- ICMP Unreachable, code 10—Administratively prohibited

Note The message "ICMP Parameter problem, code 2" identifies a specific error that occurs in the processing of a datagram. This message indicates that the router received a datagram containing a maximum length IP header but no security option. After being processed and routed to another interface, it is discovered that the outgoing interface is marked with "add a security label." Because the IP header is already full, the system cannot add a label and must drop the datagram and return an error message.

When an IP packet is rejected due to an IP security failure, an audit message is sent via Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Network Address Translation (NAT). Also, any **debug ip packet** output is appended to include a description of the reason for rejection. This description can be any of the following:

- No basic
- No basic, no response
- Reserved class
- Reserved class, no response
- Class too low, no response
- Class too high
- Class too high, bad authorities, no response
- Unrecognized class
- Unrecognized class, no response
- Multiple basic

- Multiple basic, no response
- Authority too low, no response
- Authority too high
- Compartment bits not dominated by maximum sensitivity level
- Compartment bits do not dominate minimum sensitivity level
- Security failure: extended security disallowed
- NLESO source appeared twice
- ESO source not found
- Postroute, failed xfc out
- No room to add IPSO

debug ip slb

To display debugging messages for the Cisco IOS Server Load Balancing (SLB) feature, use the **debug ip slb** command in privileged EXEC mode. To disable debug output, use the no form of this command.To display the packet path inside ASNLB, use the **debug ip slb asnr6** command.

debug ip slb [conns | dfp | icmp | asnr6 | reals | all | sticky asn *msid* **]**

no debug ip slb [conns | dfp | icmp | asnr6 | reals | all | sticky asn *msid***]**

Syntax Description

conns	Displays debugging messages for all connections being handled by Cisco IOS SLB.
dfp	Displays debugging messages for the Cisco IOS SLB DFP and DFP agents.
icmp	Displays all ICMP debugging messages for Cisco IOS SLB.
asnr6	Displays all BWG R6 debugging messages for Cisco IOS SLB.
reals	Displays debugging messages for all real servers defined to Cisco IOS SLB.
all	Displays all debugging messages for Cisco IOS SLB.
sticky asn *msid*	Displays debugging messages for BWG sticky state.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.4(15)XL	The **asnr6** keyword was added.
12.4(24)YG	The **sticky asn** keywords were added.

Usage Guidelines

See the following caution before using **debug** commands.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, only use debug commands to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network flows and fewer users. Debugging during these periods reduces the effect these commands have on other users on the system.

Examples

Here is an example of the **debug ip slb** command:

```
Router# debug ip slb all
```

```
SLB All debugging is on
```

The following example stops all debugging:

```
Router# no debug all
All possible debugging has been turned off
```

debug radius

To display debugging output for RADIUS parameters, use the **debug radius** command in privileged EXEC mode. Use the **no** version of command to disable this feature.

debug radius {**brief** | **hex**}

no debug radius {**brief** | **hex**}

Syntax Description

brief	(Optional) Displays abbreviated debug output.
hex	(Optional) Displays debugging output in hexadecimal notation.

Defaults

Debugging output in ASCII format is enabled.

Command Modes

Privileged EXEC.

Command History

Release	Modification
11.2(1)T	This command was introduced.
12.2(11)T	The brief and hex keywords were added. The default output format became ASCII rather than hexadecimal.
12.4(15)XL	This command was integrated into Cisco IOS Release 12.4(15)XL.

Usage Guidelines

RADIUS is a distributed security system that secures networks against unauthorized access. Cisco supports RADIUS under the authentication, authorization, and accounting (AAA) security system. When RADIUS is used on the router, you can use the **debug radius** command to display detailed debugging and troubleshooting information in ASCII format. Use the **debug radius brief** command for abbreviated output displaying client/server interaction and minimum packet information. Use the **debug radius hex** command to display packet dump information that has not been truncated in hex format.

Examples

Here is sample output for the **debug radius brief** command:

```
Router#debug radius briefRadius protocol debugging is on
Radius protocol brief debugging is on
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is off
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
Router#
*Feb 22 08:33:03.259: RADIUS/ENCODE(00000002):Orig. component type = DOT1X
*Feb 22 08:33:03.259: RADIUS/ENCODE: NAS PORT sending disabled
*Feb 22 08:33:03.259: RADIUS(00000002): Config NAS IP: 0.0.0.0
*Feb 22 08:33:03.259: RADIUS(00000002): Config NAS IP: 0.0.0.0
```

```
*Feb 22 08:33:03.259: RADIUS: Attribute 55 not sent, as system clock is not set
*Feb 22 08:33:03.259: RADIUS/ENCODE: Best Local IP-Address 1.8.84.1 for Radius-Server
1.8.91.8
*Feb 22 08:33:03.259: RADIUS(00000002): Send Access-Request to 1.8.91.8:1645 id 1645/1,
len 231
Router#
*Feb 22 08:33:08.007: RADIUS: Retransmit to (1.8.91.8:1645,1646) for id 1645/1
*Feb 22 08:33:08.011: RADIUS: Received from id 1645/1 1.8.91.8:1645, Access-Challenge, len
75
*Feb 22 08:33:08.011: RADIUS/DECODE: EAP-Message fragments, 29, total 29 bytes
*Feb 22 08:33:08.011: RADIUS/ENCODE(00000002):Orig. component type = DOT1X
*Feb 22 08:33:08.011: RADIUS/ENCODE: NAS PORT sending disabled
*Feb 22 08:33:08.011: RADIUS(00000002): Config NAS IP: 0.0.0.0
*Feb 22 08:33:08.011: RADIUS(00000002): Config NAS IP: 0.0.0.0
*Feb 22 08:33:08.011: RADIUS: Attribute 55 not sent, as system clock is not set
*Feb 22 08:33:08.011: RADIUS/ENCODE: Best Local IP-Address 1.8.84.1 for Radius-Server
1.8.91.8
*Feb 22 08:33:08.011: RADIUS(00000002): Send Access-Request to 1.8.91.8:1645 id 1645/2,
len 227
*Feb 22 08:33:08.019: RADIUS: Received from id 1645/2 1.8.91.8:1645, Access-Accept, len 99
*Feb 22 08:33:08.019: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Feb 22 08:33:08.031: RADIUS/E
Router#NCODE(00000003):Orig. component type = AGW
*Feb 22 08:33:08.031: RADIUS/ENCODE: NAS PORT sending disabled
*Feb 22 08:33:08.031: RADIUS(00000003): Config NAS IP: 0.0.0.0
*Feb 22 08:33:08.031: RADIUS/ENCODE: Best Local IP-Address 1.8.84.1 for Radius-Server
1.8.91.8
*Feb 22 08:33:08.031: RADIUS(00000003): Send Accounting-Request to 1.8.91.8:1646 id
1646/1, len 206
*Feb 22 08:33:08.115: RADIUS: Received from id 1646/1 1.8.91.8:1646, Accounting-response,
len 20
Router#
*Feb 22 08:34:10.623: RADIUS/ENCODE(00000003):Orig. component type = AGW
*Feb 22 08:34:10.623: RADIUS/ENCODE: NAS PORT sending disabled
*Feb 22 08:34:10.623: RADIUS(00000003): Config NAS IP: 0.0.0.0
*Feb 22 08:34:10.623: RADIUS/ENCODE: Best Local IP-Address 1.8.84.1 for Radius-Server
1.8.91.8
*Feb 22 08:34:10.623: RADIUS(00000003): Send Accounting-Request to 1.8.91.8:1646 id
1646/2, len 236
*Feb 22 08:34:10.675: RADIUS: Received from id 1646/2 1.8.91.8:1646, Accounting-response,
len 20
```

debug wimax agw aaa

To display AAA authentication or accounting related events or errors, use the **debug wimax agw aaa** command in privileged EXEC mode. Use the **no** version of the command to disable debugging.

debug wimax agw aaa {**accounting** | **authentication**} {**events** | **errors**}

no debug wimax agw aaa {**accounting** | **authentication**} {**events** | **errors**}

Syntax Description

accounting	Displays AAA accounting related events or errors.
authentication	Displays AAA authentication related events or errors.
events	Displays events related to AAA accounting or authentication.
errors	Displays errors related to AAA accounting or authentication.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample output for AAA authentication events:

```
Router#debug wim agw aaa authentication events
WiMAX AGW AAA authentication events debugging is on
Router#
*Feb 23 07:53:49.397: AGW-Aaa: <1000003B0009>Allocated AAA unqiue id = 12
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Created AAA Auth context with UID 0xC
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Creating EAP LowerLayer context
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Created EAP lower layer handle with
0x9000007
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Received EAP evt EAP_TX_PACKET(0)
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Received EAP evt
EAP_GET_AAA_METHOD_LISTS(10)
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>EAP evt EAP_GET_AAA_METHOD_LISTS(10) -
usrgrp set
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Received EAP evt EAP_GET_PEER_MAC_ADDRESS(8)
*Feb 23 07:53:49.397: AGW-Auth: <1000003B0009>Received EAP evt
EAP_CUSTOMIZE_AAA_REQUEST(7)
*Feb 23 07:53:49.405: AGW-Auth: <1000003B0009>Received EAP evt EAP_TX_PACKET(0)
*Feb 23 07:53:49.405: AGW-Auth: <1000003B0009>Received EAP evt EAP_TX_PACKET(0)
*Feb 23 07:53:49.409: AGW-Auth: <1000003B0009>Received EAP evt
EAP_GET_AAA_METHOD_LISTS(10)
*Feb 23 07:53:49.413: AGW-Auth: <10
asn#00003B0009>EAP evt EAP_GET_AAA_METHOD_LISTS(10) - Ignoring [usrgrp already set]
*Feb 23 07:53:49.413: AGW-Auth: <1000003B0009>Received EAP evt
EAP_CUSTOMIZE_AAA_REQUEST(7)
*Feb 23 07:53:49.417: AGW-Auth: <1000003B0009>Received EAP evt EAP_TX_PACKET(0)
```

```
*Feb 23 07:53:49.421: AGW-Auth: <1000003B0009>Received EAP evt
EAP_GET_AAA_METHOD_LISTS(10)
*Feb 23 07:53:49.421: AGW-Auth: <1000003B0009>EAP evt EAP_GET_AAA_METHOD_LISTS(10) -
Ignoring [usrgrp already set]
*Feb 23 07:53:49.421: AGW-Auth: <1000003B0009>Received EAP evt
EAP_CUSTOMIZE_AAA_REQUEST(7)
*Feb 23 07:53:49.425: AGW-Auth: <1000003B0009>Received EAP evt EAP_TX_PACKET(0)
*Feb 23 07:53:49.425: AGW-Auth: <1000003B0009>Received EAP evt
EAP_GET_AAA_METHOD_LISTS(10)
*Feb 23 07:53:49.425: AGW-Auth: <1000003B0009>EAP evt EAP_GET_AAA_METHOD_LISTS(10) -
Ignoring [usrgrp already set]
*Feb 23 07:53:49.685: AGW-Auth: <1000003B0009>Received EAP evt
EAP_CUSTOMIZE_AAA_REQUEST(7)
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received EAP evt EAP_KEY_AVAILABLE(3)
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received EAP evt EAP_SUCCESS(1)
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received Class attr (class-wimax-changed)
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Recevied Absolute(session) timeout 1500 secs
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Recevied Idle timeout 600 secs
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received termination action 1
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received MS-MPPE-Send-Key, length 50, key
length 32
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received MS-MPPE-Recv-Key, length 50, key
length 32
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received AAA Session ID
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Deleting EAP LowerLayer context with handle
0x9000007
*Feb 23 07:53:49.701: AGW-Aaa: <1000003B0009><F[5]>Allocated AAA unqiue id = 13
```

Here is an example of an accounting message on MS open:

```
Router#debug wimax agw aaa accounting events
WiMAX AGW AAA accounting events debugging is on router#
*Feb 23 08:09:37.521: AGW-Acct: <1000000B0002><F[4]>Invoked
get dynamic attributes for path Unknown
router#
*Feb 23 08:09:43.181: AGW-Aaa: <100000310009><F[6]>Allocated
AAA unqiue id = 15
*Feb 23 08:09:43.181: AGW-Acct: <100000310009><F[6]>Invoked
get dynamic attributes for path Start
*Feb 23 08:09:43.181: AGW-Acct: <100000310009><F[6]>Started
accounting for uid 15 with uname swimeap@wimax.org
router#
```

Note The ms open command is run on the simulator, and the debug messages are observed on the BWG.

Here is an example of an accounting message on MS close:

```
Router#debug wimax agw aaa accounting events
WiMAX AGW AAA accounting events debugging is on router#
BWG#
*Feb 23 08:11:54.829: AGW-Acct: <100000310009><F[6]>Invoked
get dynamic attributes for path Stop
*Feb 23 08:11:54.829: AGW-Acct: <100000310009><F[6]>Stopped
accounting for uid 15 with uname swimeap@wimax.org
```

Note The ms close command is run on the simulator, and the debug messages are observed on the BWG.

debug wimax agw message

To enable conditional debugging for various types of BWG messages, use the **debug wimax agw message** command in privileged EXEC mode.

debug wimax agw message [**events** | **errors** | **dump**]

Syntax Description

events	Displays brief information on the processing of all transmitted and received messages.
errors	Displays details of any errors encountered during message processing.
dump	Displays details of all transmitted and received messages. Output will include the following: • IP packet details. Source/destination addresses, version, IP header length, TOS, total length, flags, IP fragmentation details, TTL, protocol, checksum. • UDP information. Source/destination ports, checksum, length. • Function-Type and Message-Type of the message. • Dump of all the TLVs contained in the message.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example displays a successful message open:

```
Router#debug wimax agw message dump
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Rx (GigabitEthernet0/1)
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> IP: Src: 10.1.1.70, Dst: 2.2.2.2
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Version: 0x4, IHL: 0x5, TOS: 0xC0
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Total Length: 0x4A, ID: 0x1A
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Flags: Reserved: 0x0, DontFrag: 0x0,
MoreFrag: 0x0
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Fragment offset: 0x0, TTL: 0xFE, Protocol:
0x11
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Checksum: 0xAC7E
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> UDP: Src Port: 0x8B7, Dst Port: 0x8B7
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Checksum: 0x7E1B, Length: 0x36
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Message: Type 0x090F (0x09, 0x0F)
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> FT: MS State Change, MT: Pre Attachment
Request
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Version: 0x01, Flags: 0x00, Type 0x90F
```

```
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> MSID: 067622242222, Reserved_1: 0x0000, Len:
0x2E
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> TransactionID: 0x0001, Reserved_2: 0x0000,
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Rx (GigabitEthernet0/1)
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> IP: Src: 10.1.1.70, Dst: 2.2.2.2
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Version: 0x4, IHL: 0x5, TOS: 0xC0
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Total Length: 0x30, ID: 0x1B
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Flags: Reserved: 0x0, DontFrag: 0x0,
MoreFrag: 0x0
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Fragment offset: 0x0, TTL: 0xFE, Protocol:
0x11
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Checksum: 0xAC97
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> UDP: Src Port: 0x8B7, Dst Port: 0x8B7
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Checksum: 0x8A1B, Length: 0x1C
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> Message: Type 0x0911 (0x09, 0x11)
*Feb 23 08:29:28.344: AGW-Msg: <067622242222> FT: MS State Change, MT: Pre Attachment ACK
```

Here is sample Message Events output on a successful MS Close:

```
Router#debug wimax agw message events
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x3, Type: 0x304, Len: 0x38, Flag: 0x2, FT: Data Path(0x3), MT: Deregistration
Request(0x4)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] FT/MT: 3/4, Ref pt: 3, TID rcvd
0X3(3), peer 0X2(2)[9/8], our 0X8002(32770)[3/12], Previous peer 0x1(1)[9/15], Previous
our 0X8001(32769)[3/12],TID RC: 1
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] Req FT/MT: 3/4, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>Tx DstAddr: 10.1.1.70, SrcPort: 2231, TID:
0x3, Type: 0x305, Len: 0x38, Flag: 0x0, FT: Data Path(0x3), MT: Deregistration
Response(0x5)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] FT/MT: 3/4, Ref pt: 3, Retcode =
Success(0)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x3, Type: 0x306, Len: 0x1C, Flag: 0x0, FT: Data Path(0x3), MT: Deregistration Ack(0x6)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] FT/MT: 3/6, Ref pt: 3, TID rcvd
0X3(3), peer 0X3(3)[3/4], our 0X8002(32770)[3/12], Previous peer 0x2(2)[9/8], Previous our
0X8001(32769)[3/12],TID RC: 1
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] Req FT/MT: 3/6, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>Deleting the R6 TID 0X65A3B46C,
10.1.1.70/2.2.2.2/0
*Feb 23 08:33:49.064: AGW-Msg: <100022230001>[Decode] FT/MT: 3/6, Ref pt: 3, Retcode =
Success(0)
```

Here is sample Message Events output when MS open fails:

```
Router#debug wimax agw message events
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x1, Type: 0x90F, Len: 0x2E, Flag: 0x0, FT: MS State Change(0x9), MT: Pre Attachment
Request(0xF)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] Req FT/MT: 9/15, Ref pt: 3, TID RC:
6, RC: Success(0)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] Created the R6 TID 0X65A3B4A8,
10.1.1.70/2.2.2.2/9
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>Tx DstAddr: 10.1.1.70, SrcPort: 2231, TID:
0x1, Type: 0x910, Len: 0x36, Flag: 0x0, FT: MS State Change(0x9), MT: Pre Attachment
Response(0x10)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] FT/MT: 9/15, Ref pt: 3, Retcode =
Success(0)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x1, Type: 0x911, Len: 0x14, Flag: 0x0, FT: MS State Change(0x9), MT: Pre Attachment
ACK(0x11)
```

```
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] FT/MT: 9/17, Ref pt: 3, TID rcvd
0X1(1), peer 0X1(1)[9/15], our 0X8000(32768)[0/0], Previous peer 0x0(0)[0/0], Previous our
0X0(0)[0/0],TID RC: 1
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] Req FT/MT: 9/17, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>[Decode] FT/MT: 9/17, Ref pt: 3, Retcode =
Success(0)
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>FT/MT: 8/2, generated TID 0X8001(32769),
10.1.1.70/2.2.2.2/8
*Feb 23 11:00:40.408: AGW-Msg: <067611141111>Tx DstAddr: 10.1.1.70, SrcPort: 2231, TID:
0x8001, Type: 0x802, Len: 0x1D, Flag: 0x0, FT: Auth Relay(0x8), MT: EAP Transfer(0x2)
*Feb 23 11:00:40.412: AGW-Msg: <067611141111>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x2, Type: 0x802, Len: 0x31, Flag: 0x0, FT: Auth Relay(0x8), MT: EAP Transfer(0x2)
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>Tx DstAddr: 10.1.1.70, SrcPort: 2231, TID:
0x8006, Type: 0x304, Len: 0x38, Flag: 0x2, FT: Data Path(0x3), MT: Deregistration
Request(0x4)
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>Rx SrcAddr: 10.1.1.70, SrcPort: 2231, TID:
0x8006, Type: 0x305, Len: 0x38, Flag: 0x0, FT: Data Path(0x3), MT: Deregistration
Response(0x5)
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>[Decode] FT/MT: 3/5, Ref pt: 3, TID rcvd
0X8006(32774), peer 0X6(6)[8/2], our 0X8006(32774)[3/4], Previous peer 0x5(5)[8/2],
Previous our 0X8005(32773)[8/2],TID RC: 1
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>[Decode] Req FT/MT: 3/5, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>Tx DstAddr: 10.1.1.70, SrcPort: 2231, TID:
0x8006, Type: 0x306, Len: 0x1C, Flag: 0x0, FT: Data Path(0x3), MT: Deregistration Ack(0x6)
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>Deleting the R6 TID 0X65A3B4A8,
10.1.1.70/2.2.2.2/0
*Feb 23 11:00:40.468: AGW-Msg: <067611141111>[Decode] FT/MT: 3/5, Ref pt: 3, Retcode =
Success(0)
```

Here is sample Message Events output when handoff fails:

```
Router#debug wimax agw message events
*Feb 23 12:35:52.003: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.72, SrcPort: 2231, TID:
0x1, Type: 0x401, Len: 0x2C, Flag: 0x0, FT: Context Delivery(0x4), MT: Context Delivery
Request(0x1)
*Feb 23 12:35:52.003: AGW-Msg: <100022230001>[Decode] Req FT/MT: 4/1, Ref pt: 3, TID RC:
5, RC: Success(0)
*Feb 23 12:35:52.003: AGW-Msg: <100022230001>[Decode] Created the R6 TID 0X65A3B3F4,
10.1.1.72/2.2.2.2/4
*Feb 23 12:35:52.003: AGW-Msg: <100022230001>Tx DstAddr: 10.1.1.72, SrcPort: 2231, TID:
0x1, Type: 0x402, Len: 0x69, Flag: 0x0, FT: Context Delivery(0x4), MT: Context Delivery
Report(0x2)
*Feb 23 12:35:52.003: AGW-Msg: <100022230001>[Decode] FT/MT: 4/1, Ref pt: 3, Retcode =
Success(0)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.72, SrcPort: 2231, TID:
0x2, Type: 0x30C, Len: 0x1D2, Flag: 0x0, FT: Data Path(0x3), MT: Registration Request(0xC)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>[Decode] FT/MT: 3/12, Ref pt: 3, TID rcvd
0X2(2), peer 0X1(1)[4/1], our 0X8000(32768)[0/0], Previous peer 0x0(0)[0/0], Previous our
0X0(0)[0/0],TID RC: 1
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>[Decode] Req FT/MT: 3/12, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001><F[41]>Tx DstAddr: 10.1.1.72, SrcPort: 2231,
TID: 0x2, Type: 0x30D, Len: 0xC0, Flag: 0x0, FT: Data Path(0x3), MT: Registration
Response(0xD)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001><F[42]>[Decode] FT/MT: 3/12, Ref pt: 3,
Retcode = Success(0)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.72, SrcPort: 2231, TID:
0x2, Type: 0x30E, Len: 0x1C, Flag: 0x0, FT: Data Path(0x3), MT: Registration Ack(0xE)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>[Decode] FT/MT: 3/14, Ref pt: 3, TID rcvd
0X2(2), peer 0X2(2)[3/12], our 0X8000(32768)[0/0], Previous peer 0x2(2)[3/12], Previous
our 0X0(0)[0/0],TID RC: 1
```

```
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>[Decode] Req FT/MT: 3/14, Ref pt: 3, TID RC:
1, RC: Success(0)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>FT/MT: 3/4, generated TID 0X8003(32771),
10.1.1.70/2.2.2.2/3
*Feb 23 12:35:52.007: AGW-Msg: <100022230001><F[41]>Tx DstAddr: 10.1.1.70, SrcPort: 2231,
TID: 0x8003, Type: 0x304, Len: 0x38, Flag: 0x0, FT: Data Path(0x3), MT: Deregistration
Request(0x4)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001><F[42]>[Decode] FT/MT: 3/14, Ref pt: 3,
Retcode = Success(0)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>Rx SrcAddr: 10.1.1.72, SrcPort: 2231, TID:
0x3, Type: 0x402, Len: 0x69, Flag: 0x0, FT: Context Delivery(0x4), MT: Context Delivery
Report(0x2)
*Feb 23 12:35:52.007: AGW-Msg: <100022230001>[Decode] FT/MT: 4/2, Ref pt: 3,
"Retcode = Fail - Abort(1)"
```

debug wimax agw message tlv

To display various BWG TLV messages, use the **debug wimax agw message tlv** command in privileged EXEC mode.

debug wimax agw message tlv [**events** | **errors** | **dump**]

Syntax Description

events	Displays brief information on the encoding and decoding of all TLVs.
errors	Displays details of any errors encountered during TLV encoding and decoding.
dump	Displays details of all TLVs encoded and decoded. The TLV type, length, and a hex dump of the TLV value are printed.

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example displays TLV events on a successful MS Open:

```
Router#debug wimax agw message tlv events
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: MS Information(0x0001), Length:
0x0006
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Authorization Policy(0x0028), Length:
0x0002
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Base Station Information(0x0002),
Length: 0x000C
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Base Station ID(0x0014), Length:
0x0008
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: MS Information(0x0001), Length:
0x0026
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Key Change Indicator(0x005F), Length:
0x0001
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Registration Context(0x0058), Length:
0x001D
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: MTG Profile(0x0069), Length: 0x0001
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: CS Type(0x0068), Length: 0x0002
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Number of Downlink CIDs(0x006A),
Length: 0x0002
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Number of Uplink CIDs(0x006B),
Length: 0x0002
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Number of Uplink Classifiers(0x006C),
Length: 0x0002
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Base Station Information(0x0002),
Length: 0x000C
*Feb 23 08:37:59.864: AGW-Tlv: <100022230001>  Type: Base Station ID(0x0014), Length:
0x0008
```

```
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Registration Type(0x002E), Length:
0x0004
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: MS Information(0x0001), Length:
0x004C
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Anchor Gateway ID(0x001B), Length:
0x0004
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: SF Information(0x0003), Length:
0x0014
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Direction(0x005E), Length: 0x0002
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Service Flow Identifier(0x003B),
Length: 0x0004
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Reservation Result(0x0065), Length:
0x0002
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: SF Information(0x0003), Length:
0x0028
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Direction(0x005E), Length: 0x0002
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Service Flow Identifier(0x003B),
Length: 0x0004
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Reservation Result(0x0065), Length:
0x0002
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: DP Information(0x0008), Length:
0x0010
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: DP Identifier(GRE Key)(0x0023),
Length: 0x0004
*Feb 23 08:37:59.868: AGW-Tlv: <100022230001>  Type: Data Path End point
Identifier(0x0024), Length: 0x0004
```

The following example displays TLV events on a successful MS close:

```
Router#debug wimax agw message tlv dump
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>  Type: Registration Type(0x002E), Length:
0x0004
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>   Value: 4
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>  Type: Anchor Gateway ID(0x001B), Length:
0x0004
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>    Hex: < 02 02 02 02 >
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>  Type: Base Station ID(0x0014), Length:
0x0008
*Feb 23 08:39:54.424: AGW-Tlv: <100022230001>    Hex: < 0A 01 01 46 00 00 00 00 >
*Feb 23 08:39:54.428: AGW-Tlv: <100022230001>  Type: Registration Type(0x002E), Length:
0x0004
*Feb 23 08:39:54.428: AGW-Tlv: <100022230001>   Value: 4
```

debug wimax agw path

To display BS path related messages, use the **debug wimax agw path** command in privileged EXEC mode.

debug wimax agw path [**events** | **errors**]

Syntax Description

events	Displays information on BS path related events.
errors	Displays information on BS path related errors

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample Path Events output on a successful MS Open:

```
Router#debug wimax agw path events
*Feb 23 10:32:36.496: AGW-Path: <(SU)-10.1.1.70>State transition Purging -> Ready
*Feb 23 10:32:36.496: AGW-Path: <(SU)-10.1.1.70>Stopping purge timer
*Feb 23 10:32:36.496: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 54 (refcount 1) with
resend required 1
*Feb 23 10:32:36.496: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 29 (refcount 1) with
resend required 0
*Feb 23 10:32:36.504: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 53 (refcount 1) with
resend required 0
*Feb 23 10:32:36.512: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 42 (refcount 1) with
resend required 1
*Feb 23 10:32:36.512: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 81 (refcount 1) with
resend required 1
*Feb 23 10:32:36.512: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 252 (refcount 1)
with resend required 1
*Feb 23 10:32:36.516: AGW-Path: <(DG)-10.1.1.70>Stopping purge timer
*Feb 23 10:32:36.516: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 28 (refcount 1) with
resend required 0
*Feb 23 10:32:36.520: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 274 (refcount 1)
with resend required 1
*Feb 23 10:32:36.520: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 28 (refcount 1) with
resend required 0
```

Here is sample Path Events output when an MS open fails:

```
Router#debug wimax agw path events
*Feb 23 10:35:05.196: AGW-Path: <(SU)-10.1.1.70>State transition Idle -> Ready
*Feb 23 10:35:05.196: AGW-Path: <(SU)-10.1.1.70>Created path with handle 0x6B000016
*Feb 23 10:35:05.196: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 54 (refcount 1) with
resend required 1
```

```
*Feb 23 10:35:05.200: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 29 (refcount 1) with
resend required 0
*Feb 23 10:35:05.204: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 30 (refcount 1) with
resend required 0
*Feb 23 10:35:05.216: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 1048 (refcount 1)
with resend required 0
*Feb 23 10:35:05.220: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 1048 (refcount 1)
with resend required 0
*Feb 23 10:35:05.228: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 922 (refcount 1)
with resend required 0
*Feb 23 10:35:05.256: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 56 (refcount 1) with
resend required 1
*Feb 23 10:35:05.256: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 28 (refcount 1) with
resend required 0
*Feb 23 10:35:05.256: AGW-Path: <(SU)-10.1.1.70>State transition Ready -> Purging
*Feb 23 10:35:05.256: AGW-Path: <(SU)-10.1.1.70>Starting purge timer for 20000 msecs
*Feb 23 10:35:25.428: AGW-Path: <(SU)-10.1.1.70>Expired purge timer after 20000 msecs
*Feb 23 10:35:25.428: AGW-Path: <(SU)-10.1.1.70>Deleting the path with handle 0x6B000016
```

Here is sample Path Events output on a successful MS Close:

```
Router#debug wimax agw path events
*Feb 23 10:34:12.204: AGW-Path: <(SU)-10.1.1.70>Enqueuing pak of size 56 (refcount 1) with
resend required 1
*Feb 23 10:34:12.208: AGW-Path: <(DG)-10.1.1.70>Starting purge timer for 20000 msecs
*Feb 23 10:34:12.208: AGW-Path: <(SU)-10.1.1.70>State transition Ready -> Purging
*Feb 23 10:34:12.208: AGW-Path: <(SU)-10.1.1.70>Starting purge timer for 20000 msecs
*Feb 23 10:34:32.392: AGW-Path: <(DG)-10.1.1.70>Expired purge timer after 20000 msecs
*Feb 23 10:34:32.392: AGW-Path: <(DG)-10.1.1.70>Deleting the path with handle 0x35000015
*Feb 23 10:34:32.392: AGW-Path: <(SU)-10.1.1.70>Expired purge timer after 20000 msecs
*Feb 23 10:34:32.392: AGW-Path: <(SU)-10.1.1.70>Deleting the path with handle 0x63000013
```

debug wimax agw r6 flow

To display BWG flow information, use the **debug wimax agw r6 flow** command in Privileged EXEC mode.

debug wimax agw r6 flow [**events** | **errors** | **fsm events** | **fsm errors**]

Syntax Description

events	Displays information on flow creation and deletion.
errors	Displays details of any flow related errors.
fsm events	Displays information regarding the flow FSM. Output shows all state transitions, and indicates if each transition was successfully completed.
fsm errors	Display details of errors encountered in the execution of the subscriber FSM.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample R6 flow output for a successful MS Open:

```
Router#debug wimax agw r6 flow events
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>[Downlink] Predefined SF QoS info set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>[Downlink] Predefined SF IPv4 TFT set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>[Uplink] Predefined SF QoS info set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>[Uplink] Predefined SF IPv4 TFT set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>Created flow with handle 0xD0000015,
local Id 0x15 for session handle 0xE500000F
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>[ISF] Created flow with index 0
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>[Downlink] Predefined SF QoS info set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>[Downlink] Predefined SF IPv4 TFT set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>[Uplink] Predefined SF QoS info set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>[Uplink] Predefined SF IPv4 TFT set
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>Created flow with handle 0x62000016,
local Id 0x16 for session handle 0xE500000F
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[22]>[SF] Created flow with index 1
*Feb 23 10:18:00.992: AGW-Flow: <100022230001><F[21]>Creating the sigpak resend details
0x207497F0, max resend 10, timeout 10000 msecs, timer type 2(16)
*Feb 23 10:18:00.996: AGW-Flow: <100022230001><F[21]>Starting pak resend timer 0x207497F0
for 10000 msecs with max resend 10, current resend 0, timer type 2(16)
*Feb 23 10:18:00.996: AGW-Flow: <100022230001><F[21]>Deleting the sigpak resend details
0x207497F0
*Feb 23 10:18:00.996: AGW-Flow: <100022230001><F[21]>Stopping pak resend timer 0x207497F0
for 10000 msecs with max resend 10, current resend 0, timer type 2(16)
*Feb 23 10:18:00.996: AGW-Flow: <100022230001><F[21]><(DG)-10.1.1.70>Link the flow to the
path
```

Here is sample R6 flow output for a successful MS Close:

```
Router#debug wimax agw r6 flow events
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[17]>Deleting flow with handle 0x87000011
for session handle 0x7900000D
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[17]><(DG)-10.1.1.70>Delink the flow from
the path
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[17]>Deallocating the Downlink SF details
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[17]>Deallocating the Uplink SF details
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[17]>Deleting flow
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[18]>Deleting flow with handle 0x3F000012
for session handle 0x7900000D
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[18]><(DG)-10.1.1.70>Delink the flow from
the path
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[18]>Deallocating the Downlink SF details
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[18]>Deallocating the Uplink SF details
*Feb 23 10:17:08.868: AGW-Flow: <100022230001><F[18]>Deleting flow
```

Here is sample R6 Flow FSM Events output for a successful MS Open:

```
Router#debug wimax agw r6 flow fsm events
*Feb 23 10:25:44.324: AGW-FlowFSM:<067622272222><F[27]>SF Idle(0) -> SF Establishing(1) on
event Tx Reg Req(4) with retcode Ok(0)
*Feb 23 10:25:44.328: AGW-FlowFSM:<067622272222><F[27]>SF Establishing(1) -> SF
Establishing(1) on event Rx Reg Rsp(5) with retcode Ok(0)
*Feb 23 10:25:44.328: AGW-FlowFSM:<067622272222><F[27]>SF Establishing(1) -> ISF Wait For
Addr Alloc(2) on event Tx Reg Ack(6) with retcode ISF - Ok(5)
*Feb 23 10:25:44.328: AGW-FlowFSM:<067622272222><F[27]>ISF Wait For Addr Alloc(2) -> SF
Ready(4) on event SF Addr Assigned(7) with retcode Ok(0)
*Feb 23 10:25:44.328: AGW-FlowFSM:<067622272222><F[27]>SF Ready(4) -> SF Ready(4) on event
Up(1) with retcode Ok(0)
*Feb 23 10:25:44.332: AGW-FlowFSM:<067622272222><F[28]>SF Idle(0) -> SF Establishing(1) on
event Tx Reg Req(4) with retcode Ok(0)
*Feb 23 10:25:44.332: AGW-FlowFSM:<067622272222><F[28]>SF Establishing(1) -> SF
Establishing(1) on event Rx Reg Rsp(5) with retcode Ok(0)
*Feb 23 10:25:44.332: AGW-FlowFSM:<067622272222><F[28]>SF Establishing(1) -> SF Ready(4)
on event Tx Reg Ack(6) with retcode Ok(0)
*Feb 23 10:25:44.332: AGW-FlowFSM:<067622272222><F[28]>SF Ready(4) -> SF Ready(4) on event
Up(1) with retcode Ok(0)
```

Here is sample R6 Flow FSM Events output for a successful MS Close:

```
Router#debug wimax agw r6 flow fsm events
*Feb 23 10:24:06.592: AGW-FlowFSM:<067622262222><F[19]>SF Ready(4) -> SF Cleanup(7) on
event Session Closed(2) with retcode Ok(0)
*Feb 23 10:24:06.592: AGW-FlowFSM:<067622262222><F[19]>SF Cleanup(7) -> SF Cleanup(7) on
event Session Closed(2) with retcode Ok(0)
*Feb 23 10:24:06.592: AGW-FlowFSM:<067622262222><F[20]>SF Ready(4) -> SF Cleanup(7) on
event Session Closed(2) with retcode Ok(0)
*Feb 23 10:24:06.592: AGW-FlowFSM:<067622262222><F[20]>SF Cleanup(7) -> SF Cleanup(7) on
event Session Closed(2) with retcode Ok(0)
```

debug wimax agw r6 session

To display BWG R6 session information, use the **debug wimax agw r6 session** command in Privileged EXEC mode.

debug wimax agw r6 session [**events** | **errors** | **fsm events** | **fsm errors**]

Syntax Description

events	Displays information on session creation and deletion.
errors	Display details of any R6 session related errors.
fsm events	Display information regarding the session FSM. Output will show all state transitions and indicates if each transition was successfully completed.
fsm errors	Display details of any errors encountered in the execution of the session FSM.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample output for R6 session events on a successful MS Open:

```
Router#debug wimax agw r6 session events
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Created session with handle 0x61000022, Id
0x22 for subscriber handle 0x83000022
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001><(SU)-10.1.1.70>:Link the session to the
path
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Created session
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Found usrgrp **unauthenticated** based on
domain  for user
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Creating the sigpak resend details
0x654986B8, max resend 10, timeout 10000 msecs, timer type 1(2)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Starting pak resend timer 0x654986B8 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Deleting the sigpak resend details
0x654986B8
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Stopping pak resend timer 0x654986B8 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Starting protect timer Rx attach req for 110
secs
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Creating the sigpak resend details
0x2034967C, max resend 10, timeout 10000 msecs, timer type 1(8)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Starting pak resend timer 0x2034967C for
10000 msecs with max resend 10, current resend 0, timer type 1(8)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Stopping protect timer Rx attach req
```

```
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Deleting the sigpak resend details
0x2034967C
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Stopping pak resend timer 0x2034967C for
10000 msecs with max resend 10, current resend 0, timer type 1(8)
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001><F[45]>Adding Host address 2.2.0.16
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001><F[45]>Static route IPv4 addr 2.2.0.16, aggr
mask 255.255.255.255
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001><F[45]>Created new host for the session
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001><F[45]>Set host IPv4 address 2.2.0.16 for
the session
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001>Starting Lease timer for host 2.2.0.16 with
timeout 3540 seconds
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001>Inserting static route 2.2.0.16
255.255.255.255 via 0.0.0.0, idb Virtual-Access2, tableid 0
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001>Added static route/inserted address 2.2.0.16
255.255.255.255/0
*Feb 23 12:55:34.723: AGW-Sess: <1000222A0001>Ready to switch traffic for session
```

Here is sample output for R6 session events when MS open fails:

```
Router#debug wimax agw r6 session events
*Feb 23 08:51:02.728: AGW-Sess: <067611141111>Created session with handle 0x74000009, Id
0x9 for subscriber handle 0xA3000009
*Feb 23 08:51:02.728: AGW-Sess: <067611141111><(SU)-10.1.1.70>:Link the session to the
path
*Feb 23 08:51:02.728: AGW-Sess: <067611141111>Created session
*Feb 23 08:51:02.728: AGW-Sess: <067611141111>Creating the sigpak resend details
0x65AEF5B4, max resend 10, timeout 10000 msecs, timer type 1(2)
*Feb 23 08:51:02.728: AGW-Sess: <067611141111>Starting pak resend timer 0x65AEF5B4 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:51:02.732: AGW-Sess: <067611141111>Deleting the sigpak resend details
0x65AEF5B4
*Feb 23 08:51:02.732: AGW-Sess: <067611141111>Stopping pak resend timer 0x65AEF5B4 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:51:02.732: AGW-Sess: <067611141111>Username pushetty@eap-tls.com, domain is
eap-tls.com, user is pushetty, delimiter @
*Feb 23 08:51:02.732: AGW-Sess: <067611141111>Found usrgrp eap-tls.com based on domain
eap-tls.com for user pushetty@eap-tls.com
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>[Authenticating / Auth Result Obtained]

*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Creating the sigpak resend details
0x654986B8, max resend 10, timeout 10000 msecs, timer type 1(10)
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Starting pak resend timer 0x654986B8 for
10000 msecs with max resend 10, current resend 0, timer type 1(10)
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Deleting the sigpak resend details
0x654986B8
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Stopping pak resend timer 0x654986B8 for
10000 msecs with max resend 10, current resend 0, timer type 1(10)
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Deleting session with handle 0x74000009 for
subscriber handle 0xA3000009
*Feb 23 08:51:02.788: AGW-Sess: <067611141111><(SU)-10.1.1.70>Delink the session from the
path
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Deleting session from usergroup
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Deleting session
```

Here is sample output for R6 session events when MS successfully closes:

```
Router#debug wimax agw r6 session events
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Creating the sigpak resend details
0x65F35C00, max resend 10, timeout 10000 msecs, timer type 1(11)
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Starting pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(11)
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Deleting session with handle 0x49000008 for
subscriber handle 0x6000008
```

```
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Deleting the sigpak resend details
0x65F35C00
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Stopping pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(11)
*Feb 23 08:54:17.556: AGW-Sess: <067622242222><(SU)-10.1.1.70>Delink the session from the
path
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Deleting session from usergroup
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Stopping session timer
*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Deleting session
```

Here is sample output for R6 FSM Session Events on a successful MS Open:

```
Router#debug wimax agw r6 session fsm events
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Created session with handle 0x9C00000A, Id
0xA for subscriber handle 0x200000A
*Feb 23 08:56:35.700: AGW-Sess: <100022230001><(SU)-10.1.1.70>:Link the session to the
path
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Created session
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Found usrgrp **unauthenticated** based on
domain  for user
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Idle(0) -> Authorizing(1) on event Rx Pre
Attach Req(1) with retcode Ok(0)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Creating the sigpak resend details
0x65F35C00, max resend 10, timeout 10000 msecs, timer type 1(2)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Authorizing(1) -> Authorizing(1) on event
Tx Pre Attach Rsp(2) with retcode Ok(0)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Deleting the sigpak resend details
0x65F35C00
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Stopping pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Starting protect timer Rx attach req for 110
secs
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Authorizing(1) -> Registering(6) on event
Rx Pre Attach Ack(3) with retcode Authentication Skipped(4)
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Registering(6) -> Registering(6) on event
Rx Attach Req(12) with retcode Ok(0)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Creating the sigpak resend details
0x65F35C00, max resend 10, timeout 10000 msecs, timer type 1(8)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(8)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Stopping protect timer Rx attach req
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Registering(6) -> Registering(6) on event
Tx Attach Rsp(13) with retcode Ok(0)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Deleting the sigpak resend details
0x65F35C00
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Stopping pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(8)
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Registering(6) -> Ready(7) on event Rx
Attach Ack(14) with retcode Ok(0)
*Feb 23 08:56:35.700: AGW-SessFSM:<100022230001>Ready(7) -> Ready(7) on event Rx Attach
Ack(14) with retcode Ok(0)
```

Here is sample output for R6 FSM Session Events when MS Open fails:

```
Router#debug wimax agw r6 session fsm events
GW-Sess: <067611141111><(SU)-10.1.1.70>:Link the session to the path
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Created session
*Feb 23 08:59:07.448: AGW-SessFSM:<067611141111>Idle(0) -> Authorizing(1) on event Rx Pre
Attach Req(1) with retcode Ok(0)
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Creating the sigpak resend details
0x65F35C00, max resend 10, timeout 10000 msecs, timer type 1(2)
```

```
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Starting pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:59:07.448: AGW-SessFSM:<067611141111>Authorizing(1) -> Authorizing(1) on event
Tx Pre Attach Rsp(2) with retcode Ok(0)
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Deleting the sigpak resend details
0x65F35C00
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Stopping pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(2)
*Feb 23 08:59:07.448: AGW-SessFSM:<067611141111>Authorizing(1) -> Authenticating(2) on
event Rx Pre Attach Ack(3) with retcode Ok(0)
*Feb 23 08:59:07.448: AGW-SessFSM:<067611141111>Authenticating(2) -> Authenticating(2) on
event Tx EAP Pkt(5) with retcode Ok(0)
*Feb 23 08:59:07.452: AGW-SessFSM:<067611141111>Authenticating(2) -> Authenticating(2) on
event Rx EAP Pkt(4) with retcode Ok(0)
*Feb 23 08:59:07.452: AGW-Sess: <067611141111>Username pushetty@eap-tls.com, domain is
eap-tls.com, user is pushetty, delimiter @
*Feb 23 08:59:07.452: AGW-Sess: <067611141111>Found usrgrp eap-tls.com based on domain
eap-tls.com for user pushetty@eap-tls.com
*Feb 23 08:59:07.456: AGW-SessFSM:<067611141111>Authenticating(2) -> Authenticating(2) on
event Tx EAP Pkt(5) with retcode Ok(0)
*Feb 23 08:59:07.504: AGW-SessFSM:<067611141111>Authenticating(2) -> Deleting(8) on event
Auth Result Obtained(7)

*Feb 23 08:59:07.504: AGW-Sess: <067611141111>Creating the sigpak resend details
0x506F3A88, max resend 10, timeout 10000 msecs, timer type 1(10)
*Feb 23 08:59:07.504: AGW-Sess: <067611141111>Starting pak resend timer 0x506F3A88 for
10000 msecs with max resend 10, current resend 0, timer type 1(10)
*Feb 23 08:59:07.504: AGW-SessFSM:<067611141111>Deleting(8) -> Deleting(8) on event Tx
Dereg Req(22) with retcode Ok(0)
*Feb 23 08:59:07.508: AGW-SessFSM:<067611141111>Deleting(8) -> Deleting(8) on event Rx
Dereg Rsp(23) with retcode Ok(0)
*Feb 23 08:59:07.508: AGW-Sess: <067611141111>Deleting the sigpak resend details
0x506F3A88
*Feb 23 08:59:07.508: AGW-Sess: <067611141111>Stopping pak resend timer 0x506F3A88 for
10000 msecs with max resend 10, current resend 0, timer type 1(10)
*Feb 23 08:59:07.508: AGW-SessFSM:<067611141111>Deleting(8) -> Cleanup(9) on event Tx
Dereg Ack(24) with retcode Ok(0)
```

Here is sample output for R6 FSM Session Events when the MS successfully closes:

```
Router#debug wimax agw r6 session fsm events
*Feb 23 08:57:13.696: AGW-SessFSM:<100022230001>Ready(7) -> Deleting(8) on event Rx Dereq
Req(19) with retcode Ok(0)
*Feb 23 08:57:13.696: AGW-SessFSM:<100022230001>Deleting(8) -> Deleting(8) on event Rx
Dereq Req(19) with retcode Ok(0)
*Feb 23 08:57:13.696: AGW-Sess: <100022230001>Creating the sigpak resend details
0x65F35C00, max resend 10, timeout 10000 msecs, timer type 1(11)
*Feb 23 08:57:13.696: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(11)
*Feb 23 08:57:13.696: AGW-SessFSM:<100022230001>Deleting(8) -> Deleting(8) on event Tx
DeReg Rsp(20) with retcode Ok(0)
*Feb 23 08:57:13.696: AGW-SessFSM:<100022230001>Deleting(8) -> Cleanup(9) on event Rx
Dereg Ack(21) with retcode Ok(0)
*Feb 23 08:57:13.696: AGW-Sess: <100022230001>Deleting session with handle 0x9C00000A for
subscriber handle 0x200000A
*Feb 23 08:57:13.700: AGW-Sess: <100022230001>Deleting the sigpak resend details
0x65F35C00
*Feb 23 08:57:13.700: AGW-Sess: <100022230001>Stopping pak resend timer 0x65F35C00 for
10000 msecs with max resend 10, current resend 0, timer type 1(11)
*Feb 23 08:57:13.700: AGW-Sess: <100022230001><(SU)-10.1.1.70>Delink the session from the
path
*Feb 23 08:57:13.700: AGW-Sess: <100022230001>Deleting session from usergroup
*Feb 23 08:57:13.700: AGW-Sess: <100022230001>Deleting session
```

debug wimax agw r6 subscriber

To display BWG R6 subscriber information, use the **debug wimax agw r6 subscriber** command in Privileged EXEC mode.

debug wimax agw r6 subscriber [**events** | **errors**]

Syntax Description

events	Display information on subscriber creation and deletion.
errors	Display details of any subscriber related errors.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is sample R6 Subscriber Events output on a successful MS Open:

```
Router#debug wimax agw r6 subscriber events
*Feb 23 10:29:03.804: AGW-Subs: <067622242222>Created subscriber with handle 0x29000016
*Feb 23 10:29:03.804: AGW-Subs: <067622242222>Created subscriber
*Feb 23 10:29:03.820: AGW-Subs: <067622242222>Starting subscriber wait for address
allocation timer for 300 secs
*Feb 23 10:29:03.824: AGW-Subs: <067622242222>Stopping subscriber wait for address
allocation timer
```

Here is sample R6 Subscriber Events output on a successful MS Close:

```
Router#debug wimax agw r6 subscriber events
GW-Subs: <067622272222>Deleting subscriber
*Feb 23 10:27:38.924: AGW-Subs: <067622272222>Deleting a subscriber with handle 0x77000013
```

debug wimax agw redundancy

To display BWG redundancy information, use the **debug wimax agw redundancy** command in Privileged EXEC mode.

debug wimax agw redundancy [**events** | **errors** | **tlv** | **packets**]

Syntax Description

events	Displays information on redundancy related events.
errors	Displays information on redundancy related errors.
tlv	Displays information on redundancy related tlvs.
packets	Displays information on redundancy related message dumps in binary.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example displays BWG redundancy information:

```
debug wimax agw redundancy events
```

Output on ACTIVE BWG for MS Open for Ethernet-cs/Ip-cs

```
router#
*May 19 18:00:53.420: AGW-SR: Type AGW_MAC_ID(0), Length 6, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0032234AABCD>
*May 19 18:00:53.420: AGW-SR: Type AGW_SUB_AUTH_POLICY(1), Length 2, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type AGW_SUB_AUTH_AK_CONTEXT_PRESENT(9), Length 1, Class
Optional
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_ID_CTRL_REMOTE(0), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_ID_CTRL_LOCAL(1), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <4>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_LOCAL_ADDR_SIG(2), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <33686018>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_REMOTE_ADDR_SIG(3), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <167838022>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_LOCAL_UDPPORT_SIG(4), Length 2, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <2231>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_REMOTE_UDPPORT_SIG(5), Length 2, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <2231>
```

```
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_CS_TYPE(7), Length 2, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_CS_TYPE_CAPABLITY(8), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <8>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_SLA_PROFILE_NAME(9), Length 6, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <73696C766572>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_FLAG_UNAUTHENTICATED(45), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_MAX_FLOWS_SUPPORTED(48), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_SESSION_TIMEOUT(50), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT(51), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <180>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_SESSION_START_TIME(52), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1211220053>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_SEQ_ENABLED_FOR_SIGNALING(53), Length 1,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_IDS_REQUIRED_SIGNALLING(54), Length 1,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT_DIRECECTION_INBOUND(55),
Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_READY_FOR_SWITCHING_TRAFFIC(56), Length 1,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_IS_SESSION_SYNCED(57), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_BSID(17), Length 8, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0A01014600000000>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_USRGRP_DOMAIN_NAME(43), Length 15, Class
Optional
*May 19 18:00:53.420: AGW-SR: Value <756E61757468656E74696361746564>
*May 19 18:00:53.420: AGW-SR: Type UGW_SESSION_FLAG_AUTO_PROVISIONED(12), Length 1, Class
Optional
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_PATH_BSID(104), Length 8, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0A01014600000000>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_INDEX(60), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ID_DATA_LOCAL(62), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <4>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ID_DATA_REMOTE(63), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <5>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_REMOTE_ADDR_DATA(61), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <167838022>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_START_TIME(64), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1211220053>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_CREATE_TIME(65), Length 8, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0000000000000000>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_FASTSWITCHABLE(66), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SEQ_ENABLED_DATA(67), Length 1, Class
Mandatory
```

```
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_IS_FLOW_SYNCED(68), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_SENDING_ACCT_RECORD(92), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_PATH_SEND(93), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_LAST_ACCT_RECORD(94), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_TERMINATE_CAUSE(95), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_ACCT_START_SENT(97), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_DISCARD(98), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_ACCT_SESSION_ID(103), Length 4, Class Optional
*May 19 18:00:53.420: AGW-SR: Value <5>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_ID(69), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <8>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(70), Length 1,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(71), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <11>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(72), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(73), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(74), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <41>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(75), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <51>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(76), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <61>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(77), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <71>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(78), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(79), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <81>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(80),
Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(81), Length 4,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(82), Length 0, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(83), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
```

```
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(84), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <184>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CS_TYPE(85), Length 2, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <3>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(86), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(87), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(88), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CS_TYPE_PRESENT(89), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(90), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_ID(69), Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <7>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(70), Length 1,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <2>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(71), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(72), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <2>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(73), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <3>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(74), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <4>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(75), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <5>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(76), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <49>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(77), Length 4, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(78), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(79), Length
4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(80),
Length 4, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <9>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(81), Length 4,
Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(82), Length 0, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(83), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(84), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <120>
```

```
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CS_TYPE(85), Length 2, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <3>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(86), Length 1, Class Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(87), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(88), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_CS_TYPE_PRESENT(89), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <1>
*May 19 18:00:53.420: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(90), Length 1, Class
Mandatory
*May 19 18:00:53.420: AGW-SR: Value <0>
*May 19 18:00:53.420: AGW-SR:
03652A60: 00000267 00140015 00000006 0032234A  ...g.........2#J
03652A70: ABCD0001 00020000 00090001 00001500  +M..............
03652A80: A3000000 04000000 00000100 04000000  #...............
03652A90: 04000200 04020202 02000300 040A0101  ................
03652AA0: 46000400 0208B700 05000208 B7000700  F.....7.....7...
03652AB0: 02000000 08000400 00000800 09000673  ...............s
03652AC0: 696C7665 72002D00 01010030 00010100  ilver.-....0....
03652AD0: 32000400 00000000 33000400 0000B400  2.......3.....4.
03652AE0: 34000448 31C05500 35000100 00360001  4..H1@U.5....6..
03652AF0: 00003700 01000038 00010100 39000100  ..7....8....9...
03652B00: 00110008 0A010146 00000000 002B000F  .......F.....+..
03652B10: 756E6175 7468656E 74696361 74656400  unauthenticated.
03652B20: 0C000100 0016000C 00680008 0A010146  .........h.....F
03652B30: 00000000 0017018B 00000187 003C0001  .............<..
03652B40: 00003E00 04000000 04003F00 04000000  ..>.......?.....
03652B50: 05003D00 040A0101 46004000 044831C0  ..=.....F.@..H1@
03652B60: 55004100 08000000 00000000 00004200  U.A...........B.
03652B70: 01000043 00010000 44000100 005C0004  ...C....D....\..
03652B80: 00000000 005D0004 00000000 005E0004  .....].......^..
03652B90: 00000000 005F0001 00006100 01000062  ....._....a....b
03652BA0: 00010000 67000400 00000500 45000400  ....g......E...
03652BB0: 00000800 46000101 00470004 0000000B  ....F....G......
03652BC0: 00480004 00000000 00490004 00000000  .H.......I......
03652BD0: 004A0004 00000029 004B0004 00000033  .J.....).K.....3
03652BE0: 004C0001 3D004D00 04000000 47004E00  .L..=.M.....G.N.
03652BF0: 0100004F 00040000 00510050 00040000  ...O.....Q.P....
03652C00: 00000051 00040000 00000052 00000053  ...Q.......R...S
03652C10: 00010000 540001B8 00550002 00030056  ....T..8.U.....V
03652C20: 00010100 57000101 00580001 01005900  ....W....X....Y.
03652C30: 0101005A 00010000 45000400 00000700  ...Z....E.......
03652C40: 46000102 00470004 00000001 00480004  F....G.......H..
03652C50: 00000002 00490004 00000003 004A0004  .....I.......J..
03652C60: 00000004 004B0004 00000005 004C0001  .....K.......L..
03652C70: 31004D00 04000000 00004E00 0101004F  1.M.......N....O
03652C80: 00040000 00000050 00040000 00090051  .......P.......Q
03652C90: 00040000 00000052 00000053 00010000  .......R...S....
03652CA0: 54000178 00550002 00030056 00010100  T..x.U.....V....
03652CB0: 57000101 00580001 01005900 0101005A  W....X....Y....Z
03652CC0: 00010000 18000000                    ........
*May 19 18:00:53.420: AGW-SR: <0032234AABCD><F[4]>Session (Setup) Sync to Standby
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ALLOCATED_ADDR(19), Length 4, Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <33685507>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_TABLE_ID(20), Length 0, Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_ALLOC_SOURCE(21), Length 4, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <5>
```

```
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_REAL_LENGTH(22), Length 2, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <1040>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ALLOCATED_PREFIX_LENGTH(23), Length 1, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <16>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_AGGREGATE_PREFIX_LENGTH(24), Length 1, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <32>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_ORG_TYPE(25), Length 1, Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <1>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_TYPE_NUM(26), Length 1, Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <33>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_STATIC_ROUTE_ADDED(33), Length 1, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <1>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_TYPE_STATIC_ALLOCATED(34), Length 1,
Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <0>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_ALLOCATED(35), Length 1,
Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <1>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_REQUEST(36), Length 1, Class
Mandatory
*May 19 18:00:53.444: AGW-SR: Value <0>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_IP_KEY(37), Length 8, Class Mandatory
*May 19 18:00:53.444: AGW-SR: Value <0202000300000000>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_DHCP_SERVER_ADDR(27), Length 4, Class Optional
*May 19 18:00:53.444: AGW-SR: Value <0>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_DHCP_SERVER_XID(28), Length 4, Class Optional
*May 19 18:00:53.444: AGW-SR: Value <2095>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_TYPE(29), Length 1,
Class Optional
*May 19 18:00:53.444: AGW-SR: Value <1>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_HARDWARE_ADDRESS_LEN(30), Length 1, Class
Optional
*May 19 18:00:53.444: AGW-SR: Value <6>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_DHCP_CLIENT_ADDR_LEASE_TIME(31), Length 4,
Class Optional
*May 19 18:00:53.444: AGW-SR: Value <3540>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_CLIENT_HARDWARE_ADDRESS(32), Length 16, Class
Optional
*May 19 18:00:53.444: AGW-SR: Value <0032234AABCD00000000000000000000>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ETHER_TYPE(38), Length 4, Class Optional
*May 19 18:00:53.444: AGW-SR: Value <2>
*May 19 18:00:53.444: AGW-SR: Type UGW_SR_HOST_ETHER_HDR(39), Length 30, Class Optional
*May 19 18:00:53.444: AGW-SR: Value
<0032234AABCD00000C07AC0181000003025CAAAA03000000080000000000>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_ETHER_HDR_LEN(40), Length 2, Class Optional
*May 19 18:00:53.444: AGW-SR: Value <26>
*May 19 18:00:53.444: AGW-SR: Type UGW_HOST_STATIC_HOST(41), Length 1, Class Optional
*May 19 18:00:53.444: AGW-SR: Value <0>
*May 19 18:00:53.444: AGW-SR: Attr Type:UGW_HOST_FLOW_INDEX Length: 1 Value: 0
*May 19 18:00:53.444: AGW-SR:
03653100:                           000600CA              ...J
03653110: 00140000 001900C2 000000BE 00130004  .......B...>....
03653120: 02020003 00140000 00150004 00000005  ................
03653130: 00160002 04100017 00011000 18000120  ...............
03653140: 00190001 01001A00 01210021 00010100  .........!.!....
03653150: 22000100 00230001 01002400 01000025  "....#....$....%
03653160: 00080202 00030000 0000001B 00040000  ................
03653170: 0000001C 00040000 082F001D 00010100  ........./......
03653180: 1E000106 001F0004 00000DD4 00200010  ...........T. ..
03653190: 0032234A ABCD0000 00000000 00000000  .2#J+M..........
```

```
036531A0: 00260004 00000002 0027001E 0032234A  .&.......'...2#J
036531B0: ABCD0000 0C07AC01 81000003 025CAAAA  +M....,......\**
036531C0: 03000000 08000000 00000028 0002001A  ...........(....
036531D0: 00290001 000012                      .).....
*May 19 18:00:53.444: AGW-SR: <0032234AABCD><F[4]>Host 2.2.0.3 create synced to standby
BWG#



Standby - For MS open (ethernet-cs)
===================================

asn#
*May 19 18:00:53.431: AGW-SR:
036566D0: 00140015 00000006 0032234A ABCD0001  .........2#J+M..
036566E0: 00020000 00090001 00001500 A3000000  ............#...
036566F0: 04000000 00000100 04000000 04000200  ................
03656700: 04020202 02000300 040A0101 46000400  ............F...
03656710: 0208B700 05000208 B7000700 02000000  ..7.....7.......
03656720: 08000400 00000800 09000673 696C7665  ...........silve
03656730: 72002D00 01010030 00010100 32000400  r.-....0....2...
03656740: 00000000 33000400 0000B400 34000448  ....3.....4.4..H
03656750: 31C05500 35000100 00360001 00003700  1@U.5....6....7.
03656760: 01000038 00010100 39000100 00110008  ...8....9.......
03656770: 0A010146 00000000 002B000F 756E6175  ...F.....+..unau
03656780: 7468656E 74696361 74656400 0C000100  thenticated.....
03656790: 0016000C 00680008 0A010146 00000000  .....h.....F....
036567A0: 0017018B 00000187 003C0001 00003E00  .........<....>.
036567B0: 04000000 04003F00 04000000 05003D00  ......?.......=.
036567C0: 040A0101 46004000 044831C0 55004100  ....F.@..H1@U.A.
036567D0: 08000000 00000000 00004200 01000043  ..........B....C
036567E0: 00010000 44000100 005C0004 00000000  ....D....\......
036567F0: 005D0004 00000000 005E0004 00000000  .].......^......
03656800: 005F0001 00006100 01000062 00010000  ._....a....b....
03656810: 67000400 00000500 45000400 00000800  g.......E.......
03656820: 46000101 00470004 0000000B 00480004  F....G.......H..
03656830: 00000000 00490004 00000000 004A0004  .....I.......J..
03656840: 00000029 004B0004 00000033 004C0001  ...).K.....3.L..
03656850: 3D004D00 04000000 47004E00 0100004F  =.M.....G.N....O
03656860: 00040000 00510050 00040000 00000051  .....Q.P.......Q
03656870: 00040000 00000052 00000053 00010000  .......R...S....
03656880: 540001B8 00550002 00030056 00010100  T..8.U.....V....
03656890: 57000101 00580001 01005900 0101005A  W....X....Y....Z
036568A0: 00010000 45000400 00000700 46000102  ....E.......F...
036568B0: 00470004 00000001 00480004 00000002  .G.......H......
036568C0: 00490004 00000003 004A0004 00000004  .I.......J......
036568D0: 004B0004 00000005 004C0001 31004D00  .K.......L..1.M.
036568E0: 04000000 00004E00 0101004F 00040000  ......N....O....
036568F0: 00000050 00040000 00090051 00040000  ...P.......Q....
03656900: 00000052 00000053 00010000 54000178  ...R...S....T..x
03656910: 00550002 00030056 00010100 57000101  .U.....V....W...
03656920: 00580001 01005900 0101005A 00010000  .X....Y....Z....
03656930: 18000000 19000000                    ........
*May 19 18:00:53.431: AGW-SR: Type AGW_MAC_ID(0), Length 6, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0032234AABCD>
*May 19 18:00:53.431: AGW-SR: Type AGW_SUB_AUTH_POLICY(1), Length 2, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type AGW_SUB_AUTH_AK_CONTEXT_PRESENT(9), Length 1, Class
Optional
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Usar Name not found
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_ID_CTRL_REMOTE(0), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
```

```
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_ID_CTRL_LOCAL(1), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <4>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_LOCAL_ADDR_SIG(2), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <33686018>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_REMOTE_ADDR_SIG(3), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <167838022>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_LOCAL_UDPPORT_SIG(4), Length 2, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <2231>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_REMOTE_UDPPORT_SIG(5), Length 2, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <2231>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_CS_TYPE(7), Length 2, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_CS_TYPE_CAPABLITY(8), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <8>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_SLA_PROFILE_NAME(9), Length 6, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <73696C766572>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_FLAG_UNAUTHENTICATED(45), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_MAX_FLOWS_SUPPORTED(48), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_SESSION_TIMEOUT(50), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT(51), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <180>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_SESSION_START_TIME(52), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1211220053>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_SEQ_ENABLED_FOR_SIGNALING(53), Length 1,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_IDS_REQUIRED_SIGNALLING(54), Length 1,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT_DIRECECTION_INBOUND(55),
Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_READY_FOR_SWITCHING_TRAFFIC(56), Length 1,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_IS_SESSION_SYNCED(57), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_BSID(17), Length 8, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0A01014600000000>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_USRGRP_DOMAIN_NAME(43), Length 15, Class
Optional
*May 19 18:00:53.431: AGW-SR: Value <756E61757468656E74696361746564>
*May 19 18:00:53.431: AGW-SR: Type UGW_SESSION_FLAG_AUTO_PROVISIONED(12), Length 1, Class
Optional
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_PATH_BSID(104), Length 8, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0A01014600000000>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_INDEX(60), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ID_DATA_LOCAL(62), Length 4, Class Mandatory
```

```
*May 19 18:00:53.431: AGW-SR: Value <4>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ID_DATA_REMOTE(63), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <5>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_REMOTE_ADDR_DATA(61), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <167838022>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_START_TIME(64), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1211220053>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_CREATE_TIME(65), Length 8, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0000000000000000>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_FASTSWITCHABLE(66), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SEQ_ENABLED_DATA(67), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_IS_FLOW_SYNCED(68), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_SENDING_ACCT_RECORD(92), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_PATH_SEND(93), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_LAST_ACCT_RECORD(94), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_TERMINATE_CAUSE(95), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_ACCT_START_SENT(97), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_DISCARD(98), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_ACCT_SESSION_ID(103), Length 4, Class Optional
*May 19 18:00:53.431: AGW-SR: Value <5>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_ID(69), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <8>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(70), Length 1,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(71), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <11>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(72), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(73), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(74), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <41>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(75), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <51>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(76), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <61>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(77), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <71>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(78), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
```

```
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(79), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <81>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(80),
Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(81), Length 4,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(82), Length 0, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(83), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(84), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <184>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CS_TYPE(85), Length 2, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <3>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(86), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(87), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(88), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CS_TYPE_PRESENT(89), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(90), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_ID(69), Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <7>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(70), Length 1,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <2>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(71), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(72), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <2>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(73), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <3>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(74), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <4>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(75), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <5>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(76), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <49>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(77), Length 4, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(78), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(79), Length
4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
```

```
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(80),
Length 4, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <9>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(81), Length 4,
Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(82), Length 0, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(83), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(84), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <120>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CS_TYPE(85), Length 2, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <3>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(86), Length 1, Class Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(87), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(88), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_CS_TYPE_PRESENT(89), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <1>
*May 19 18:00:53.431: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(90), Length 1, Class
Mandatory
*May 19 18:00:53.431: AGW-SR: Value <0>
*May 19 18:00:53.439: AGW-SR:
03656C20:                   00140000 001900C2          .......B
03656C30: 000000BE 00130004 02020003 00140000  ...>............
03656C40: 00150004 00000005 00160002 04100017  ................
03656C50: 00011000 18000120 00190001 01001A00  ....... ........
03656C60: 01210021 00010100 22000100 00230001  .!.!...."....#..
03656C70: 01002400 01000025 00080202 00030000  ..$....%........
03656C80: 0000001B 00040000 0000001C 00040000  ................
03656C90: 082F001D 00010100 1E000106 001F0004  ./..............
03656CA0: 00000DD4 00200010 0032234A ABCD0000  ...T. ...2#J+M..
03656CB0: 00000000 00000000 00260004 00000002  .........&......
03656CC0: 0027001E 0032234A ABCD0000 0C07AC01  .'...2#J+M....,.
03656CD0: 81000003 025CAAAA 03000000 08000000  .....\**........
03656CE0: 00000028 0002001A 00290001 00001200  ...(.....).......
03656CF0: 010000                               ...
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ALLOCATED_ADDR(19), Length 4, Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <33685507>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_TABLE_ID(20), Length 0, Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_ALLOC_SOURCE(21), Length 4, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <5>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_REAL_LENGTH(22), Length 2, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <1040>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ALLOCATED_PREFIX_LENGTH(23), Length 1, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <16>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_AGGREGATE_PREFIX_LENGTH(24), Length 1, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <32>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_ORG_TYPE(25), Length 1, Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <1>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_TYPE_NUM(26), Length 1, Class Mandatory
```

```
*May 19 18:00:53.439: AGW-SR: Value <33>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_STATIC_ROUTE_ADDED(33), Length 1, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <1>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_TYPE_STATIC_ALLOCATED(34), Length 1,
Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <0>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_ALLOCATED(35), Length 1,
Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <1>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_REQUEST(36), Length 1, Class
Mandatory
*May 19 18:00:53.439: AGW-SR: Value <0>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_IP_KEY(37), Length 8, Class Mandatory
*May 19 18:00:53.439: AGW-SR: Value <0202000300000000>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_DHCP_SERVER_ADDR(27), Length 4, Class Optional
*May 19 18:00:53.439: AGW-SR: Value <0>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_DHCP_SERVER_XID(28), Length 4, Class Optional
*May 19 18:00:53.439: AGW-SR: Value <2095>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_TYPE(29), Length 1,
Class Optional
*May 19 18:00:53.439: AGW-SR: Value <1>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_HARDWARE_ADDRESS_LEN(30), Length 1, Class
Optional
*May 19 18:00:53.439: AGW-SR: Value <6>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_DHCP_CLIENT_ADDR_LEASE_TIME(31), Length 4,
Class Optional
*May 19 18:00:53.439: AGW-SR: Value <3540>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_CLIENT_HARDWARE_ADDRESS(32), Length 16, Class
Optional
*May 19 18:00:53.439: AGW-SR: Value <0032234AABCD00000000000000000000>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ETHER_TYPE(38), Length 4, Class Optional
*May 19 18:00:53.439: AGW-SR: Value <2>
*May 19 18:00:53.439: AGW-SR: Type UGW_SR_HOST_ETHER_HDR(39), Length 30, Class Optional
*May 19 18:00:53.439: AGW-SR: Value
<0032234AABCD00000C07AC0181000003025CAAAA03000000080000000000>
BWG#
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_ETHER_HDR_LEN(40), Length 2, Class Optional
*May 19 18:00:53.439: AGW-SR: Value <26>
*May 19 18:00:53.439: AGW-SR: Type UGW_HOST_STATIC_HOST(41), Length 1, Class Optional
*May 19 18:00:53.439: AGW-SR: Value <0>
*May 19 18:00:53.439: AGW-SR: <0032234AABCD><F[4]>Subscriber 2.2.0.3 synced from active
```

Output on STANDBY BWG for MS Open

```
       Mar  4 20:09:29.224: AGW-SR:
20135C40:                           001400A9              ...)
20135C50: 00000006 06761112 11110001 00020012  .....v..........
20135C60: 00030014 1EB253DD E845CFF0 C5281F33  .....2S]hEOpE(.3
20135C70: AF951520 22FE51FF 00020004 00000001  /.. "~Q.........
20135C80: 00040008 E0D148B4 9E578601 00050002  ....`QH4.W......
20135C90: 3A980006 00020001 00070001 00000800  :...............
20135CA0: 01000009 00010100 0A000E0A 01014602  ..............F.
20135CB0: 02020206 76111211 11000B00 02800900  ....v...........
20135CC0: 0C000103 000D0001 0C000E00 02800800  ................
20135CD0: 0F000108 00100001 05001100 02000900  ................
20135CE0: 12000109 00130001 08001400 02000800  ................
20135CF0: 15000108 00160001 02001500 F3000000  ............s...
20135D00: 04000000 00000100 04000000 05000200  ...............

20135D10: 04020202 02000300 040A0101 46000400  ............F...
20135D20: 0208B700 05000208 B7001E00 01000020  ..7.....7......
20135D30: 00010000 22000100 00210001 01002300  ....".....!....#.
20135D40: 0400003A 98002400 04000000 00002500  ...:..$.......%.
```

```
20135D50: 08000000 0010B765 E8002600 01000027  ......7eh.&....'
20135D60: 00010000 28000100 00290001 01002A00  ....(....)....*.
20135D70: 0100001F 00403C9E 68DEDCDD 94126A63  .....@<.h^\]..jc
20135D80: B21697BC 95E0140C E89BFD1D 31DB19B8  2..<.`..h.}.1[.8
20135D90: F95C8E1A ECC83CCE 2F570CD8 176637C4  y\..lH<N/W.X.f7D
20135DA0: D8AD4E43 7DEA7D88 8BDC44DC 35FEFC20  X-NC}j}..\D\5~|
20135DB0: 679740D4 028B001B 00147075 73686574  g.@T......pushet
20135DC0: 74794065 61702D74 6C732E63 6F6D001C  ty@eap-tls.com..
20135DD0: 00072A2A 616E792A 2A000600 13636C61  ..**any**....cla
20135DE0: 73732D77 696D6178 2D636861 6E676564  ss-wimax-changed
20135DF0: 0016000C 00550008 0A010146 00000000  .....U.....F....
20135E00: 0017017C 00000178 002B0001 00002D00  ...|...x.+....-.
20135E10: 04000000 08002E00 04000000 19002F00  ................/.
20135E20: 08000000 0010B766 C8003000 08000000  ......7fH.0.....
20135E30: 00000000 00003100 01000032 00010000  ......1....2....
20135E40: 33000100 00490004 00000001 004A0004  3....I.......J..
20135E50: 00000000 004B0004 00000001 004C0001  .....K.......L..
20135E60: 00004D00 0102004E 00010100 4F000100  ..M....N....O...
20135E70: 00540004 0000000E 00340004 00000010  .T.......4......
20135E80: 00350001 01003600 04000000 0B003700  .5....6.......7.
20135E90: 04000000 00003800 04000000 00003900  ......8.......9.
20135EA0: 04000000 00003A00 04000000 33003B00  ......:.....3.;.
20135EB0: 013D003C 00040000 0047003D 00010000  .=.<.....G.=....
20135EC0: 3E000400 00005100 3F000400 00000000  >.....Q.?.......
20135ED0: 40000400 00000000 41000000 42000100  @.......A...B...
20135EE0: 00430001 00004400 01010045 00010100  .C....D....E....
20135EF0: 46000101 00470001 00003400 04000000  F....G....4.....
20135F00: 0F003500 01020036 00040000 00010037  ..5....6.......7
20135F10: 00040000 00020038 00040000 00030039  .......8.......9
20135F20: 00040000 0004003A 00040000 0005003B  .......:.......;
20135F30: 00013100 3C000400 00000000 3D000101  ..1.<.......=...
20135F40: 003E0004 00000000 003F0004 00000009  .>.......?......
20135F50: 00400004 00000000 00410000 00420001  .@.......A...B..
20135F60: 00004300 01000044 00010100 45000101  ..C....D....E...
20135F70: 00460001 01004700 01000017 00028009  .F....G........
20135F80: 00180000 00190094 00000090 00080004  ................
20135F90: 02020002 00090002 0000000A 00040000  ................
20135FA0: 0005000B 00020420 000C0001 20000D00  ....... .... ...
20135FB0: 0120000E 00010100 0F000121 00160001  . .........!....
20135FC0: 01001700 01000018 00010100 19000100  ................
20135FD0: 001A0008 02020002 00000000 00100004  ................
20135FE0: 00000000 00110004 00001415 00120001  ................
20135FF0: 01001300 01060014 00100676 11121111  ...........v....
20136000: 00000000 00000000 00000015 00040000  ...........
20136010: 0DD40007 00010000 56000101 7A        .T......V...z
Mar  4 20:09:29.228: AGW-SR: Type AGW_MAC_ID(0), Length 6, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <067611121111>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_POLICY(1), Length 2, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <18>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AK(3), Length 20, Class Optional
Mar  4 20:09:29.228: AGW-SR: Value <1EB253DDE845CFF0C5281F33AF95152022FE51FF>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AK_METHOD(2), Length 4, Class Optional
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AKID(4), Length 8, Class Optional
Mar  4 20:09:29.228: AGW-SR: Value <E0D148B49E578601>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AKLIFETIME(5), Length 2, Class Optional
Mar  4 20:09:29.228: AGW-SR: Value <15000>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_CMAC_KEY_COUNT(6), Length 2, Class Optional
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AK_SEQUENCE_NUM(7), Length 1, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_PMK_SEQUENCE_NUM(8), Length 1, Class
Optional
```

```
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type AGW_SUB_AUTH_AK_CONTEXT_PRESENT(9), Length 1, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type AGW_TID_HASH_KEY(10), Length 14, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0A0101460202020206761112111 1>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_TID(11), Length 2, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <32777>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_TID_FT(12), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <3>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_TID_MT(13), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <12>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_PREVIOUS_TID(14), Length 2, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <32776>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_PREVIOUS_TID_FT(15), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <8>
Mar  4 20:09:29.228: AGW-SR: Type AGW_OUR_PREVIOUS_TID_MT(16), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <5>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_TID(17), Length 2, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <9>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_TID_FT(18), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <9>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_TID_MT(19), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <8>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_PREVIOUS_TID(20), Length 2, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <8>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_PREVIOUS_TID_FT(21), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <8>
Mar  4 20:09:29.228: AGW-SR: Type AGW_PEER_PREVIOUS_TID_MT(22), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <2>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_ID_CTRL_REMOTE(0), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_ID_CTRL_LOCAL(1), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <5>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_LOCAL_ADDR_SIG(2), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <33686018>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_REMOTE_ADDR_SIG(3), Length 4, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <167838022>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_LOCAL_UDPPORT_SIG(4), Length 2, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <2231>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_REMOTE_UDPPORT_SIG(5), Length 2, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <2231>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_FLAG_UNAUTHENTICATED(30), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_FLAG_NW_BEHIND_MS(32), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_FLAG_FRAMED_ROUTE_DOWNLOADED(34), Length 1,
Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_MAX_FLOWS_SUPPORTED(33), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_SESSION_TIMEOUT(35), Length 4, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <15000>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT(36), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_SESSION_START_TIME(37), Length 8, Class
Mandatory
```

```
Mar  4 20:09:29.228: AGW-SR: Value <0000000010B765E8>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_SEQ_ENABLED_FOR_SIGNALING(38), Length 1,
Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_IDS_REQUIRED_SIGNALLING(39), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT_DIRECECTION_INBOUND(40), Length
1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_READY_FOR_SWITCHING_TRAFFIC(41), Length 1,
Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_IS_SESSION_SYNCED(42), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_MASTER_SESSION_KEY(31), Length 64, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value
<3C9E68DEDCDD94126A63B21697BC95E0140CE89BFD1D31DB19B8F95C8E1AECC83CCE2F570CD8176637C4D8AD4
E437DEA7D888BDC44DC35FEFC20679740D4028B>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_USRGRP_USER_NAME(27), Length 20, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value <707573686574747940656170 2D746C732E636F6D>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_USRGRP_DOMAIN_NAME(28), Length 7, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value <2A2A616E792A2A>
Mar  4 20:09:29.228: AGW-SR: Type UGW_SESSION_ACCT_AAA_AT_CLASS(6), Length 19, Class
Optional
Mar  4 20:09:29.228: AGW-SR: Value <636C6173732D77696D61782D6368616E676564>
Mar  4 20:09:29.228: AGW-SR: Type UGW_PATH_BSID(85), Length 8, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0A01014600000000>
Mar  4 20:09:29.228: AGW-SR: <067611121111><F[0]>Replacing Local Acct Context Session
IdReceived From Active: 14
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_INDEX(43), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ID_DATA_LOCAL(45), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <8>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ID_DATA_REMOTE(46), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <25>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_START_TIME(47), Length 8, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0000000010B766C8>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_CREATE_TIME(48), Length 8, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0000000000000000>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_FASTSWITCHABLE(49), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_SEQ_ENABLED_DATA(50), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_IS_FLOW_SYNCED(51), Length 1, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_SENDING_ACCT_RECORD(73), Length 4, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_PATH_SEND(74), Length 4, Class Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_LAST_ACCT_RECORD(75), Length 4, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_TERMINATE_CAUSE(76), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <0>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_AIRLINK_STATE(77), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <2>
```

```
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_ACCT_START_SENT(78), Length 1, Class
Mandatory
Mar  4 20:09:29.228: AGW-SR: Value <1>
Mar  4 20:09:29.228: AGW-SR: Type UGW_FLOW_ACCT_DISCARD(79), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_ACCT_SESSION_ID(84), Length 4, Class Optional
Mar  4 20:09:29.232: AGW-SR: Value <14>
Mar  4 20:09:29.232: AGW-SR: Type AGW_FLOW_CURR_TID_USED(23), Length 2, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <32777>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_ID(52), Length 4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <16>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(53), Length 1,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(54), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <11>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(55), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(56), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(57), Length 4,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(58), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <51>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(59), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <61>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(60), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <71>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(61), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(62), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <81>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(63), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(64), Length 4,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(65), Length 0, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(66), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(67), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(68), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(69), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(70), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(71), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
```

```
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_ID(52), Length 4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <15>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(53), Length 1,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <2>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(54), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(55), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <2>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(56), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <3>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(57), Length 4,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <4>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(58), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <5>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(59), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <49>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(60), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(61), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(62), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(63), Length
4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <9>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(64), Length 4,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(65), Length 0, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(66), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(67), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(68), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(69), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(70), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(71), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ALLOCATED_ADDR(8), Length 4, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <33685506>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_TABLE_ID(9), Length 2, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_ALLOC_SOURCE(10), Length 4, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <5>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_REAL_LENGTH(11), Length 2, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1056>
```

```
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ALLOCATED_PREFIX_LENGTH(12), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <32>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_AGGREGATE_PREFIX_LENGTH(13), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <32>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_ORG_TYPE(14), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_TYPE_NUM(15), Length 1, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <33>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_STATIC_ROUTE_ADDED(22), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_TYPE_STATIC_ALLOCATED(23), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_ALLOCATED(24), Length 1,
Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_REQUEST(25), Length 1, Class
Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_IP_KEY(26), Length 8, Class Mandatory
Mar  4 20:09:29.232: AGW-SR: Value <0202000200000000>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_SERVER_ADDR(16), Length 4, Class Optional
Mar  4 20:09:29.232: AGW-SR: Value <0>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_SERVER_XID(17), Length 4, Class Optional
Mar  4 20:09:29.232: AGW-SR: Value <5141>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_TYPE(18), Length 1, Class
Optional
Mar  4 20:09:29.232: AGW-SR: Value <1>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_LEN(19), Length 1, Class
Optional
Mar  4 20:09:29.232: AGW-SR: Value <6>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_CLIENT_HARDWARE_ADDRESS(20), Length 16,
Class Optional
Mar  4 20:09:29.232: AGW-SR: Value <06761112111100000000000000000000>
Mar  4 20:09:29.232: AGW-SR: Type UGW_HOST_DHCP_CLIENT_ADDR_LEASE_TIME(21), Length 4,
Class Optional
Mar  4 20:09:29.232: AGW-SR: Value <3540>
Mar  4 20:09:29.232: AGW-SR: <067611121111><F[8]>Subscriber 2.2.0.2 synced from active
```

debug wimax agw slb

To display BWG server-load-balancing(SLB) information, use the **debug wimax agw slb** command in Privileged EXEC mode.

debug wimax agw slb [events | errors | packets]

Syntax Description

events	Displays information on SLB related events.
errors	Displays information on SLB related errors.
packets	Displays information on SLB related message dumps in binary.

Command Default

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example displays BWG SLB information:

```
router#debug wimax agw slb events
```

debug wimax agw switching

To display BWG switching information, use the **debug wimax agw switching** command in Privileged EXEC mode.

debug wimax agw switching [**errors** | **events** | **arp events** | **arp errors** | **arp packet** [**brief** | **detail**]| **gre events** | **gre errors** | **gre packet** [**brief** | **detail**] | **udp** [**events** | **errors**] | **udp packet** [**brief** | **detail**] | **dhcp** [**errors** | **events**] | **pmip** [**errors** | **events** | **fsm** [**errors** | **events**] | **packet** [**detail** | **brief**]] | **pppoe** [**errors** | **events**]]

Syntax Description

events	Displays information on bearers / signaling related events.
errors	Displays information on bearers / signaling related errors.
arp events	Displays information on arp related events.
arp errors	Displays information on arp related errors.
brief	Displays brief packet information.
detail	Displays detailed packet information.
arp packet	Displays information on arp related packet dump.
gre events	Displays information on bearer GRE related events.
gre errors	Displays information on bearer GRE related errors.
gre packet	Displays information on bearer GRE related packet being switched.
gre packet	Displays information on bearer GRE related packet dump being switched.
udp events	Displays information on signaling UDP related events.
udp errors	Displays information on signaling UDP related errors.
udp packet	Displays information on related signaling UDP packet being switched.
udp packet	Displays information on related signaling UDP packet dump being switched.
dhcp events	Displays information on IOS DHCP interaction related events.
dhcp errors	Displays information on IOS DHCP interaction related errors.
pmip errors	Displays information on Proxy Mobile IP errors.
pmip events	Displays information on Proxy Mobile IP events.
pmip fsm	Displays information on Proxy Mobile IP Finite State Machine (fsm)
pmip packet	Displays information on Proxy Mobile IP packets.
pppoe errors | events	Displays information on PPPoe errors or events.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(24)YG	The **pmip** and **pppoe** keywords and options were added.

Examples

The following example displays various BWG switching information:

```
router#debug wimax agw switching
WiMAX AGW switching events debugging is on
WiMAX AGW switching errors debugging is on
WiMAX AGW switching UDP events debugging is on
WiMAX AGW switching UDP errors debugging is on
WiMAX AGW switching UDP packets debugging is on
WiMAX AGW switching UDP packet detail dump debugging is on
WiMAX AGW switching GRE events debugging is on
WiMAX AGW switching GRE errors debugging is on
WiMAX AGW switching GRE packets debugging is on
WiMAX AGW switching GRE packet detail dump debugging is on
WiMAX AGW switching DHCP events debugging is on
WiMAX AGW switching DHCP errors debugging is on
WiMAX AGW switching DHCP packets debugging is on
WiMAX AGW switching DHCP packet detail dump debugging is on
```

The following sample output illustrates an MS Open:

```
*Aug 30 22:52:44.012: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Session
Signal:Sending UDP 54 bytes pak
*Aug 30 22:52:44.012: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Session
Signal:Sending UDP 81 bytes pak
*Aug 30 22:52:44.012: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Flow
Signal:Sending UDP 252 bytes pak
*Aug 30 22:52:44.016: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Flow
Signal:Sending UDP 28 bytes pak
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>CEF Upstream Et0/0:Rcvd
GRE 646 bytes with flags crKss, version 0x0, procotol 0x800
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>CEF Upstream Vi2:Rcvd
604(646) byte pak, TOS 0X0
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream
Et0/0:Rcvd GRE 646 bytes with flags crKss, version 0x0, procotol 0x800
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream Et0/0
Inner pak 646 bytes pak(retval 0x0, is_ours 1)
contiguous pak, size 646
         AA BB CC 03 34 00 AA BB CC 03 35 00 08 00 45 00
         02 78 00 11 00 00 FD 2F AB FB 0A 01 01 46 02 02
         02 02 20 00 08 00 00 00 00 05 45 00 02 5C 00 4B
         00 00 FE 11 B0 3C 05 05 05 05 FF FF FF FF 00 44
         00 43 02 48 32 06 01 01 ...
*Aug 30 22:52:44.016: AGW-DHCP: <100022270001>PROCESS Upstream DHCP from MS:IP
Src=5.5.5.5, IP Dst=255.255.255.255, gi=0.0.0.0, len=584, sfid=ox9
*Aug 30 22:52:44.016: AGW-DHCP: <100022270001>PROCESS Upstream Decode DHCP
DISCOVER:len=576, ci=0.0.0.0, gi=0.0.0.0, si=0.0.0.0, yi=0.0.0.0, sfid=0x9(9)
*Aug 30 22:52:44.016: AGW-DHCP: <100022270001>PROCESS Upstream Options for DHCP DISCOVER :
53(1),57(2),61(7),12(13),55(5),255(0),
*Aug 30 22:52:44.016: AGW-DHCP: <100022270001>PROCESS Upstream Added Option 82 Subscriber
ID: 1000.2227.0001, Circuit ID: 9
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream
Vi2:Rcvd 620(662) bytes pak, TOS 0X0
*Aug 30 22:52:44.016: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream GRE
pak Rcvd 620(662) bytes pak
contiguous pak, size 620
         45 00 02 6C 00 4B 00 00 FE 11 A9 D4 02 02 02 02
         0B 01 01 5D 00 44 00 43 02 58 9C 40 01 01 06 00
         00 00 08 33 00 00 80 00 00 00 00 00 00 00 00 00
         00 00 00 00 02 02 02 02 10 00 22 27 00 01 00 00
         00 00 00 00 00 00 00 00 ...
bwg#
*Aug 30 22:52:44.600: %RADIUS-4-RADIUS_DEAD: RADIUS server 1.8.91.8:1645,1646 is not
responding.
```

```
*Aug 30 22:52:44.600: %RADIUS-4-RADIUS_ALIVE: RADIUS server 1.8.91.8:1645,1646 is being
marked alive.
BWG#
*Aug 30 22:52:46.032: AGW-DHCP: <100022270001>PROCESS Downstream DHCP to MS:IP
Src=2.2.2.2, IP Dst=2.2.2.2, len=308
*Aug 30 22:52:46.032: AGW-DHCP: <100022270001>PROCESS Downstream Decode DHCP
OFFER:len=300, ci=0.0.0.0, gi=2.2.2.2, si=0.0.0.0, yi=2.2.0.89, sfid=0x9(9)
*Aug 30 22:52:46.032: AGW-DHCP: <100022270001>PROCESS Downstream Options for DHCP OFFER :
53(1),54(4),51(4),58(4),59(4),1(4),82(14),255(0),
*Aug 30 22:52:46.032: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Received 328 bytes pak
contiguous pak, size 328
         45 00 01 48 00 0A 00 00 FF 11 BA 9B 00 00 00 00
         FF FF FF FF 00 43 00 44 01 34 9D 5D 02 01 06 00
         00 00 08 33 00 00 80 00 00 00 00 00 02 02 00 59
         00 00 00 00 00 00 00 00 10 00 22 27 00 01 00 00
         00 00 00 00 00 00 00 00 ...
*Aug 30 22:52:46.032: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Vi2:Sending 356(328) bytes pak, TOS 0X0
*Aug 30 22:52:46.032: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Vi2:GRE packet of 356 bytes
contiguous pak, size 356
         45 00 01 64 00 0D 00 00 FF 2F AB 13 02 02 02 02
         0A 01 01 46 20 00 08 00 00 00 00 05 45 00 01 48
         00 0A 00 00 FF 11 BA 9B 00 00 00 00 FF FF FF FF
         00 43 00 44 01 34 9D 5D 02 01 06 00 00 00 08 33
         00 00 80 00 00 00 00 00 ...
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>CEF Upstream Et0/0:Rcvd
GRE 646 bytes with flags crKss, version 0x0, procotol 0x800
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>CEF Upstream Vi2:Rcvd
604(646) byte pak, TOS 0X0
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream
Et0/0:Rcvd GRE 646 bytes with flags crKss, version 0x0, procotol 0x800
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream Et0/0
Inner pak 646 bytes pak(retval 0x0, is_ours 1)
contiguous pak, size 646
         AA BB CC 03 34 00 AA BB CC 03 35 00 08 00 45 00
         02 78 00 12 00 00 FD 2F AB FA 0A 01 01 46 02 02
         02 02 20 00 08 00 00 00 00 05 45 00 02 5C 00 4D
         00 00 FE 11 B0 3A 05 05 05 05 FF FF FF FF 00 44
         00 43 02 48 3D 19 01 01 ...
*Aug 30 22:52:46.040: AGW-DHCP: <100022270001>PROCESS Upstream DHCP from MS:IP
Src=5.5.5.5, IP Dst=255.255.255.255, gi=0.0.0.0, len=584, sfid=ox9
*Aug 30 22:52:46.040: AGW-DHCP: <100022270001>PROCESS Upstream Decode DHCP
REQUEST:len=576, ci=0.0.0.0, gi=0.0.0.0, si=0.0.0.0, yi=0.0.0.0, sfid=0x9(9)
*Aug 30 22:52:46.040: AGW-DHCP: <100022270001>PROCESS Upstream Options for DHCP REQUEST :
53(1),57(2),61(7),54(4),50(4),51(4),12(13),55(5),255(0),
*Aug 30 22:52:46.040: AGW-DHCP: <100022270001>PROCESS Upstream Added Option 82 Subscriber
ID: 1000.2227.0001, Circuit ID: 9
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream
Vi2:Rcvd 620(662) bytes pak, TOS 0X0
*Aug 30 22:52:46.040: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Upstream GRE
pak Rcvd 620(662) bytes pak
contiguous pak, size 620
         45 00 02 6C 00 4D 00 00 FE 11 A9 D2 02 02 02 02
         0B 01 01 5D 00 44 00 43 02 58 9E F9 01 01 06 00
         00 00 08 33 00 00 80 00 00 00 00 00 00 00 00 00
         00 00 00 00 02 02 02 02 10 00 22 27 00 01 00 00
         00 00 00 00 00 00 00 00 ...
*Aug 30 22:52:46.044: AGW-DHCP: <100022270001>PROCESS Downstream DHCP to MS:IP
Src=2.2.2.2, IP Dst=2.2.2.2, len=313
*Aug 30 22:52:46.044: AGW-DHCP: <100022270001>PROCESS Downstream Decode DHCP ACK:len=305,
ci=0.0.0.0, gi=2.2.2.2, si=0.0.0.0, yi=2.2.0.89, sfid=0x9(9)
```

```
*Aug 30 22:52:46.044: AGW-DHCP: <100022270001>PROCESS Downstream Options for DHCP ACK :
53(1),54(4),51(4),58(4),59(4),12(13),1(4),82(14),255(0),
*Aug 30 22:52:46.044: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Received 333 bytes pak
contiguous pak, size 333
         45 00 01 4D 00 0B 00 00 FF 11 BA 95 00 00 00 00
         FF FF FF FF 00 43 00 44 01 39 13 30 02 01 06 00
         00 00 08 33 00 00 80 00 00 00 00 00 02 02 00 59
         00 00 00 00 00 00 00 00 10 00 22 27 00 01 00 00
         00 00 00 00 00 00 00 00 ...
*Aug 30 22:52:46.044: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Vi3:Sending 361(333) bytes pak, TOS 0X0
*Aug 30 22:52:46.044: AGW-GRE: <100022270001><(DG)-10.1.1.70><F[5]>PROCESS Downstream
Vi3:GRE packet of 361 bytes
BWG#
contiguous pak, size 361
         45 00 01 69 00 0E 00 00 FF 2F AB 0D 02 02 02 02
         0A 01 01 46 20 00 08 00 00 00 00 05 45 00 01 4D
         00 0B 00 00 FF 11 BA 95 00 00 00 00 FF FF FF FF
         00 43 00 44 01 39 13 30 02 01 06 00 00 00 08 33
         00 00 80 00 00 00 00 00 ...
*Aug 30 22:52:46.044: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Flow
Signal:Sending UDP 274 bytes pak
*Aug 30 22:52:46.048: AGW-UDP: <100022270001><(SU)-10.1.1.70>PROCESS Downstream Flow
Signal:Sending UDP 28 bytes pak
```

Here is an example of ARP related debug information:

```
Router# debug wimax agw switching arp
*Feb
*Apr 30 20:14:40.031: AGW-ARP: <00322346ABCD>PROCESS Upstream ARP from MS:IP
Src=2.2.0.145, IP Dst=2.2.2.2, MAC Src=0032.2346.abce, MAC Dst=ffff.ffff.ffff, sfid=0x1
*Apr 30 20:14:40.031: AGW-ARP: <00322346ABCD>PROCESS Upstream Decode ARP REQUEST:IP
Src=2.2.0.145, IP Dst=2.2.2.2, MAC Src=0032.2346.abce, MAC Dst=ffff.ffff.ffff,
*Apr 30 20:14:40.031: AGW-ARP: <00322346ABCD>PROCESS Downstream Decode ARP REPLY:IP
Src=2.2.2.2, IP Dst=2.2.0.145, MAC Src=0000.0c07.ac01, MAC Dst=0032.2346.abce,
*Apr 30 20:14:40.031: AGW-ARP: <00322346ABCD><(DG)-10.1.1.70><F[1]>PROCESS Downstream
Vi2:Sending 82(28) bytes pak, TOS 0X0

*Apr 30 20:14:40.031: AGW-ARP: <00322346ABCD><(DG)-10.1.1.70><F[1]>PROCESS Downstream
Vi2:GRE packet of 82 bytes
contiguous pak, size 82
         45 00 00 52 03 72 00 00 FF 2F A8 C0 02 02 02 02
         0A 01 01 46 20 00 65 58 00 00 00 01 00 32 23 46
         AB CE 00 00 0C 07 AC 01 81 00 00 03 00 1C AA AA
         03 00 00 00 08 06 00 01 08 00 06 04 00 02 00 00
         0C 07 AC 01 02 02 02 02 ...
```

Example of ARP Debugs for Static Host reject when host limit reached and idle timer not expired:

```
Router# debug wimax agw switching arp

*Nov 28 05:12:56.909: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.220, IP Dst=11.1.3.3, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,

sfid=0x1F
*Nov 28 05:12:56.909: AGW-ARP: <100022ED1111>PROCESS Upstream Decode ARP REQUEST:IP

Src=11.1.3.220, IP Dst=11.1.3.3, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff, *Nov 28
05:12:56.909: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.3, IP Dst=11.1.3.220, sfid=0x1F, host create failed.
```

Example of ARP Debugs for Static Host accept when host limit reached but idle timer expired

```
Router# debug wimax agw switching arp

*Apr 30 20:21:17.767: AGW-ARP: <00322346ABCD>PROCESS Upstream ARP from MS:IP
*Apr 30 21:25:01.903: AGW-ARP: <00322346ABCD>PROCESS Upstream ARP from MS:IP
Src=2.2.0.153, IP Dst=2.2.2.2, MAC Src=0032.2346.abd6, MAC Dst=ffff.ffff.ffff, sfid=0x3
*Apr 30 21:25:01.903: AGW-ARP: <00322346ABCD>PROCESS Upstream Decode ARP REQUEST:IP
Src=2.2.0.153, IP Dst=2.2.2.2, MAC Src=0032.2346.abd6, MAC Dst=ffff.ffff.ffff,
*Apr 30 21:25:01.903: AGW-ARP: <00322346ABCD>PROCESS Downstream Decode ARP REPLY:IP
Src=2.2.2.2, IP Dst=2.2.0.153, MAC Src=0000.0c07.ac01, MAC Dst=0032.2346.abd6,
*Apr 30 21:25:01.903: AGW-ARP: <00322346ABCD><(DG)-10.1.1.70><F[2]>PROCESS Downstream
Vi2:Sending 82(28) bytes pak, TOS 0X0

*Apr 30 21:25:01.903: AGW-ARP: <00322346ABCD><(DG)-10.1.1.70><F[2]>PROCESS
Downstream Vi2:GRE packet of 82 bytes
contiguous pak, size 82
         45 00 00 52 01 5D 00 00 FF 2F AA D5 02 02 02 02
         0A 01 01 46 20 00 65 58 00 00 00 01 00 32 23 46
         AB D6 00 00 0C 07 AC 01 81 00 00 03 00 1C AA AA
         03 00 00 00 08 06 00 01 08 00 06 04 00 02 00 00
         0C 07 AC 01 02 02 02 02 ...
```

Example of ARP Debugs when Receiving an Invalid ARP Request:

```
Router# debug wimax agw switching arp

*Nov 28 05:14:49.205: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.220, IP Dst=255.255.255.255, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,

sfid=0x1F
*Nov 28 05:14:49.205: AGW-ARP: <100022ED1111>PROCESS Upstream Decode ARP REQUEST:IP

Src=11.1.3.220, IP Dst=255.255.255.255, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,
*Nov 28 05:14:49.205: AGW-ARP: <100022ED1111>PROCESS Upstream IP Src=11.1.3.220, IP

Dst=255.255.255.255, Received Invalid ARP request. BWG does not send reply pu-asn# *Nov 28
05:14:49.205: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.220, IP Dst=255.255.255.255, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,

sfid=0x1F, decode failed
```

Example of ARP Debugs when Receiving a Gratuitous ARP:

```
Router# debug wimax agw switching arp

*Nov 28 05:18:45.829: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.220, IP Dst=11.1.3.220, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,

sfid=0x1F
*Nov 28 05:18:45.829: AGW-ARP: <100022ED1111>PROCESS Upstream Decode ARP REQUEST:IP

Src=11.1.3.220, IP Dst=11.1.3.220, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff, *Nov 28
05:18:45.829: AGW-ARP: <100022ED1111>PROCESS Upstream IP Src=11.1.3.220, IP

Dst=11.1.3.220, Received Gratuitous ARP Request. BWG does not send reply *Nov 28
05:18:45.829: AGW-ARP: <100022ED1111>PROCESS Upstream ARP from MS:IP

Src=11.1.3.220, IP Dst=11.1.3.220, MAC Src=1000.22ed.111a, MAC Dst=ffff.ffff.ffff,

sfid=0x1F, decode failed
```

debug wimax agw vtemplate

To display BWG vtemplate information, use the **debug wimax agw vtemplate** command in Privileged EXEC mode. Use the **no** version of the command to turn off debugging.

debug wimax agw vtemplate [**events** | **errors**]

no debug wimax agw vtemplate

Syntax Description

events	Displays information on Virtual-template related events.
errors	Displays information on Virtual-template related errors.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example displays BWG vtemplate information:

```
router#debug wimax agw vtemplate events
```

default-gateway

To configure the default-gateway under the PMIP profile configuration, use the default-gateway command. Use the **no** form of this command to disable this function.

default-gateway *ip-address*

[no] default-gateway *ip-address*

Syntax Description

ip-address	The IPv4 address of the default gateway.

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration (config).

Command History

Release	Modification
12.4(24)YG2	This command was introduced.

Examples

The following example shows how to configure the default-gateway under a PMIP profile configuration:

```
wimax agw pmip profile pmip1
      proxy-mn
        dns-server primary  10.1.1.1 secondary 10.1.1.2
        default-gateway 10.1.1.3
```

dhcp gateway address

To specify the IP address of the DHCP relay which the server is supposed to communicate with in the BWG, use the **dhcp gateway address** command in user group configuration mode. Use the **no** form of the command to revert to the default gateway IP address.

dhcp gateway address *gateway-address*

no dhcp gateway address *gateway-address*

Syntax Description

gateway-address	Specifies the IP address of the DHCP Relay. The IP address specified as the gateway address must be the IP address of the BWG Virtual-Template (either primary or one of the secondary IP addresses).

Defaults

By default the BWG VT primary IP address is used.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The IP address specified as the gateway address must be the IP address of the BWG Virtual-Template (either primary or one of the secondary IP addresses).

Examples

The following example illustrates how to configure DHCP relay using the **dhcp gateway address** command:

```
Router(config-gw-ug)# dhcp gateway address gateway-address
```

Related Commands

Command	Description
dhcp server primary	Specifies the external DHCP server used for DHCP IP address allocation.

dhcp release relay-only

To enable the BWG to only handle relayed DHCP RELEASEs from DHCP clients (the BWG will no longer generate a DHCP RELEASE on behalf of subscriber's hosts), use the **dhcp release relay-only** command in User group configuration sub mode. Use the no form of the command to disable this feature.

dhcp release relay-only

no dhcp release relay-only

Syntax Description

There are no keywords or arguments for this command.

Defaults

The default setting is that this command is disabled.

Command Modes

User group configuration sub mode.

Command History

Release	Modification
12.4(15)XL4	This command was introduced.

Examples

The following example enables the command:

```
router(config-gw-ugl)# dhcp release relay-only
```

dhcp server primary

To specify the external DHCP servers for IP address allocation, use the **dhcp server primary** command in user group configuration mode. Use the **no** form of the command to remove the DHCP server configuration.

dhcp server primary *primary-address* **[backup** *backup-address***] [vrf]**

no dhcp server primary *primary-address* **[backup** *backup-address***] [vrf]**

Syntax Description

primary-address	Specifies the IP address of the primary DHCP server
backup *backup-address*	Specifies the IP address of the backup DHCP server.
vrf	Indicates if the address is in the VRF scope.

Defaults

There are no default values.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The IP address specified as the gateway address must be the IP address of the BWG Virtual-Template (either primary, or one of the secondary IP addresses).

Examples

The following example illustrates how to configure DHCP servers using **dhcp server primary** command:

```
router(config-gw-ug)# dhcp server primary 10.10.10.10 backup 10.10.10.11
```

direction

To specify the direction of the service-flow the configuration is done, and to enter a subcommand mode use the **direction** command in service flow configuration subcommand mode. Use the **no** version of this command to remove the corresponding configuration from the direction specified.

direction {**uplink** | **downlink**}

Syntax Description

uplink	Service Flow Uplink direction configuration commands.
downlink	Service Flow Downlink direction configuration commands.

Defaults

There are no default values.

Command Modes

Service flow configuration subcommand mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example specifies the service flow direction to the uplink:

```
router(config-gw-sf)#direction uplink
```

dns-server

To configure the DNS server under a PMIP profile configuration use the dns-server command. Use the **no** form of this command to disable this function.

dns-server primary *ip-address* **secondary** *ip-address*

no dns-server primary *ip-address* **secondary** *ip-address*

Syntax Description

ip-address	The IPv4 address of the primary or secondary DNS server.

Defaults

There are no default values.

Command Modes

Privileged EXEC configuration (config)

Command History

Release	Modification
12.4(24)YG2	This command was introduced.

Examples

The following example shows how to configure the primary and secondary dns-servers under a PMIP profile configuration:

```
wimax agw pmip profile pmip1
      proxy-mn
        dns-server primary  10.1.1.1 secondary 10.1.1.2
```

encapsulation agw

To clone a Virtual-Access interface of encapsulation type BWG, use the **encapsulation agw** command in Virtual-Template configuration mode.

encapsulation agw

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default values.

Command Modes

Interface configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example enables you to clone a Virtual-Access interface of encapsulation type BWG:

```
router(config)# interface Virtual-Template1
ipaddress 2.2.2.2 255.255.0.0

router(config-if)# encapsulation agw
ip mtu 1440
no keepalive
```

The Gi address is picked from the Virtual Address by default. It can be overridden by the User-Group Configuration.

host-overflow

To enable the DHCP Host Caching feature and configure the size of the cache list and the idle timer, use the **host-overflow** command in user group configuration submode. Use the no form of the command to disable this feature.

host-overflow [**size** *1-100*] [**min-idle** *1- 60*]

no host-overflow [**size** *1-100*] [**min-idle** *1- 60*]

Syntax Description

size *1-100*	Specifies the size of the cache list. The range is 1-100, the default value is 50.
min-idle *1- 60*	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 range is 1-60, the default value is 5, represented in minutes.

Defaults

The **size** default value is 50. The **min-idle** timer value default value is 5 minutes.

Command Modes

User group configuration sub mode.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Usage Guidelines

- 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.

Examples

The following example enables the default values:

```
router(usr-grp)#host-overflow size 50 min-idle 5
```

ip-addr

To specify the base stations that are allowed to connect to the BWG, and the base station group they belong to, use the **ip-addr** command in base-station group configuration sub mode. Use the **no** form of the command to revert to the default behavior.

ip-addr *start-ip-addr end-ip-addr*

no ip-addr

Syntax Description

start-ip-addr	Specifies the start IP address.
end-ip-addr	Specifies the end IP address.

Defaults

By default, all IP addresses are allowed for the base-station group.

Command Modes

Base-station group configuration sub mode.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

Here is an example of the **ip-addr** command:

```
router(config-wimax-agw-bs)# ip-addr 11.1.27.1 11.1.27.255
```

ip access-group

To specify IPv4 access permissions between a subscriber and an external host through the BWG at a particular access point, use the **ip access-group** command in user group configuration mode. Use the **no** form of the command to disable the input access list.

access-group *access-group-number* {**in** | **out** | **passthru**}

Syntax Description

access-group-number	Specifies the access group number.
in	Filters packets going to the subscriber (upstream).
out	Filters packets coming from the subscriber (downstream).
passthru	Packets passing the filter rule defined by the ACL are allowed to pass.

Defaults

There are no default values.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example enables access group number 4:

```
router# ip access-group 4 in
```

ip redirect traffic

To enable the BWG to redirect all upstream traffic to the configured next hop address, use the **ip redirect traffic** command in wimax gateway user-group submode. Use the **no** form of the command to disable this feature.

ip redirect traffic all *address*

no ip redirect traffic

Syntax Description

all *address*	Specifies that all ip traffic flows with the specified address are redirected.

Defaults

There are no default values.

Command Modes

Gateway user group configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is an example of the **ip redirect traffic** command:

```
Router(config)#wimax agw user group-list wimax
Router(config-gw-ugl)# user-group domain cisco.com
Router(config-gw-ug)#ip redirect ?
  traffic  User group IP redirect traffic configuration commands
Router(config-gw-ug)#ip redirect traffic ?
  all  Redirect all traffic

Router(config-gw-ug)#ip redirect traffic all ?
  A.B.C.D  Redirect IP address

Router(config-gw-ug)#ip redirect traffic all 10.1.1.5
Router(config-gw-ug)#end


wimax agw user group-list wimax
 user-group domain cisco.com
  sla profile-name silver
  ip redirect traffic all 10.1.1.5
  ip static-allowed
```

ip route aggregate

To aggregate routes automatically based on the mask returned by servers if set to auto, use the **ip route aggregate** command in global configuration mode. Use the **no** form of the command to disable route aggregation.

ip route aggregate {**A.B.C.D** | **auto**}

no ip route aggregate {**A.B.C.D** | **auto**}

Syntax Description

A.B.C.D	Specifies a route based on a specific IP prefix and mask. When specified, only those routes are aggregated to one route.
auto	Specifies aggregate routes automatically based on the mask returned by servers.

Defaults

There is no default value.

Command Modes

Global configuration mode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

The following example configures an auto aggregated route:

```
router(config)# wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  sla profile-name gold
  dhcp server primary 12.1.1.2
!
user-group domain cisco.com
  aaa accounting method-list agw
  sla profile-name gold
  ip static-allowed
  ip route aggregate auto
```

ip static-allowed

To allow the creation of static hosts for sessions that are part of a specific user-group, use the **ip static-allowed** command in usergroup configuration mode. Use the **no** form of the command to disable this feature.

ip static-allowed

no ip static-allowed

Syntax Description

There are no keywords or arguments.

Defaults

The default value is no ip static hosts are allowed.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

The following example allows static hosts for 2 separate user groups:

```
user-group domain cisco.com
  aaa accounting method-list agw
  sla profile-name gold
  ip static-allowed
  ip route aggregate auto
!
user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name gold
  ip static-allowed
  user auto-provisioning
  proxy realm cisco.com password ciscoway
```

maximum-latency

To configure the time period between the reception of a packet by the BS or MS on its network interface, and the delivery of the packet to the RF Interface of the peer device, use the **maximum-latency** subcommand in service flow qos info configuration submode. Use the **no** form of the command to disable this feature.

maximum-latency *maximum-latency-value*

Syntax Description

maximum-latency-value	Specifies the time between the reception of a packet by the BS or MS on its network interface, and the delivery of the packet to the RF Interface of the peer device. Default value is 0.

Defaults

Default value is 0.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If configured, this parameter represents a service commitment (or admission criteria) at the BS or MS and is guaranteed by the BS or MS. A BS or MS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.

Examples

The following examples configure a maximum latency value of 1 and 11:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
```

```
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

maximum-traffic-burst

To configure the maximum burst size that the service flow can accommodate, use the **maximum-traffic-burst** subcommand in service flow qos information configuration submode. Use the **no** form of the command to disable this feature.

maximum-traffic-burst *maximum-traffic-burst-value*

Syntax Description

maximum-traffic-burst-value	Specifies the maximum burst size of the service flow. Default values is 0.

Defaults

Default values is 0.

Command Modes

Service flow qos information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

Since the physical speed of ingress/egress ports, the air interface, and the backhaul are greater than the maximum-sustained-traffic-rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service. This assumes the service is not currently using any of its available resources.

Examples

The following examples configure a maximum traffic burst size of 2 and 21:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
```

```
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

maximum-traffic-rate-sustained

To define the peak information rate of the service flow, use the **maximum-traffic-rate-sustained** subcommand in service flow qos information configuration submode. Use the **no** form of the command to disable this feature.

maximum-traffic-rate-sustained *maximum-traffic-rate-sustained-value*

Syntax Description

maximum-traffic-rate-sustained-value	Specifies the peak information rate of the service flow. The rate is expressed in bits per second, and pertains to the SDUs at the input of the system. The range is *0-4294967295* measured in bits per second

Defaults

There is no default value.

Command Modes

Service flow qos information configuration subcommand.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a boundary, not a guarantee that the rate is available.

Examples

The following example specifies different **maximum-traffic-rate-sustained** values:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
```

```
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

media-flow-type

To configure the parameter that describes the application type that is used as a hint in admission decisions (for instance, VoIP, video, PTT, gaming, etc.), use the **media-flow-type** subcommand in service flow qos information configuration submode. Use the **no** form of the command to disable this functionality.

media-flow-type *media-flow-type-hex-string*

no media-flow-type

Syntax Description

media-flow-type-hex-string	Specifies the application type that is used as a hint in admission decisions. Application types include VoIP, video, PTT, gaming, etc.

Defaults

There are no default values.

Command Modes

Service flow qos information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example configures two different media-flow-type values:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
```

```
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

minimum-traffic-rate-reserved

To specify the minimum rate reserved for a specific service flow use the **minimum-traffic-rate-reserved** subcommand in service flow qos information configuration submode. Use the **no** form of the command to disable this feature.

minimum-traffic-rate-reserved *minimum-traffic-rate-reserved-value*

no minimum-traffic-rate-reserved *minimum-traffic-rate-reserved-value*

Syntax Description

minimum-traffic-rate-reserved-value	Specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second, and specifies the minimum amount of data transported on behalf of the service flow when averaged over time.

Defaults

There are no default values.

Command Modes

Service flow qos information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The specified rate is only honored when sufficient data is available for scheduling. When sufficient data does not exist, the available data is transmitted as soon as possible.

Examples

The following example configures a *minimum-traffic-rate-reserved-value* of *4*:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9
```

pak-classify-rule

To specify which packet classification rule profile is associated under the corresponding cs-type, use the **pak-classify-rule** subcommand in service flow direction cs-type configuration submode. Use the **no** version of the command to remove the packet classification rule.

pak-classify-rule *pak-classify-rule-profile-name*

no pak-classify-rule *pak-classify-rule-profile-name*

Syntax Description

pak-classify-rule-profile-name	Specifies the name of the packet classification rule profile.

Defaults

There are no default values.

Command Modes

Service flow direction configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example specifies a packet classification rule profile named “uplink2”:

```
router(config-gw-sf-dir)#pak-classify-rule uplink2
```

policy-transmission-request

To specify options for PDU formation, for uplink service flows, and to configure restrictions on the types of bandwidth request options that may be used, use the **policy-transmission-request** subcommand in service flow QoS information configuration submode. An attribute is enabled by setting the corresponding bit position to 1. Use the **no** form of the command to disable this functionality.

policy-transmission-request *policy-transmission-request-value*

no policy-transmission-request *policy-transmission-request-value*

Syntax Description

policy-transmission-request-value	Specifies the value of the policy transmission request. Range of values is *0-4294967295* 32-bit bitmask. • Bit #0 Service flow shall not use broadcast bandwidth request opportunities.(Uplink only) • Bit #1 Reserved. • Bit #2 The service flow shall not piggyback requests with data (Uplink only). • Bit #3 The service flow shall not fragment data. • Bit #4 The service flow shall not suppress payload headers (CS parameter). • Bit #5 The service flow shall not pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 The service flow shall not include CRC in the MAC PDU. • All other bit positions are reserved.

Defaults

There are no default values.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

An attribute is enabled by setting the corresponding bit position to 1.

Examples

The following example illustrates how to configure the **policy-transmission-request** subcommand:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
```

```
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

precedence

To specify the precedence of the cs-type under the direction which it is configured, use the **precedence** command in service flow direction cs-type submode. The **precedence** is used as a tie-breaker when an MS can support more than one cs-type. Use the **no** version of the command to remove the precedence information from the corresponding cs-type.

precedence *1-2*

no precedence

Syntax Description

1-2	Specifies the precedence of the cs-type under which it is configured. The precedence is used as a tie-breaker when an MS can support more than one cs-type. A larger value indicates a higher priority. The default value is **1**.

Defaults

The default value is **1**.

Command Modes

Service flow direction cs-type configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Examples

The following example specifies a packet classification rule profile named “uplink2” with different precedence set for cs-type ip-cs and cs-type ethernet-cs:

```
wimax agw service-flow profile isf
 direction downlink
  cs-type ip-cs
   pak-classify-rule isf-classifier-downlink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-downlink
   precedence 2
  qos-info isf-qos-downlink
 !
 direction uplink
  cs-type ip-cs
   pak-classify-rule isf-classifier-uplink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-uplink
   precedence 2
   vlan 2 vrf vrf_1
   vlan range 3 10 vrf vrf_2
   vrf-default vrf_1
  qos-info isf-qos-uplink
```

priority

To set the priority of a packet classification rule under the profile, use the **priority** subcommand in packet classify rule submode. Use the **no** form of the command to unconfigure the priority of the packet classification rule.

priority {ip | vlan | ethernet} permit {*0-255* | **gre** | **tcp** | **icmp** | **udp** | **ip**} {*src-address src-mask* | **any** | **host** *src-address*} [**range** *src-port-low* [*src-port-high*] {*dst-address dst-mask* | **any** | **host** *dst-address*} [**range** *dst-port-low* [*dst-port-high*][**tos** *tos-low tos-mask tos-high*]

no priority

Syntax Description

ip | vlan | ethernet	The types of packet classification rules to apply priority values to.
permit	Specifies the type of permit, IPv4, VLAN, or Ethernet.
0-255	Specifies the priority of the packet classification rule.
gre	Specifies **gre** as the packet classification.
tcp	Specifies **tcp** as the packet classification.
icmp	Specifies **icmp** as the packet classification.
udp	Specifies **udp** as the packet classification.
ip	Specifies **ip** as the packet classification.
src-address	Specifies the source address.
src-mask	Specifies the source mask.
any	Specifies any address or mask.
host	Specifies the host source address.
src-port-low	Specifies the source low port value.
src-port-high	Specifies the source high port value.
dst-address	Specifies the destination address.
dst-port-low	Specifies the lowest port value in a range of destination port values.
dst-port-high	Specifies the highest port value in a range of destination port values.
dst-mask	Specifies the dst mask.
tos-low	Specifies the tos low value.
tos-mask	Specifies the tos mask.
tos-high	Specifies the tos high value.

Defaults

The default is to use the ISF (Initial Service Flow) to send the packet.

Command Modes

Packet classify rule configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The Cisco BWG currently supports IPv4, Ethernet and VLAN related rules.

Each packet classification rule should have a unique priority associated with it. Each flow can have zero or more classifier rules. The higher the priority, the higher is the rule precedence. If a packet matches a rule, the corresponding flow is chosen to send that packet.

Examples

The following example illustrates the various options under the **priority** command:

```
router(config-gw-pak-classify-rule-pr)#priority
IPv4 classifiers===>
ip permit {0-255 | gre | tcp | icmp | udp | ip} {src-address src-mask | any | host
src-address} [range src-port-low [src-port-high] {dst-address dst-mask | any | host
dst-address} [range dst-port-low [dst-port-high] [tos tos-low tos-mask tos-high]
Ethernet related classifiers ===>
ethernet permit {src_mac src_mac_mask | any} {dst_mac dst_mac_mask | any} {0-FFFF | any |
arp | ipv4}]

VLAN related classifiers ===>
vlan permit {2-4095 | any } priority { 0-7 | any | range #start #end }
```

Here is an example of the **priority** command:

```
wimax agw service-flow pak-classify-rule profile sec1-classifier-uplink
 priority 0
  ipv4 permit ip any any
  ethernet permit any any any
  vlan any priority any
 !
 priority 1
  vlan 300 priority 4 7
 !
 priority 2
  ethernet permit 0032.00AE.0023 ffff.ffff.ffff any arp
 !
 priority 3
  ipv4 permit ip 2.2.2.2 255.255.255.0 192.168.102.0 /24 tos 0 255 100
 !
 priority 4
  ethernet permit any 0032.00AE.0023 ffff.ffff.ffff 8100
  vlan permit 900 priority 4
 !
 priority 5
  ipv4 permit ip 2.2.2.2 255.255.255.0 192.168.102.0 /24 tos 0 255 100
  ethernet permit 001C.B046.041B ffff.ffff.0000 0032.00AE.0023 ffff.0000.0000 ipv4
  vlan permit 300 priority range 4 7
```

proxy realm

To specify how the BWG should populate the RADIUS Access Request message for users who support PPP/PAP methods of authentication, use the **proxy realm** sub command in unauthenticated user group mode. Use the **no** form of the command to disable this feature.

Note Configuring proxy-realm for EAP users is possible but serves no purpose.

proxy realm *realm-name* **password** *password*

no proxy realm *realm-name* **password** *password*

Syntax Description

realm-name	Specifies the name of the realm.
password *password*	Specifies the password.

Defaults

There are no default values.

Command Modes

User group configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

If configured, the user name and password sent in the Access-Request (since the user is authenticated based on the PAP of PPP) will be set to *mac@realm*, and given a password respectively.

If the proxy realm is not configured, the user name will be *mac,* and *cisco* will be used as password in the Access-Request.

Examples

The following example illustrates how to configure the **proxy realm** command:

```
router(config)#user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name gold
  ip static-allowed
  user auto-provisioning
  proxy realm cisco.com password ciscoway
```

qos-info

To specify which QoS information profile is associated under the corresponding direction, use the **qos-info** subcommand in service flow direction configuration submode. Use the **no** form of the command to remove the QoS information from the corresponding direction.

qos-info *qos-profile-name*

no qos-info *qos-profile-name*

Syntax Description

qos-profile-name	Specifies the name of the QoS information profile.

Defaults

There are no default values.

Command Modes

Service flow direction configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example illustrates how to configure the **qos-info** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9
```

radius-server vsa send accounting wimax

To enable WiMAX RADIUS VSAs to be sent in accounting requests (Start, Int, Stop) from the BWG, use the **radius-server vsa send accounting wimax** command in global configuration mode. Use the **no** form of the command to disable this feature.

radius-server vsa send accounting wimax

no radius-server vsa send accounting wimax

Syntax Description

There are no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example enables RADIUS VSAs to be sent in accounting requests from the BWG:

```
Router(config)#radius-server vsa send accounting wimax
```

radius-server vsa send authentication wimax

To enable the WiMAX RADIUS VSAs to be sent out in authentication requests (Access-Request) from the BWG, use the **radius-server vsa send authentication wimax** command in global configuration mode. Use the **no** form of the command to disable this feature.

radius-server vsa send authentication wimax

no radius-server vsa send authentication wimax

Syntax Description

There are no keywords or arguments.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example enables the BWG to send RADIUS VSAs out in authentication requests:

```
Router(config)#radius-server vsa send authentication wimax
```

reduced-resources-code

To configure the code that indicates that the requesting entity will accept reduced resources if the requested resources are not available, use the **reduced-resources-code** subcommand in service flow QoS information configuration submode. Use the **no** form of the command to disable this function.

reduced-resources-code *reduced-resources-code-value*

no reduced-resources-code

Syntax Description

reduced-resources-code -value	Specifies the value of the reduction in resources.

Defaults

There is no default value.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example illustrates how to configure the **reduced-resources-code** command:

```
router(config-gw-sf-qos-info)#reduced-resources-code reduced-resources-code-value
```

reference-point r6

To configure various R6 parameters, including keepalive, base station path and response configuration commands, use the **reference-point r6** subcommand in base station group configuration submode. Use the **no** form of the command to disable these parameters.

reference-point r6 [**keepalive** | **path** {**purge-timeout** *value*} | **response** | **udp ip dscp** *value* | **session-maturity-period** *value*]

no reference-point r6

Syntax Description

keepalive	Enables the BWG-BS keepalive feature.
path	Specifies the WiMAX BWG BS R6 reference point base station path.
purge-timeout *value*	Specifies WiMAX BWG BS R6 reference point path purge timeout value. As soon as the last session associated with the BS path goes away, the path purge timer is started to remove the path after the timer expiry. The timeout value is measured in minutes. If the purge timer is not configured, the default value is 24 hours.
response	Enables WiMAX BWG BS R6 reference point response configuration commands.
udp ip dscp *value*	Specifies the DSCP marking for R6 signaling messages. Range is [*0-63*]. Default is 48.
session-maturity-period *value*	Specifies the time after which the session is considered matured. Range is [1-30] seconds. Default is 5 seconds

Defaults

The timeout value is measured in minutes. If the purge timer is not configured, the default value is 24 hours.

Command Modes

Base station group configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(24)YG	**session-maturity-period** sub-option was introduced.

Examples

The following example illustrates how to configure the **reference-point r6** command:

```
BWG(config-wimax-agw-bs)#ref r6 ?
  keepalive                Enable AGW-BS keepalive feature
  path                     WiMAX AGW BS R6 reference point base station path
  response                 WiMAX AGW BS R6 reference point response
                           configuration commands
  session-maturity-period  WiMAX AGW BS R6 reference point time after session
                           considered mature
  udp                      WiMAX AGW BS R6 reference point UDP configuration
                           commands
```

```
BWG(config-wimax-agw-bs)#ref r6 udp ip dscp ?
  <0-63>  WiMAX AGW BS R6 reference point UDP IP set DSCP to value (default 48)

BWG(config-wimax-agw-bs)#ref r6 session-maturity-period ?
  <1-30>  Session maturity period value (default 5 seconds)
```

reference-point r6 keepalive max-failures-allowed

To configure the the number of times the BWG attempts to resend the KeepAlive request before tearing down the session, use the **reference-point r6 keepalive max-failures-allowed** command in base station submode configuration. Use the **no** form of the command to disable this feature.

reference-point r6 keepalive max-failures-allowed *maximum-retries*

no reference-point r6 keepalive max-failures-allowed *maximum-retries*

Syntax Description

maximum-retries	Specifies the number of times the BWG attempts to resend the KeepAlive request before tearing down the session.

Defaults

The default setting is disabled.

Command Modes

Base station configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Examples

The following example illustrates the default behavior for the **reference-point r6 keepalive max-failures-allowed** command:

```
wimax agw base-station group default
  reference-point r6 keepalive timeout 30
  reference-point r6 response retransmit 10
  reference-point r6 response timeout 10
```

reference-point r6 keepalive timeout

To specify the keepalive interval in seconds, use the **reference-point r6 keepalive timeout** command in base station configuration mode. Use the **no** form of the command to disable this command.

reference-point r6 keepalive timeout *interval*

no reference-point r6 keepalive timeout *interval*

Syntax Description

interval	Specifies the keepalive interval in seconds. The default value is 60 seconds.

Defaults

The default setting is 60 seconds.

Command Modes

Base station configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Examples

The following example illustrates the default behavior for the **reference-point r6 response keepalive timeout** command:

```
wimax agw base-station group default
  reference-point r6 keepalive timeout 30
  reference-point r6 response retransmit 10
  reference-point r6 response timeout 10
```

reference-point r6 response retransmits

To specify the number of times the BWG attempts to re-send R6 messages when it does not receive a response from the BS, use the **reference-point r6 response retransmits** command in base station configuration submode. Use the **no** form of the command to disable this feature.

reference-point r6 response retransmits *retransmit value*

no reference-point r6 response retransmits

Syntax Description

retransmit value	Specifies the number of times the AGW attempts to resend R6 messages after no response from the BS. The default value is 5.

Defaults

The default value is 5.

Command Modes

Base station configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The action taken on the maximum retries being reached depends on the timer that expired.

Examples

The following example illustrates the default behavior for the **reference-point r6 response retransmits** command:

```
Router(bs-config)#reference-point r6 response retransmits 5
```

reference-point r6 response timeout

To configure the amount of time the BWG waits for a response from the BS after a request has been sent, use the **reference-point r6 response timeout** command in base station configuration submode. Use the **no** form of the command to reset the timeout value to its default value of 5 seconds.

reference-point r6 response timeout *timeout value*

no reference-point r6 response timeout *timeout value*

Syntax Description

timeout value	Specifies the amount of time the BWG waits for a response from the BS after a request has been sent. The value is measured in seconds. The default value is 5 seconds.

Defaults

The default value is 5 seconds.

Command Modes

Base station configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If a response is not received within the configured interval, the BWG will retransmit the message until the maximum number of retries configured is reached.

Examples

The following example illustrates that the BWG waits for a response from the BS for 10 seconds:

```
router (config) #reference-point r6 response timeout 10
```

sdu-size

To configure the parameter that represents the number of bytes in the fixed size Service Data Unit (SDU), use the **sdu-size** subcommand in service flow QoS information configuration submode. Use the **no** form of the command to disable this feature.

sdu-size *sdu-size-value*

no sdu-size

Syntax Description

sdu-size-value	Specifies the number of bytes in the fixed size SDU. You can use this parameter for a UGS service flow when the length of IP packets on the data plane is fixed, and known in advance (this is typically the case for flows generated by a specific codec). The range is *0-255*. The default value is 49 bytes.

Defaults

The *sdu-size-value* default value is 49 bytes.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example illustrates how to configure the **sdu-size** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
```

```
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

security subscriber address-filtering ingress

To enable the Ingress address filtering for the subscriber, use the **security subscriber address-filtering ingress** command in user group configuration mode. Use the **no** form of the command to disable Ingress address filtering.

security subscriber address-filtering ingress

no security subscriber address-filtering ingress

Syntax Description

There are no keywords or arguments.

Defaults

The feature is disabled.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

When enabled in the upstream path, the source IP address in the packet is verified against the allowed set of addresses that are allocated to the subscriber, or Hosts behind the subscriber, or Framed route attribute (if downloaded from the AAA server). If the source IP address does not match, the packet is dropped for the subscriber.

Examples

The following example enables the **security subscriber address-filtering ingress** command:

```
Router(config-gw-ug)#security subscriber address-filtering ingress
```

service-flow pre-defined profile

To specify the number of pre-defined service flows to be opened for a subscriber, use the **service-flow pre-defined profile** command in user group configuration mode. Use the **no** form of the command to disable predefined service flows.

service-flow pre-defined {**isf** | **secondary** *secondary-index* | **critical**} **profile** *sf-profile-name* {**cr** | **encap-type none** [**cr** |**vlan-id** *vlan-number*]}

no service-flow pre-defined {**isf** | **secondary** *secondary-index* | **critical**} **profile** *sf-profile-name* {**cr** | **encap-type none** [**cr** |**vlan-id** *vlan-number*]}

Syntax Description

isf	The service flow is assumed to be the initial service flow.
secondary *secondary-index*	Represents the auxiliary service flows for the subscriber.
critical	Marks the service flow as critical.
profile *sf-profile-name*	Enables the service flow profile and profile name of the flow.
cr	Specifies the classification rule.
encap-type none	Specifies that the data encapsulation type is none.
vlan-id *vlan-number*	Specifies the vlan ID number.

Defaults

There are no default values.

Command Modes

SLA profile configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL1	The **cr**, **encap-type none**, and **vlan-id** *vlan-number* keywords and arguments were added.
12.4(24)YG	The **critical** keyword was added.

Usage Guidelines

Currently 1 initial service flow and 1 secondary service flow is allowed per subscriber. Each service flow can be associated with a pre-configured service flow for QoS and packet classification rule parameters in the uplink and downlink direction.

The BWG controls the BS's local switching through Data Path Encapsulation Type (NONE) and Data Path ID (Priority + VLAN ID) in the R6 DP Registration Request message. Note that the VLAN ID defined here can be overwritten from AAA. The VLAN Priority (the 3 most significant bits in VLAN tag) comes from DSCP/Precedence defined for the service flow. If DSCP/Precedence is not locally defined, it is calculated based on WiMAX QoS Data Delivery Service Type used for the service flow.

The **critical** keyworde 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.

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

Examples

The following example enables the initial service flow:

```
wimax agw sla profile gold
    service-flow pre-defined isf profile isf encap-type none vlan 10
    service-flow pre-defined secondary profile sec1 encap-type none vlan 10
```

service mode maintenance

To enable the User Group Maintenance mode feature that allows you to to block any new CPE from entering a particular user group so that the you can clear all of the subscribers (if needed), use the **service mode maintenance** global configuration command. Use the no form of the command to disable this feature.

service mode maintenance

no service mode maintenance

Syntax Description

There are no keywords or arguments for this command.

Defaults

By default, maintenance mode is disabled.

Command Modes

User group configuration submode.

Command History

Release	Modification
12.4(15)XL4	This command was introduced.

Examples

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
```

set

To specify what DSCP or TOS marking needs to be applied for the subscriber packets in the downstream direction, use the **set** subcommand in service flow direction configuration submode. Use the **no** form of the command to disable this feature. By default no marking is done.

set [**dscp** *dscp-value* | **precedence** *precedence-value* | **r3**]

no set [**dscp** *dscp-value* | **precedence** *precedence-value* | **r3**]

Syntax Description

dscp *dscp-value*	Sets the GW service flow Differentiated services codepoint (DSCP) specific values. The range is 0-63. The default value is 0.
precedence *precedence-value*	Sets the GW service flow precedence specific values. The range is 0-7.
r3	Sets the GW R3 reference point configuration commands.

Defaults

By default, no marking is done. The default value for dscp is 0.

Command Modes

Service flow direction configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example specifies the *precedence-value* and *dscp-value* arguments:

```
router(config-gw-sf-dir)#set dscp ?
  <0-63>   Differentiated services codepoint value
  af11     Match packets with AF11 dscp (001010)
  af12     Match packets with AF12 dscp (001100)
  af13     Match packets with AF13 dscp (001110)
  af21     Match packets with AF21 dscp (010010)
  af22     Match packets with AF22 dscp (010100)
  af23     Match packets with AF23 dscp (010110)
  af31     Match packets with AF31 dscp (011010)
  af32     Match packets with AF32 dscp (011100)
  af33     Match packets with AF33 dscp (011110)
  af41     Match packets with AF41 dscp (100010)
  af42     Match packets with AF42 dscp (100100)
  af43     Match packets with AF43 dscp (100110)
  cs1      Match packets with CS1(precedence 1) dscp (001000)
  cs2      Match packets with CS2(precedence 2) dscp (010000)
  cs3      Match packets with CS3(precedence 3) dscp (011000)
  cs4      Match packets with CS4(precedence 4) dscp (100000)
  cs5      Match packets with CS5(precedence 5) dscp (101000)
  cs6      Match packets with CS6(precedence 6) dscp (110000)
  cs7      Match packets with CS7(precedence 7) dscp (111000)
  default  Match packets with default dscp (000000)
  ef       Match packets with EF dscp (101110)
  r3       Set GW service flow R6 dscp with R3 dscp value         NEW
```

The next two are new additions for direction uplink. The BWG marks the outbound R3 IP DSCP value either by specifiying a value (set r3 dscp *value*), or using the outer IP DSCP value (**set r3 dscp r6-outer**). If either is not specified, the default is to have no change to the inner IP DSCP value. Here is an example:

```
router(config-gw-sf-dir)#set ?
  dscp        Set GW service flow dscp specific values
  precedence  Set GW service flow Precedence specific values
  r3          Set GW R3 reference point configuration commands    NEW

router(config-gw-sf-dir)#set r3 dscp ?                          ALL NEW BELOW
  <0-63>    Differentiated services codepoint value
  af11      Match packets with AF11 dscp (001010)
  af12      Match packets with AF12 dscp (001100)
  af13      Match packets with AF13 dscp (001110)
  af21      Match packets with AF21 dscp (010010)
  af22      Match packets with AF22 dscp (010100)
  af23      Match packets with AF23 dscp (010110)
  af31      Match packets with AF31 dscp (011010)
  af32      Match packets with AF32 dscp (011100)
  af33      Match packets with AF33 dscp (011110)
  af41      Match packets with AF41 dscp (100010)
  af42      Match packets with AF42 dscp (100100)
  af43      Match packets with AF43 dscp (100110)
  cs1       Match packets with CS1(precedence 1) dscp (001000)
  cs2       Match packets with CS2(precedence 2) dscp (010000)
  cs3       Match packets with CS3(precedence 3) dscp (011000)
  cs4       Match packets with CS4(precedence 4) dscp (100000)
  cs5       Match packets with CS5(precedence 5) dscp (101000)
  cs6       Match packets with CS6(precedence 6) dscp (110000)
  cs7       Match packets with CS7(precedence 7) dscp (111000)
  default   Match packets with default dscp (000000)
  ef        Match packets with EF dscp (101110)
  r6-outer  Set GW service flow R3 dscp with R6 dscp value

router(config-gw-sf-dir)#set precedence precedence-value

<0-7>           Precedence value
  critical        Set packets with critical precedence (5)
  flash           Set packets with flash precedence (3)
  flash-override  Set packets with flash override precedence (4)
  immediate       Set packets with immediate precedence (2)
  internet        Set packets with internetwork control precedence (6)
  network         Set packets with network control precedence (7)
  priority        Set packets with priority precedence (1)
  routine         Set packets with routine precedence (0)
```

service wimax agw

To enable the BWG functionality on the router, use the **service wimax agw** command in global configuration mode. Use the **no** version of the command to disable BWG functionality; all configured BWG-specific command lines will also be removed.

service wimax agw

no service wimax agw

Syntax Description

There are no arguments or keywords.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

The **no** version of the command will disable the BWG functionality and all the configured BWG-specific command lines will be removed. The **no** version of the command will be allowed only if there no session being serviced on the BWG.

Examples

The following example enables the BWG:

```
router(config)#service wimax agw
```

show ip mobile proxy

To display information about a proxy Mobile IP host, use the **show ip mobile proxy** command in privileged EXEC mode.

show ip mobile proxy [host [nai *string*] **| registration | traffic]**

Syntax Description

host	(Optional) Displays information about the proxy host.
nai *string*	(Optional) Network access identifier.
registration	(Optional) Displays proxy registration information.
traffic	(Optional) Displays information about RADIUS sessions being handled by IOS SLB.

Defaults

The command is disabled by default.

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T for PDSN platforms.

Examples

The following is sample output from the **show ip mobile proxy registration** command:

```
router# show ip mobile proxy registration

Proxy Mobile Node Registrations:
100022240001@cisco.com:
    Registration accepted 06/16/08 18:42:36
    Next Re-registration 00:21:27
    Registration sequence number 1
    Care-of addr 14.1.1.30, HA addr 14.1.1.80, Home addr 5.1.0.2
    Flags sbdmg-T-, Identification CC01329C.68498C88
    Lifetime requested 00:50:00 (3000), granted 00:50:00, remaining 00:46:27
    Revocation negotiated
```

show ip slb sessions

To display information about sessions handled by Cisco IOS Server Load Balancing (IOS SLB), use the **show ip slb sessions** command in privileged EXEC mode.

show ip slb sessions [**gtp** | **gtp-inspect** | **ipmobile** | **radius**] [**vserver** *virtual-server*] [**client** *ip-address netmask*] [**asnr6**] [**detail**]

Syntax Description

gtp	(Optional) Displays information about general packet radio service (GPRS) Tunneling Protocol (GTP) sessions being handled by IOS SLB.
gtp-inspect	(Optional) Displays information about GTP sessions being handled by IOS SLB that have GTP cause code inspection enabled.
ipmobile	(Optional) Displays information about Mobile IP sessions being handled by IOS SLB.
radius	(Optional) Displays information about RADIUS sessions being handled by IOS SLB.
vserver *virtual-server*	(Optional) Displays information about sessions being handled by the specified virtual server.
client *ip-address netmask*	(Optional) Displays information about sessions associated with the specified client IP address or subnet.
asnr6	(Optional) Displays information about ASN sessions.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp** and **gtp-inspect** keywords were added.
12.2(14)ZA2	The **ipmobile** keyword was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.4(15)XL	The **asnr6** keyword was added.

Examples

The following is sample output from the **show ip slb sessions** command for ASN sessions:

```
router# show ip slb sessions asnr6

vserver         MSID              Base Station      real             state
-------------------------------------------------------------------------------10.10.10.10
001646013fc0      5.5.5.5           10.10.1.1        ASNR6_REQ

router# show ip slb session asnr6 detail

   ASN, client = 12.12.12.1:2231, virtual = 3.3.3.3:2231
   state = ASNR6_ESTAB, real = 2.2.2.2
   Key = 0000000100020003, retry = 1
```

show ip slb sticky

To display information about load balancing stickiness, use the **show ip slb sticky** command in Privileged EXEC mode.

show ip slb sticky asn [*msid* **|** *nai***]**

Syntax Description

asn *msid* | *nai*	(Optional) Displays information about BWG stickiness using the *msid* or *nai* arguments.

Defaults

There are no default values for this command.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

Here is an example configuration:

```
show ip slb sticky asn msid <macid>
MSID                Real      Group Id vs_index   NAI
-----------------------------------------------------
ABCD.12FE.3467   10.10.10.1   5         10        abc@cisco.com
2247.1130.8642   10.10.10.2   5         10        bcd@abc.com

- show ip slb sticky asn nai abc@cisco.com
MSID                Real      Group Id vs_index   NAI
-----------------------------------------------------
ABCD.12FE.3467   10.10.10.1   5         10        abc@cisco.com

- show ip slb stats
MWTCL06-SW1#sh ip slb stats
Pkts via normal switching:     101126
Pkts via special switching:    0
Pkts via slb routing:          0
Pkts Dropped:                  0
Connections Created:           101068
Connections Established:       0
Connections Destroyed:         101067
Connections Reassigned:        0
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS framed-ip Sticky Count: 0
RADIUS username Sticky Count:  0
RADIUS cstn-id Sticky Count:   0
GTP imsi Sticky Count:         0
Failed Correlation Injects:    0
```

```
Pkt fragments drops in ssv:    0
ASN MSID sticky count:         1

router#show ip slb vservers name VS detail
VS, state = OPERATIONAL, v_index = 9, interface(s) = <any>
  virtual = 3.2.3.1/32:2231, UDP, service = ASN, advertise = TRUE
  server farm = 7200-FARM, delay = 10, idle = 100
  asn: request idle = 90
  asn: delete notif recvd = 2, nai-update notif recvd = 2
  asn: Notification Errors : Deletes = 1, nai-updates = 0
  sticky: <none>
  sticky: group id = 4097 <assigned>
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 156, syns = 0, syn drops = 0
  standby group = None
-------------------------------------------------------
               |      delete     |    nai-updates
   Real commn: |--------+--------+--------+-------------
  Port = 63082 |  Recv  | Errors |  Recv  |  Errors
---------------+--------+--------+--------+-------------
    15.15.15.4       1         1        1         0
    15.15.15.5       1         0        1         0
```

Fields to display communication port between the vserver VS and BWG, delete notification received and NAI updates and notification because of stale session in wrong reals will be added as shown above.

```
router#show ip slb session asn <cr>
vserver         MSID             Base Station     real             state
-----------------------------------------------------------------------------
10.10.10.10     001646013fc0     5.5.5.5          10.10.1.1        ASN_ESTAB
```

show subscriber msid bs-list

To view the allowed BS list, use the **show subscriber msid bs-list** command in the Privileged EXEC mode.

show subscriber msid *msid* **bs-list**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

Here is an example of the **show subscriber msid bs-list** command:

```
router#show wimax agw subscriber msid 0900.0502.1000 bs-list
 MSID 0900.0502.1000
  Allowed Base Station(s):
   0A 0A 0A 4D
   AA AA AA
```

show wimax agw

To display various system parameters, including BWG software version, number of base stations allowed, number of subscribers allowed, and others, use the **show wimax agw** privileged EXEC command.

show wimax agw

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL3	This command was enhanced to display the following: • Current number of sessions with all IP packets redirected • IP-GRE Traffic Rcvd redirected • Eth-GRE Traffic Rcvd redirected
12.4(24)YG	This command was enhanced to display the following: • Current number of subscribers PMIP enabled.

Usage Guidelines

The output of this show command contains the following information:

- Version of WiMAX BWG Software
- Maximum number of base stations allowed
- Maximum number of subscribers allowed
- Number of base stations currently connected
- Number of R6 sessions currently active
- Number of IP CS flows currently active
- Number of Ethernet CS flows currently active
- Number of IP CS hosts currently active
- Number of Ethernet CS hosts currently active
- Number of IP CS data packets and bytes sent
- Number of IP CS data packets and bytes received
- Number of Ethernet CS data packets and bytes sent
- Number of Ethernet CS data packets and bytes received

- Number of IP CS packets and bytes received redirected
- Number of Ethernet CS packets and bytes received redirected
- Current number of framed routes
- Current number of subscribers using framed routes
- Current number of users auto-provisioned sessions
- Current number of sessions with all IP packets redirected

Examples

The following is sample output for the **show wimax agw** command:

```
Broadband wireless gateway version 1.1, service is enabled
 Signaling UDP port 2231
 Maximum Number of base station 500 allowed
 Maximum Number of subscriber 20000 allowed
  Current number of framed routes 0
  Current number of subscribers using framed routes 0
  Current number of signalling paths 1
  Current number of data paths 1
  Current number of subscribers 1
  Current number of sessions 1
  Current number of user auto-provisioned sessions 0
  Current number of flows 2
  Current number of hosts 0
  Current number of sessions with all ip packets redirected 0
  IP-GRE traffic Sent 0 packets, 0 bytes
  IP-GRE traffic Rcvd 0 packets, 0 bytes
  IP-GRE Traffic Rcvd redirected 0 packets, 0 bytes
  Eth-GRE traffic Sent 2 packets, 748 bytes
  Eth-GRE traffic Rcvd 2 packets, 1208 bytes
  Eth-GRE Traffic Rcvd redirected 0 packets, 0 bytes
```

Display information about the BWG redundancy specific statistics.

```
Snapshot:
           WiMAX BWGBWG Session Redundancy Counters
           Redundancy Events Counters On Active
           Session Events
           Session Up Success               : 100
           Session Down Success             : 10

           Flow Events

           Flow Up Success                  : 200
           Flow Down Success      : 0
           Host Events

           Host Up Success                  : 300
           Host Down Success                : 100
           Authentication Events
           Re-authentication Update Success : 10
           Accounting Events
           Accounting Update Success
```

Here is an example for BWG IOS Release 12.4(15)XL3:

```
BWG-2#sh wim agw
Broadband wireless gateway version 1.2, service is enabled
 Signaling UDP port 2231
```

```
Session Redundancy State ACTIVE
Maximum Number of base station 500 allowed
Maximum Number of subscriber 20000 allowed
 Current number of framed routes 0
 Current number of subscribers using framed routes 0
 Current number of signalling paths 1
 Current number of data paths 1
 Current number of subscribers 1
 Current number of sessions 1
 Current number of user auto-provisioned sessions 0
 Current number of flows 2
 Current number of hosts 0
 Current number of sessions with all ip packets redirected 0
 IP-GRE traffic Sent 4 packets, 1212 bytes
 IP-GRE traffic Rcvd 6 packets, 3624 bytes
 IP-GRE Traffic Rcvd redirected 0 packets, 0 bytes
 Eth-GRE traffic Sent 0 packets, 0 bytes
 Eth-GRE traffic Rcvd 0 packets, 0 bytes
 Eth-GRE Traffic Rcvd redirected 0 packets, 0 bytes
```

show wimax agw fsm dhcp-proxy

To show how many sessions are in the various states of the DHCP/MIP proxy state machine, use the **show wimax agw fsm dhcp-proxy** command in privileged EXEC mode.

show wimax agw fsm dhcp-proxy

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Examples

The following is sample output for the **show wimax agw fsm dhcp-proxy** command:

```
router#show wimax agw fsm dhcp-proxy
AGW Proxy FSM
 Number of element(s) currently in following states
 ---------------------------------------------------
  Init(0) = 0, Registering(1) = 0, Registered(2) = 0
  Deregistering(3) = 0, Assigning(4) = 0, Ready(5) = 1
  Cleanup(6) = 0
```

show wimax agw message

To display information about the messages supported by the BWG, use the **show wimax agw message** command in privileged EXEC mode.

show wimax agw message [*function-type-no*]

Syntax Description

function-type-no	Function type value of the message to be displayed.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If a Function-Type number is not specified, then the command displays information about all the supported Function-Types.

The output of this show command contains the following information:

- Function-Type number
- Name of the Function-Type
- Possible reference points over which this Function-Type can be received
- Number of possible message types for this Function-Type
- Details for each message type, which include
- Message-Type number
- Message-Type name
- Reference points over which this Message-Type can be received
- Whether a reply is expected for this Message-Type

Examples

The following is sample output for the **show wimax agw message** [*function-type-no*] command:

```
Message function type Data Path(3/0x3)
 Highest message type value 16
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type Deregistration Request(4/0x4)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Deregistration Response(5/0x5)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Deregistration Ack(6/0x6)
```

```
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Not expecting response for this message
   Message type Registration Request(12/0xC)
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Expecting response for this message
   Message type Registration Response(13/0xD)
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Expecting response for this message
   Message type Registration Ack(14/0xE)
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Not expecting response for this message

Message function type Context Delivery(4/0x4)

router#sh wimax agw message
Message function type Data Path(3/0x3)
 Highest message type value 16
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type Deregistration Request(4/0x4)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Deregistration Response(5/0x5)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Deregistration Ack(6/0x6)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message
  Message type Registration Request(12/0xC)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Registration Response(13/0xD)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Registration Ack(14/0xE)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message

Message function type Context Delivery(4/0x4)
 Highest message type value 4
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type Context Delivery Request(1/0x1)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Context Delivery Report(2/0x2)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message

Message function type Auth Relay(8/0x8)
 Highest message type value 10
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type EAP Start(1/0x1)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message
  Message type EAP Transfer(2/0x2)
Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message
  Message type Key Change Directive(5/0x5)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Key Change Confirm(6/0x6)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Key Change ACK(7/0x7)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
```

```
    Not expecting response for this message
   Message type CMAC Key Count Update(8/0x8)
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Expecting response for this message
   Message type CMAC Key Count Update Ack(9/0x9)
    Reference pts on which rcvd/sent BS <-> AGW R6(8)
    Not expecting response for this message

Message function type MS State Change(9/0x9)
 Highest message type value 18
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type Attachment Response(7/0x7)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Attachment Request(8/0x8)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Attachment ACK(9/0x9)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message
  Message type Pre Attachment Request(15/0xF)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Pre Attachment Response(16/0x10)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Pre Attachment ACK(17/0x11)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message

Message function type Keepalive(20/0x14)
 Highest message type value 3
 Reference pts on which rcvd/sent BS <-> AGW R6(8)
  Message type Keepalive Request(1/0x1)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Expecting response for this message
  Message type Keepalive Response(2/0x2)
   Reference pts on which rcvd/sent BS <-> AGW R6(8)
   Not expecting response for this message
```

show wimax agw path

To display base station information, use the **show wimax agw path** command in privileged EXEC mode.

show wimax agw path [*bs-ip-address*] [**brief**]

Syntax Description

bs-ip-address	For each base station, the following information will be displayed: Control path details • BS IP Address • Number of sessions currently active • Number of packets and bytes transmitted to the base station • Number of packets and bytes received from the base station Data path details • BS IP Address • Number of flows currently active • Number of packets and bytes switched in CEF and process paths for this base station If the base station IP address is not specified, the command will display information about all of the base stations currently connected to the BWG.
brief	If the **brief** keyword is specified, then the output will contain a list of all the current sessions in column format, containing the following information • BS IP Address • Number of sessions currently active • FSM state • Number of packets and bytes sent/received from the base station

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following is sample output for the **show wimax agw path** command:

```
Router#show wimax agw path brief
Base station Type     Elements   State   Pkts-Rx    Pkts-Tx    Bytes-Rx   Bytes-Tx
10.1.1.84 Sig-UDP    1          Ready       134        135            11196      9404
10.1.1.84 Data-GRE 1            --       10811      10816      6983906    3860167
10.1.1.84 IP-GRE                   --        0811          16       6983000    3860000
```

```
Eth-GRE                 --       10000     10800       906           167

Router#show wimax agw path data
Path type Data-GRE
 Number of flows connected 1
 Address local 2.2.2.2(AF_INET), remote 10.1.1.84(AF_INET)
 IP Traffic sent 10833 packets, 3866236 bytes
 IP Traffic received 10828 packets, 6994888 bytes
 Ethernet Traffic sent 10833 packets, 3866236 bytes
 Ethernet Traffic received 10833 packets, 3866236 bytes


Router#show wimax agw path 10.1.1.70
Path type Sig-UDP
 State current Ready, old Idle
 Number of sessions connected 1
 Number of old sessions connected 0
 Address local 11.1.4.0(AF_INET), remote 10.1.4.77(AF_INET)
 UDP port local 2231(0x8B7), remote 2231(0x8B7)
 Identification Peer 0x0A01044D, Our 0x0B010400
 IP-GRE traffic sent 15 packets, 4643 bytes
 IP-GRE traffic received 14 packets, 2879 bytes


Path type Data-GRE
 Number of flows connected 2
 Address local 11.1.4.0(AF_INET), remote 10.1.4.77(AF_INET)
 Ethernet-GRE traffic sent 2 packets, 832 bytes
 Ethernet-GRE traffic received 2 packets, 1320 bytes
 IP-GRE traffic sent 0 packets, 0 bytes
 IP-GRE traffic received 0 packets, 0 bytes
```

show wimax agw redundancy status

To display session redundancy status on the BWG, use the **show wimax agw redundancy status** command in privileged EXEC mode.

show wimax agw redundancy status

Syntax Description

There are no keywords or arguments for this command.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following is sample output for the **show wimax agw redundancy status** command:

```
Router#show wimax agw redundancy status
           WiMAX AGW Session Redundancy is enable
           WiMAX AGW Session Redundancy system status
           AGW state = STANDBY HOT
           AGW-peer state = ACTIVE
           WiMAX AGW Session Redundancy Status Summary
                        Synced from active
           Subscriber            1
           Flows                 2
           Hosts                 0
```

show wimax agw statistics

To display statistics per reference point, use the **show wimax agw statistics** command in privileged EXEC mode.

show wimax agw statistics [**dfp** | **dhcp-relay** | **dhcp-proxy** | **internal** | **arp**] | [**brief**]

Syntax Description

dfp	(Optional) Displays dfp status on the BWG.
dhcp-relay	(Optional) Displays the number for DHCP messages transmitted and received to and from the DHCP server when the BWG acts as a DHCP relay.
dhcp-proxy	(Optional) Displays the number for DHCP messages transmitted and received to and from the DHCP client when the BWG acts as a DHCP proxy.
internal	(Optional) Displays PMIP statistics.
arp	(Optional) The following information is displayed for the ARP related command: • Total number of ARP requests received • Total number of ARP reply sent • Total number of ARP packets dropped
brief	Provides abbreviated show output for options.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(15)XL1	Keepalive statistics were added.
12.4(24)YG	The **dhcp-proxy** and **dhcp-relay** keywords were added. Additionally, PMIP, ARP, DHCP and other statistics were added to the **internal** keyword output.

Usage Guidelines

In BWG Release 2.0, the following information is added for the **show wimax agw statistics internal** command:

- Number of packets dropped due to Static IP Host not authorized by AAA (previously - Number of packets dropped due to Static IP Host not allowed)
- Number of packets dropped due to Static IP Host not authorized by HA
- Data packets dropped DHCP packets received during MIP registration
- Data packets dropped ARP packets received during MIP registration
- Data packets dropped non-ARP and non-DHCP packets received during MIP registration
- Total subscriber PMIP enabled created

- Total subscriber PMIP enabled deleted
- Number of packets dropped due to MIP registration incomplete

For each reference point, the following information will be displayed

- Number of function types (FT) and message types (MT) sent over this reference point
- Number of function types (FT) and message types (MT) received over this reference point

Examples

The following is sample output for the **show wimax agw statistics** command:

```
Router#show wimax agw statistics
Message function type MS State Change(9/0x9)
  Message type Attachment Response(7/0x7)
   Number of messages sent 4
   Number of messages received 0
   Number of messages resent 0
  Message type Attachment Request(8/0x8)
   Number of messages sent 0
   Number of messages received 4
   Number of messages resent 0
  Message type Attachment ACK(9/0x9)
   Number of messages sent 0
   Number of messages received 4
   Number of messages resent 0
  Message type Pre Attachment Request(15/0xF)
   Number of messages sent 0
   Number of messages received 4
   Number of messages resent 0
  Message type Pre Attachment Response(16/0x10)
   Number of messages sent 4
   Number of messages received 0
   Number of messages resent 0
  Message type Pre Attachment ACK(17/0x11)
   Number of messages sent 0
   Number of messages received 4
   Number of messages resent 0
```

Data Path Statistics

```
Router#show wimax agw statistics
Message function type Data Path(3/0x3)
  Message type Deregistration Request(4/0x4)
   Number of messages sent 1
   Number of messages received 1
   Number of messages resent 0
  Message type Deregistration Response(5/0x5)
   Number of messages sent 1
   Number of messages received 0
   Number of messages resent 0
  Message type Deregistration Ack(6/0x6)
   Number of messages sent 0
   Number of messages received 1
   Number of messages resent 0
  Message type Registration Request(12/0xC)
   Number of messages sent 8
   Number of messages received 1
   Number of messages resent 0
  Message type Registration Response(13/0xD)
   Number of messages sent 1
   Number of messages received 8
```

```
   Number of messages resent 0
  Message type Registration Ack(14/0xE)
   Number of messages sent 8
   Number of messages received 1
   Number of messages resent 0
```

The following information will be displayed for ARP related command

```
Router# sh wim agw statistics arp

Total number of ARP requests received
Total number of ARP reply sent
Total number of ARP packets dropped
```

Timeout Statistics

```
Message function type Keepalive(20/0x14)
  Message type Keepalive Request(1/0x1)
   Number of messages sent 21
   Number of messages received 0
   Number of messages resent 0
  Message type Keepalive Response(2/0x2)
   Number of messages sent 0
   Number of messages received 21
   Number of messages resent 0
```

Here are examples of the **show wimax agw statistics dhcp-relay** and **show wimax agw statistics dhcp-proxy** commands:

```
BWG#sh wim agw statistics dhcp-relay
Last clearing of "show wimax agw statistics dhcp-relay" counters never

   Tx to DHCP server Discover 171, Request 143
   Tx to DHCP server Release 0, Decline 0
   Tx to DHCP server Inform 0
   Rx from DHCP server Offer 115, Ack 116
   Rx from DHCP server Nak 0, Unknown 0

BWG#show wimax agw statistics dhcp-proxy
Last clearing of "show wimax agw statistics dhcp-proxy" counters never

   Rx from DHCP client Discover 24, Request 65
   Rx from DHCP client Release 0, Decline 0
   Rx from DHCP client Inform 0
   Tx to DHCP client Offer 24, Ack 65
   Tx to DHCP client Nak 0, Unknown 0
```

show wimax agw subscriber

To display subscriber information, use the **show wimax agw subscriber** command in privileged EXEC mode. If the subscriber *macid* is not specified, the output displays information about all the subscribers currently connected to the BWG.

show wimax agw subscriber [**msid** *macid* [**overflowed-host**]] [**bsid**] [**brief** {**flow** | **host** | **session** | **traffic**}] [**internal**]

Syntax Description

msid	Displays information about the mobile subscriber.
macid	If the subscriber *macid* is not specified, the output displays information about all the subscribers currently connected to the BWG.
overflowed-host	(Optional) Displays the overflowed hosts.
brief	Displays output that contains a list of all the subscribers currently connected. Contains the following information: • Subscriber MACID • Local/remote IP addresses of the signaling end points for this subscriber • Local/remote UDP ports of the signaling end points for this subscriber • Number of flows currently active
flow	Displays brief output related to flows.
host	Displays brief output related to the host.
session	Displays brief output related to sessions.
traffic	Displays brief output related to traffic.
bsid	When **bsid** is specified, it only displays the subscribers related to the BS. **msid** and **bsid** are mutually exclusive.
internal	Displays internal MIP statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Release	Modification
12.4(15)XL3	This comand was modified to display the following: • Display SLA profiles (from the list received from AAA) used to set up the flow. • Indicate the SF from which the flow is setup.
12.4(24)YG	This command was modified to display the following: • Subscriber capability of using PMIP • MIP information such as: – Details Host – Number of packets • The **overflowed-host** keyword was added.

Usage Guidelines

The following information will be displayed for each subscriber:

- Subscriber MACID
- Local/remote IP addresses of the signaling end points for this subscriber
- Local/remote UDP ports of the signaling end points for this subscriber
- Subscriber FSM information
- Number of flows currently active
- Details Hosts - This information has been updated to include the number of hosts rejected and number of static hosts aged out.
- Static IP permissions, classifier information, QoS details, idle timer status & SLA information.
- Details for all the flows - This information have been updated to include CS-type.
- Authentication details (i.e. unauthenticated, single-EAP, double-EAP, etc.)
- Data Encapsulation type and VLAN ID - For “control only”.
- You can view subscribers on a specific BS, or a particular subscriber.

If the **brief** keyword is specified, then the output will contain the following information:

- Subscriber MACID
- Local/remote IP addresses of the signaling end points for this subscriber
- Local/remote UDP ports of the signaling end points for this subscriber
- Number of flows currently active

In Release 2.0 the output reflects the PMIP context information in the BWG. The PMIP tunnel and registry information is obtained from the standard proxy mobile IP commands.

The following information has been added:

- Subscriber capability of using PMIP
- MIP information such as:
  - HA Address
  - Home Address

  //if host-config exists,

  - Home Network Prefix Length
  - Default Gateway
  - Primary DNS
  - Secondary DNS
- Details Host
  - Host PMIP status (whether address allocated using PMIP)
- Number of packets dropped due to incomplete MIP registration

In addition to the above, in BWG Release 2.0, the following information has been added to the **wimax agw subscriber internal** command:

- MIP information such as:
  - MN-HA Key
  - MN-HA-Spi
  - HA-RK-Key
  - HA-RK-Key-Spi
  - Lifetime Requested
  - Mip-Flag
  - AAA-Pmip-Flag
  - Pmip-Cli-Conf-Flag

Examples

The following is sample output for the **show wimax agw subscriber** command:

```
BWG-2#sh wim agw sub
MSID 1000.2227.0001
 CPE is non-nomadic
 Static IP address list downloaded
 Subscriber Age 000:15:55
 Base Station ID 0x0E01010300000000
 Auth policy 0X0(0)
 PMIP permitted
 PMIP HA Address 14.1.1.80
 PMIP Reg Lifetime is 3000
 PMIP Home Address 5.1.0.1
 PMIP host cfg dns ext(primary addr) 14.1.1.200
 PMIP host cfg dns ext(secondary addr) 14.1.1.201
 PMIP host cfg prefix length 16
 Subscriber address 5.1.0.1, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP proxy
 Subscriber address assigned using PMIP
 Subscriber address assigned on flow downlink ID 401
 Subscriber address prefix len allocated 32, aggregate 0
 Subscriber address IP-GRE traffic sent 0 packets, 0 bytes
 Subscriber address IP-GRE traffic received 0 packets, 0 bytes
 Subscriber address Eth-GRE traffic sent 0 packets, 0 bytes
 Subscriber address Eth-GRE traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 2343, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 1000.2227.0001, length 6
 Subscriber address DHCP Refresh time 3000 seconds
 Subscriber idle time 00:15:57
 Subscriber host accounting not enabled
 Subscriber address format ARPA, type Ether
```

```
Number of hosts rejected 0
Number of packets dropped due to Static IP Host not authorized by AAA 0
Number of packets dropped due to Static IP Host not authorized by HA 0
Number of packets dropped due to MIP registration incomplete 1
Number of static hosts aged out 0
Number of handoff rejected due to unapproved BS 0
Number of Host behind 0
Number of sessions 1
 Session details:
  FSM in state Ready(7) on last event Post Attachment(17)
  Username 100022270001@unauthenticated.com
  Authentication method PAP
  Session Hotlining Inactive
  AAA Termination action 0
  Associated user group unauthenticated
  Associated SLA Profile Name silver
  Signalling address local 3.3.3.3, remote 14.1.1.3
  Signalling UDP port local 2231, remote 2231
  Idle for inbound 00:15:58, outbound 00:15:58
  Absolute timeout 80000, remaining 22:00:30
  Ingress Address filtering 0 packets, 0 bytes
  Session Up for traffic
  Number of flows 5
   Flow details ISF(0)
    SF Profile name isf
    FSM in state SF Ready(4) on last event Up(1)
    Transaction ID used 0X8001(32769)
    Data ID local 0xC9(201), remote 0xC5(197)
    Data address local 3.3.3.3, remote 14.1.1.3
    Data traffic sent 2 packets, 626 bytes
    Data traffic received 3 packets, 1812 bytes
    Accounting last record sent Start(1)
    Accounting start response Unknown
    Idle for inbound 00:15:58, outbound 00:15:58
    Service Flow information Downlink:
     Identifier 401
     Set dscp cs1
     QoS information:
      data-delivery-service best-effort
      maximum-traffic-rate-sustained 0, traffic-priority 0
      policy-transmission-request 0
      reduced-resources-code 0
     media-flow-type 02123424231412
     Classifier information:
      priority 1
       ipv4 permit ip any any
       ethernet permit any any any
       vlan permit any any
     CS Type information:
      Ethernet CS
    Service Flow information Uplink:
     Identifier 402
     Set dscp cs2
     QoS information:
      data-delivery-service best-effort
      maximum-traffic-rate-sustained 0, traffic-priority 0
      policy-transmission-request 0
      reduced-resources-code 0
      media-flow-type 0a45464748
     Classifier information:
      priority 1
       ipv4 permit ip any any
       ethernet permit any any any
       vlan permit any any
```

```
  CS Type information:
   Ethernet CS
Flow details Secondary(1)
 SF Profile name sec1
 FSM in state SF Ready(4) on last event Up(1)
 Transaction ID used 0X8002(32770)
 Data ID local 0xCA(202), remote 0xC6(198)
 Data address local 3.3.3.3, remote 14.1.1.3
 Data traffic sent 0 packets, 0 bytes
 Data traffic received 0 packets, 0 bytes
 Accounting last record sent Start(1)
 Accounting start response Unknown
 Idle for inbound 00:16:02, outbound 00:16:02
 Service Flow information Downlink:
  Identifier 403
  Set dscp af11
  QoS information:
   data-delivery-service best-effort
   maximum-traffic-rate-sustained 0, traffic-priority 0
   policy-transmission-request 0
   reduced-resources-code 0
   media-flow-type 02123424231412
  Classifier information:
   priority 2
    ipv4 permit ip any any
    ethernet permit any any any
    vlan permit any any
  CS Type information:
   Ethernet CS
 Service Flow information Uplink:
  Identifier 404
  Set dscp af12
  QoS information:
   data-delivery-service best-effort
   maximum-traffic-rate-sustained 0, traffic-priority 0
   policy-transmission-request 0
   reduced-resources-code 0
   media-flow-type 0a45464748
  Classifier information:
   priority 2
    ipv4 permit ip any any
    ethernet permit any any any
    vlan permit any any
  CS Type information:
   Ethernet CS
Flow details Secondary(2)
 SF Profile name sec2
 FSM in state SF Ready(4) on last event Up(1)
 Transaction ID used 0X8003(32771)
 Data ID local 0xCB(203), remote 0xC7(199)
 Data address local 3.3.3.3, remote 14.1.1.3
 Data traffic sent 0 packets, 0 bytes
 Data traffic received 0 packets, 0 bytes
 Accounting last record sent Start(1)
 Accounting start response Unknown
 Idle for inbound 00:16:03, outbound 00:16:03
 Service Flow information Downlink:
  Identifier 405
  Set dscp af11
  QoS information:
   data-delivery-service best-effort
   maximum-traffic-rate-sustained 0, traffic-priority 0
   policy-transmission-request 0
   reduced-resources-code 0
```

```
    media-flow-type 02123424231412
   Classifier information:
    priority 3
     ipv4 permit ip any any
     ethernet permit any any any
     vlan permit any any
   CS Type information:
    Ethernet CS
  Service Flow information Uplink:
   Identifier 406
   Set dscp af12
   QoS information:
    data-delivery-service best-effort
    maximum-traffic-rate-sustained 0, traffic-priority 0
    policy-transmission-request 0
    reduced-resources-code 0
    media-flow-type 0a45464748
   Classifier information:
    priority 3
     ipv4 permit ip any any
     ethernet permit any any any
     vlan permit any any
    CS Type information:
    Ethernet CS
 Flow details Secondary(3)
  SF Profile name sec3
  FSM in state SF Ready(4) on last event Up(1)
  Transaction ID used 0X8004(32772)
  Data ID local 0xCC(204), remote 0xC8(200)
  Data address local 3.3.3.3, remote 14.1.1.3
  Data traffic sent 0 packets, 0 bytes
  Data traffic received 0 packets, 0 bytes
 Accounting last record sent Start(1)
  Accounting start response Unknown
  Idle for inbound 00:16:03, outbound 00:16:03
  Service Flow information Downlink:
   Identifier 407
   Set dscp af11
   QoS information:
    data-delivery-service best-effort
    maximum-traffic-rate-sustained 0, traffic-priority 0
    policy-transmission-request 0
    reduced-resources-code 0
    media-flow-type 02123424231412
   Classifier information:
    priority 4
     ipv4 permit ip any any
     ethernet permit any any any
     vlan permit any any
   CS Type information:
    Ethernet CS
  Service Flow information Uplink:
   Identifier 408
   Set dscp af12
   QoS information:
    data-delivery-service best-effort
    maximum-traffic-rate-sustained 0, traffic-priority 0
    policy-transmission-request 0
    reduced-resources-code 0
    media-flow-type 0a45464748
   Classifier information:
    priority 4
     ipv4 permit ip any any
     ethernet permit any any any
```

```
        vlan permit any any
      CS Type information:
       Ethernet CS
    Flow details Secondary(4)
SF Profile name sec4
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8005(32773)
     Data ID local 0xCD(205), remote 0xC9(201)
     Data address local 3.3.3.3, remote 14.1.1.3
     Data traffic sent 0 packets, 0 bytes
     Data traffic received 0 packets, 0 bytes
     Accounting last record sent Start(1)
     Accounting start response Unknown
     Idle for inbound 00:16:03, outbound 00:16:03
     Service Flow information Downlink:
      Identifier 409
      Set dscp af11
      QoS information:
       data-delivery-service best-effort
       maximum-traffic-rate-sustained 0, traffic-priority 0
       policy-transmission-request 0
       reduced-resources-code 0
       media-flow-type 02123424231412
      Classifier information:
       priority 5
        ipv4 permit ip any any
        ethernet permit any any any
        vlan permit any any
      CS Type information:
       Ethernet CS
     Service Flow information Uplink:
      Identifier 410
      Set dscp af12
      QoS information:
       data-delivery-service best-effort
       maximum-traffic-rate-sustained 0, traffic-priority 0
       policy-transmission-request 0
       reduced-resources-code 0
       media-flow-type 0a45464748
      Classifier information:
   priority 5
        ipv4 permit ip any any
        ethernet permit any any any
        vlan permit any any
      CS Type information:
       Ethernet CS
```

```
BWG# show wimax agw subscriber brief [traffic]
MSID                Base Station    Pkts-Tx    Bytes-Tx          Pkts-Rx    Bytes-Rx
1000.2223.0001 10.5.5.3           0           0                0           0
1000.2224.0001 10.5.5.3             0             0                  0             0
BWG# show wimax agw subscriber brief flow [traffic]
 MSSID              Base Station Idx Pkts-Tx  Bytes-Tx        Pkts-Rx    Bytes-Rx
1000.2223.0001 10.5.5.3       0  0            0                0           0
1000.2223.0001 10.5.5.3       1  0            0                0           0
1000.2224.0001 10.5.5.3       0  0            0                0           0
1000.2224.0001 10.5.5.3        1  0             0                  0             0
BWG# show wimax agw subscriber brief host [traffic]
MSID                  Base Station    Index Pkts-Tx    Bytes-Tx             Pkts-Rx
Bytes-Rx
1000.2223.0001 10.5.5.3           1         0                0                    0
0
```

```
1000.2224.0001 10.5.5.3          1        0                0                    0
0
```

Here is an example of the **show wimax agw subscriber** command for IOS Release 12.4(15)XL3:

```
BWG#sh wim agw subs , ms 0032.235F.ABCD
MSID 0032.235F.ABCD
CPE Settings: 7
 CPE is nomadic
 Static IP addresses permitted
 Subscriber Age 000:03:39
 Base Station ID 0x0A010646
 Auth policy 0X12(18), Single-EAP, CMAC
 AK Ctx method C-MAC(1), Lifetime 65535
 AK Ctx Seq No. AK 0, PMK 0
 AK Ctx C-MAC key count 1
 Subscriber address 11.1.0.2, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 Subscriber address assigned on flow downlink ID 9
 Subscriber address prefix len allocated 16, aggregate 32
 Subscriber address IP-GRE traffic sent 0 packets, 0 bytes
 Subscriber address IP-GRE traffic received 0 packets, 0 bytes
 Subscriber address Eth-GRE traffic sent 0 packets, 0 bytes
 Subscriber address Eth-GRE traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 9148, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 0032.235F.ABCD, length 6
 Subscriber address DHCP Refresh time 18000 seconds
 Subscriber address format ARPA, type Ether
 Number of hosts rejected 0
 Number of packets dropped due to Static IP Host not allowed 0
 Number of static hosts aged out 0
 Number of handoff rejected due to unapproved BS 0
 Number of Host behind 0
 Number of sessions 1
  Session details:
   FSM in state Ready(7) on last event Rx Attach Ack(16)
   Username rahumani@eap-tls.com
   Authentication method EAP
   AAA Framed route 5.5.0.0, mask 255.255.0.0
   AAA Session-id length 4, 0x30313233
   AAA Termination action 1
   AAA Class class-wimax-changed
   Reauthentication attempts from subscriber 0, ASNGW 0
   Associated user group cisco.com
   Associated SLA Profile Name silver,platinum,gold
   Signalling address local 11.1.6.1, remote 10.1.6.70
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:03:37, outbound 00:03:37
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 4
    Flow details ISF(0)
     SF profile name isf
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8009(32777)
     Data ID local 0x5(5), remote 0xE(14)
     Data address local 11.1.6.1, remote 10.1.6.70
     Data traffic sent 2 packets, 748 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting disabled
     Idle for inbound 00:03:37, outbound 00:03:37
     Service Flow information Downlink:
      Identifier 9
      Set DSCP (DDS) 30
      QoS information:
```

```
    Data-delivery-service real-time-variable-rate
    Minimum traffic-rate-reserved 4, Maximum latency 1
    Unsolicited interval-polling 9, Traffic-priority 1
    Maximum traffic-rate-sustained 3, Request/Transmission-policy 5
    Maximum traffic-burst-rate 2
    Reduced-resources-code 0
   Classifier information:
    priority 0
     ipv4 permit ip any any
     ethernet permit any any any
     vlan permit 5 0
   CS Type information:
    Ethernet CS
  Service Flow information Uplink:
   Identifier 10
   Set DSCP af22
   QoS information:
    Data-delivery-service best-effort
    Maximum traffic-rate-sustained 0 Traffic-priority 0
    Request/Transmission-policy 51
    Reduced-resources-code 0
   Classifier information:
    priority 0
     ipv4 permit ip any any
     ethernet permit any any any
     vlan permit 10 any
   CS Type information:
    Ethernet CS
 Flow details Secondary(1)
  SF profile name sec
  FSM in state SF Ready(4) on last event Up(1)
  Transaction ID used 0X800A(32778)
  Data ID local 0x6(6), remote 0xF(15)
  Data address local 11.1.6.1, remote 10.1.6.70
  Data traffic sent 0 packets, 0 bytes
  Data traffic received 0 packets, 0 bytes
  Accounting disabled
  Idle for inbound 00:03:39, outbound 00:03:39
  Service Flow information Downlink:
   Identifier 11
   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 1
     ethernet permit any 1000.2223.0002 FFFF.FFFF.FFFF any
   CS Type information:
    Ethernet CS
  Service Flow information Uplink:
   Identifier 12
   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 1
     ethernet permit any any ether_type arp
   CS Type information:
    Ethernet CS
 Flow details Secondary(2)
  SF profile name sec2
  FSM in state SF Ready(4) on last event Up(1)
  Transaction ID used 0X800B(32779)
  Data ID local 0x7(7), remote 0x10(16)
  Data address local 11.1.6.1, remote 10.1.6.70
  Data traffic sent 0 packets, 0 bytes
  Data traffic received 0 packets, 0 bytes
  Accounting disabled
  Idle for inbound 00:03:39, outbound 00:03:39
  Service Flow information Downlink:
   Identifier 13
   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
  Service Flow information Uplink:
   Identifier 14
   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
     ipv4 permit ip any any
   CS Type information:
    Ethernet CS
 Flow details Secondary(3)
  SF profile name sec3
  FSM in state SF Ready(4) on last event Up(1)
  Transaction ID used 0X800C(32780)
  Data ID local 0x8(8), remote 0x11(17)
  Data address local 11.1.6.1, remote 10.1.6.70
  Data traffic sent 0 packets, 0 bytes
  Data traffic received 0 packets, 0 bytes
  Accounting disabled
  Idle for inbound 00:03:39, outbound 00:03:39
  Service Flow information Downlink:
   Identifier 15
   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 3
       ethernet permit any 1000.2223.0004 FFFF.FFFF.FFFF any
     CS Type information:
      Ethernet CS
    Service Flow information Uplink:
     Identifier 16
     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 3
       ipv4 permit ip any any
     CS Type information:
      Ethernet CS
```

Here is an example of the BWG 2.0 **show wimax agw subscriber internal** command:

```
SAMI_BWG#sh wim agw statistics inter | in CoA

  Total CoA requests received 0
  Total CoA success notifications sent 0
  Total CoA failure notifications sent 0

SAMI_BWG6#sh wim agw statistics inter | inc L2
    Upstream L2 Data packets dropped due to error 0
    Downstream L2 Data packets dropped due to error 0


SAMI_BWG6#sh wim agw statistics inter | inc ACL
  Total uplink packets dropped due to hotlining ACL deny 0
  Total downlink packets dropped due to hotlining ACL deny 0
  Total uplink packets dropped due to user-group ACL deny 0
  Total downlink packets dropped due to user-group ACL deny 0
  Total downlink packets dropped due to paging ACL deny 0
```

In BWG Release 2.0 the **show wimax agw sub brief host** command is modified so that 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
```

Here is an example of the flow details in **show wimax agw subscriber** that indicate if a flow is critical or not:

```
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
```

show wimax agw tlv

show wimax agw tlv [**cisco** | **NWG**] [*tlv-type]*

Syntax Description

cisco	Cisco-R6 tlv type.
NWG	BWG-R6 tlv type.
tlv-type	Displays information about the supported TLVs.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
12.4(24)YG	The **cisco**, and **NWG** options were introduced.

Usage Guidelines

If a TLV type is not specified, the command will display information on all the supported TLVs.

The output of this show command contains the following information:

- TLV Type
- Name of the TLV
- Minimum and maximum allowed lengths for the TLV
- Number of nested TLVs allowed for the TLV
- Whether this TLV can be nested as part of another TLV

Examples

The following is sample output for the **show wimax agw tlv** command:

```
router# show wimax agw tlv cisco

TLV name MS Information(1/0x1)
 Maximum size is 0
 Storage type is Nested

TLV name Base Station Information(2/0x2)
 Maximum size is 0
 Storage type is Nested

TLV name SF Information(3/0x3)
 Maximum size is 0
 Storage type is Nested

TLV name RT-VR Data Delivery Service(5/0x5)
 Maximum size is 0
 Storage type is Nested
```

```
TLV name Authentication Complete(6/0x6)
 Maximum size is 0
 Storage type is Nested

TLV name BE Data Delivery Service(7/0x7)
 Maximum size is 0
 Storage type is Nested

TLV name DP Information(8/0x8)
 Maximum size is 0
 Storage type is Nested

TLV name NRT-VR Data Delivery Service(9/0x9)
 Maximum size is 0
 Storage type is Nested

TLV name UGS Data Delivery Service(13/0xD)
 Maximum size is 0
 Storage type is Nested

TLV name ERT-VR Data Delivery Service(14/0xE)
 Maximum size is 0
 Storage type is Nested

TLV name Packet Classification Rule(15/0xF)
 Maximum size is 0
 Storage type is Nested

TLV name AK Context(16/0x10)
 Maximum size is 0
 Storage type is Nested

TLV name Base Station ID(20/0x14)
 Maximum size is 8
 Storage type is Hexadecimal

TLV name Reject Cause Code(21/0x15)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name AK(22/0x16)
 Maximum size is 20
 Storage type is Hexadecimal

TLV name AK Indentifier(23/0x17)
 Maximum size is 8
 Storage type is Hexadecimal
TLV name AK Life Time(24/0x18)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name AK Sequence number(25/0x19)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Authentication Result(26/0x1A)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Anchor Gateway ID(27/0x1B)
 Maximum size is 16
 Storage type is Hexadecimal
```

```
TLV name Authenticator ID(28/0x1C)
 Maximum size is 16
 Storage type is Hexadecimal

TLV name Classifier Action(30/0x1E)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Classifier Rule Priority(31/0x1F)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name DP Identifier(GRE Key)(35/0x23)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Data Path End point Identifier(36/0x24)
 Maximum size is 4
 Storage type is Hexadecimal

TLV name Authorization Policy(40/0x28)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name PKMv2 Message Code(42/0x2A)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Registration Type(46/0x2E)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name QoS Information(48/0x30)
 Maximum size is 0
 Storage type is Nested

TLV name SDU size(55/0x37)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Service Flow Identifier(59/0x3B)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Tolerated jitter(60/0x3C)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Traffic Priority(61/0x3D)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Maximum latency(67/0x43)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Maximum sustained traffic rate(68/0x44)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Maximum traffic burst(69/0x45)
 Maximum size is 4
 Storage type is Integer - size 4 bytes
```

```
TLV name Minimum Reserved Traffic Rate(70/0x46)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Media Flow Type(72/0x48)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name IP destination address and mask(73/0x49)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name IP source address and mask(74/0x4A)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name IP TOS/DSCP range and mask(75/0x4B)
 Maximum size is 3
 Storage type is Hexadecimal

TLV name IP Protocol(82/0x52)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name Protocol destination port range(83/0x53)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name EAP Payload(85/0x55)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name Registration Context(88/0x58)
 Maximum size is 0
 Storage type is Nested

TLV name CMAC Key Count(91/0x5B)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Combined Resources Required(92/0x5C)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Context Purpose Indicator(93/0x5D)
 Maximum size is 4
 Storage type is Integer - size 4 bytes
TLV name Direction(94/0x5E)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Key Change Indicator(95/0x5F)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Protocol source port range(96/0x60)
 Maximum size is 0
 Storage type is Hexadecimal

TLV name Reduced Resources Code(97/0x61)
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Request Or Transmission Policy(98/0x62)
```

```
 Maximum size is 4
 Storage type is Integer - size 4 bytes

TLV name Reservation Action(99/0x63)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Reservation Result(101/0x65)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Unsolicited Grant Interval(102/0x66)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Unsolicited Polling Interval(103/0x67)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name CS Type(104/0x68)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name MTG Profile(105/0x69)
 Maximum size is 1
 Storage type is Integer - size 1 byte

TLV name Number of Downlink CIDs(106/0x6A)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Number of Uplink CIDs(107/0x6B)
 Maximum size is 2
 Storage type is Integer - size 2 bytes

TLV name Number of Uplink Classifiers(108/0x6C)
 Maximum size is 2
 Storage type is Integer - size 2 bytes
```

show wimax agw user-group

To display information about user groups configured on the BWG, use the **show wimax age user-group** command in Privileged EXEC mode.

show wimax age user-group [**any** | **brief** | **name** | **unauthenticated**]

Syntax Description

any	(Optional) Displays any user-group details.
brief	(Optional) Displays brief output.
name	(Optional) Displays the user-group name.
unauthenticated	(Optional) Displays unauthenticated user-group details.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(15)XL	This command was introduced.
	New CoA counters were added to the show output.

Usage Guidelines

The following information will be displayed for each user-group.

- Service mode
- Associated sessions
- Number of times User-group overwritten
- Total number of IP-CS packets and bytes sent
- Total number of IP-CS packets and bytes received
- Total number of Eth-CS packets and bytes sent
- Total number of Eth-CS packets and bytes received
- Total number of IP-GRE packets and bytes received redirected
- Total number of Ethernet-GRE packets and bytes received redirected
- Total number of new sessions rejected for the user-group by the BWG during maintenance mode

If the **brief** keyword is specified, then the output will contain a list of all the User groups currently connected in column format, as well as the following information

- Associated sessions
- Total number of packets and bytes sent
- Total number of packets and bytes received

Examples

Here is example output for the **show wimax agw user-group** command:

```
router# show wimax agw user-group
AGW User-Group-List
There are 3 user-groups configured in list wimax

User group domain name any
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


User group domain name cisco
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


User group domain name unauthenticated
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes

router#show wimax agw user-group brief ?

Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
any             0         0         0         0         0
cisco           0         0         0         0         0
unauthenticated 0         0         0         0         0

Router#show wimax agw user-group any
User group domain name any
 Service mode operational
 Sessions 0 associated
 IP-GRE Traffic Sent 0 packets, 0 bytes
 IP-GRE Traffic Received 0 packets, 0 bytes
 Ethernet-GRE traffic Sent 0 packets, 0 bytes
 Ethernet-GRE Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes
 IP-GRE Traffic Received redirected 0 packets, 0 bytes
 Ethernet-GRE Traffic Received redirected 0 packets, 0 bytes


Router#show wimax agw user-group any
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
any                       0               0         0              0                   0
 IP-GRE            -            0       0           0               0
 Eth-GRE           -            0       0           0               0
wimax.org           0               0         0              0                   0
 IP-GRE            -            0       0           0               0
 Eth-GRE           -            0       0           0               0
eap-tls.com          0               0         0              0                   0
 IP-GRE            -            0       0           0               0
 Eth-GRE           -            0       0           0               0
Unauthenticated 2         14166     4659466   14161     8553244
 IP-GRE               -         14000     4650000   161         3244
   Eth-GRE            -          166         9466         14000     8550000
```

```
Router#show wimax agw statistics arp
Last clearing of "show wimax agw statistics arp" counters never
 Total number of ARP requests received 0
 Total number of ARP reply sent 0
 Total number of ARP packets dropped 0


router#show wimax agw user-group any brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
any             0         0         0         0         0

router#show wimax agw user-group name ?
  WORD  Enter User-group Name

router#show wimax agw user-group name cisco ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group name cisco

User group domain name cisco
-------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


router#show wimax agw user-group name cisco brief ?
  |  Output modifiers
  <cr>

router#show wimax agw user-group name cisco brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
cisco 0         0         0         0         0


router#show wimax agw user-group unauthenticated ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group unauthenticated

User group domain name unauthenticated
-------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes

BWG#sh wimax agw user-group unauthenticated b
BWG#sh wimax agw user-group unauthenticated brief ?
  |  Output modifiers
  <cr>

router#show wimax agw user-group unauthenticated brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
unauthenticated    0         0         0         0           0
```

The following example illustrates the new CoA counters in BWG Release 2.0:

```
SAMI_BWG#sh wim agw user-group unauth | inc CoA

 Total CoA requests received 0
 Total CoA success notifications sent 0
 Total CoA failure notifications sent 0
```

Here is an example that shows new sessions rejected for the user-group by the BWG during maintenance mode:

```
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
```

sla profile-name

To configure the sla profile under a user group under the user group list, and to specify the number of flows that must be used for a session that is opened with this group-list, use the **sla profile-name** subcommand in user group configuration mode. Use the **no** form of the command to disable the sla profile.

sla profile-name *profile-name*

no sla profile-name *profile-name*

Syntax Description

profile-name	Specifies the profile name.

Defaults

There are no default values.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

This command configures the sla profile under the user group list. The **sla profile** specifies the number of flows that must be used for a session that is opened with this group-list. The sla profile coming from AAA will override the sla profile configured in user-group, if valid. This can be configured for other user groups as well.

Note This configuration is mandatory.

Examples

The following example illustrates the **sla profile-name** command:

```
wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  sla profile-name gold
  dhcp server primary 12.1.1.2
!
user-group domain cisco.com
  aaa accounting method-list agw
  sla profile-name gold
  ip static-allowed
  ip route aggregate auto
!
```

```
user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name gold
  ip static-allowed
  user auto-provisioning
  proxy realm cisco.com password ciscoway
```

subscriber redundancy rate

To configure broadband subscriber session redundancy policy for synchronization between high availability (HA) active and standby processors, use the **subscriber redundancy** command in global configuration mode. To delete the policy, use the no form of this command.

subscriber redundancy [bulk limit cpu *percentage* **delay** *seconds* **allow** *value***] [dynamic limit cpu** *percentage* **delay** *seconds* **allow** *value***] [delay** *time***] [rate** *sessions time***]**

no subscriber redundancy

Syntax Description

bulk limit cpu	(Optional) Configures bulk synchronization redundancy policy.
dynamic	(Optional) Configures dynamic synchronization redundancy policy.
limit cpu *percentage*	(Optional) Specifies CPU busy threshold value as a percentage. Range 0 to 100, default 90.
delay *seconds*	(Optional) Specifies delay in seconds before the CCM component synchronizes sessions after the CPU busy threshold is exceeded.
allow *value*	(Optional) Specifies the minimum number of sessions to synchronize once the CPU busy threshold is exceeded and the specified delay is met. Range is 1 to 2,147,483,637, default is 25.
delay *time*	(Optional) Specifies minimum amount of time in seconds that a session must be ready before dynamic synchronization occurs. Range is 1 to 33,550.
rate *sessions time*	(Optional) Specifies number of sessions per time period for bulk and dynamic synchronization. • sessions—Range 1 to 32,000, default is 250. • time—Range in seconds is 1 to 33,550, default is 1.

Command Default

Subscriber redundancy policy applies default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.2(31)SB2	This command was introduced.

Usage Guidelines

Cisco IOS HA functionality for broadband protocols and applications allows for stateful switchover (SSO) and in service software upgrade (ISSU) features that minimize planned and unplanned downtime and failures. HA uses the cluster control manager (CCM) to manage the capability to synchronize subscriber session bring up on the standby processor of a redundant processor system. Use the subscriber redundancy bulk command to create and modify redundancy policy used during bulk (startup) synchronization. Use the subscriber redundancy dynamic command to tune subscriber redundancy policies that throttle dynamic synchronization by monitoring CPU usage and sync rates. Use the subscriber redundancy delay command to establish session duration minimums for synchronization and manage dynamic syncing of short duration calls. Use the subscriber redundancy rate command to throttle the number of sessions to be synchronized per period.

Examples

The following example configures 300 sessions to be synchronized per second during bulk and dynamic synchronization:

```
router(config)# subscriber redundancy rate 300 1
```

timeout authentication

To configure the delay of the attachment response, use the **timeout authentication** command in user group submode. Use the no version to disable this feature.

timeout authentication *1-20*

no timeout authentication *1-20*

Syntax Description

1-20	Value in seconds of the timeout authentication response. The range is 1 to 20 seconds. The default value is 4.

Defaults

The default value is 4.

Command Modes

User group configuration sub mode.

Command History

Release	Modification
12.4(15)XL5	This command was introduced.

Usage Guidelines

This command is only configurable under the **unauthenticated** user-group.

By default, the BWG is designed to delay the Attachment Response. The BWG supports this feature only for PAP authenticated users.

Examples

The following example illustrates the use of the **timout authentication** command:

```
router(config-gw-ug)#timeout authentication 15
```

timeout cache-session

To enable the Session Caching feature and to set the cache timeout, use the **timeout cache-session** command in User Group configuration submode. Use the no form of the command to disable this feature.

timeout cache-session [**follow-dhcp-lease** | *1-259200*]

no timeout cache-session

Syntax Description

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.
1-259200	The session cache timeout value between 1 second and 259200sec (3 days).

Defaults

The default value is the **follow-dhcp-lease** option.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL4	This command was introduced.

Usage Guidelines

The 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.

Examples

The following example illustrates the default value of the **timeout cache-session** command:

```
router(config-gw-ug)# timeout cache-session follow-dhcp-lease
```

timeout idle

To specify the idle timeout for a subscriber, use the **timeout idle** command in user group configuration submode. Use the **no** form of the command to disable this feature.

timeout idle *timeout value* [**inbound**]

Syntax Description

timeout value	Value in seconds of the idle timeout. Timeout value range is 1 to 4294967 seconds. There is no default timeout value, it must be specified in the configuration.
inbound	Assumes the subscriber is idle if no upstream traffic is seen for the specified period of time.

Defaults

There are no default values. The *timeout value* must be specified in the configuration.

Command Modes

User group configuration mode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

When configured, the timer starts. If no traffic is seen for the subscriber over the session for specified period of time, then the subscriber is removed by sending a de-registration to the base station. If **inbound** is configured, the subscriber is assumed to idle if no upstream traffic is seen for the specified period of time. By default, the idle timeout feature is disabled. The idle *timeout value* can be downloaded from the AAA server as well, and if downloaded the AAA value is given precedence over the configured value.

Examples

The following example illustrates the **timeout idle** command:

```
router(config-gw-ug)#timeout idle 15
```

timeout session

To specify the session or absolute timeout value for a subscriber, use the **timeout session** command in user group configuration submode. Use the **no** form of the command to delete the timeout session values for a subscriber.

timeout session *timeout value*

no timeout session

Syntax Description

timeout value	Specifies the timeout session value in seconds. The *timeout value* range is 1 to 4294967 seconds. There is no default timeout value, it must be specified in the configuration.

Defaults

The session timeout feature is disabled by default. The *timeout value* range is 1 to 4294967 seconds. There is no default timeout value, it must be specified in the configuration.

Command Modes

User group configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

When configured, the session timeout timer is started on the successful authentication of authenticated calls, or when the traffic path is ready for unauthenticated calls. Upon successful reauthentication, the timer is restarted.

Examples

The following example configures a session timeout value of 3600 seconds:

```
router(config-gw-ug)#timeout session 3600
```

tolerated-jitter

To configure the maximum delay variation (jitter) for the service flow connection, use the **tolerated-jitter** subcommand in service flow QoS information configuration submode. Use the **no** form of the command to disable this function.

tolerated-jitter *tolerated-jitter-value*

no tolerated-jitter *tolerated-jitter-value*

Syntax Description

tolerated-jitter-value	Specifies the maximum delay variation value for the service flow connection. The range is *0-4294967295* measured in bits per second

Defaults

There are no default values.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	

Examples

The following example illustrates the **tolerated jitter** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
```

```
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

traffic-priority

To specify the priority assigned to a service flow, use the **traffic-priority** subcommand in service flow QoS information configuration submode. Use the **no** form of the command to disable the command.

traffic-priority *traffic-priority-value*

no traffic-priority

Syntax Description

traffic-priority-value	Specifies the priority value assigned to a service flow. The range is *0-7*. Higher numbers indicate higher priority. Default value is 0.

Defaults

Default value is 0.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If two service flows are identical in all QoS parameters except priority, the higher priority service flow is given lower delay, and higher buffering preference. For non-identical service flows, the priority parameter does not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.

Examples

The following example sets the service flow priority value to **1** and **3**:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
```

```
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

unsolicited-interval-grant

To specifies the nominal interval between successive data grant opportunities for this service flow, use the **unsolicited-interval-grant** command in service flow QoS information configuration submode. Use the **no** form of the command to disable this feature.

unsolicited-interval-grant *unsolicited-interval-grant-value*

no unsolicited-interval-grant

Syntax Description

unsolicited-interval-grant-value	Specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for a UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec). The range is *0-65535* measured in milliseconds.

Defaults

No default behavior or values.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example illustrates the use of the **unsolicited-interval-grant** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
```

```
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

unsolicited-interval-polling

To specify the maximal nominal interval between successive polling grant opportunities for a service flow, use the **unsolicited-interval-polling** command in service flow QoS information configuration submode.

unsolicited-interval-polling *unsolicited-interval-polling-value*

Syntax Description

unsolicited-interval-polling-value	Specifies the maximal nominal interval between successive polling grant opportunities for a service flow. The range is *0-65535* measured in milliseconds.

Defaults

There are no default values.

Command Modes

Service flow QoS information configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following is sample output for the **unsolicited-interval-polling** command:

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
 unsolicited-interval-polling 91
!
```

```
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

user auto provisioning

To instruct the BWG to allow a user entry even after receiving an Access-Reject from the RADIUS server, use the **user auto provisioning** command in user configuration mode. Use the **no** form of the command to disable user auto provisioning.

user auto provisioning

no user auto provisioning

Syntax Description

There are no keywords or arguments.

Defaults

There are no default values.

Command Modes

User group configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

If this command is not configured, users will not be allowed to enter.

This command can be configured for other user groups, but configuring it for a user group other that unauthenticated does not enable this feature for those user groups.

Examples

The following example illustrates how to configure unauthenticated users:

```
user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name gold
  ip static-allowed
  user auto-provisioning
  proxy realm cisco.com password ciscoway
```

user-group (user group list configuration submode)

To configure a user group under the user group list, use the **user-group** subcommand in user group list configuration submode.

user-group {**any** | **unauthenticated** | **domain** *domain-name*}

no user-group {**any** | **unauthenticated** | **domain** *domain-name*}

Syntax Description

any	Configures any user group - For an authenticated user where no user-group based on the domain is found, they are defaulted into this category. For example, if you receive a user with the NAI "abc@cisco2.com" but do not have a user-group domain for cisco2.com, this user will fall into the **any** user group category.
unauthenticated	Configures all unauthenticated users of the user groups.
domain	Configures domain based user groups - In cases where the user is authenticated, the AGW will try to discover the user based on the domain name part of the NAI received. The NAI received is expected to be of the format "userpart@domain". In order to match a user-group (for example, abc@cisco.com), you need to configure user-group domain "cisco.com" and put all per-domain configurations under this user-group.
domain-name	Specifies the domain name.

Defaults

There are no default values.

Command Modes

User group list configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

Release 1.0 of the Cisco BWG supports the user-groups **any** and **unauthenticated**.

Examples

The following example illustrates how to configure unauthenticated users:

```
Router(config-gw-ugl)#user-group unauthenticated
```

vlan (service flow direction cs-type submode)

To specify the vlan to vrf mapping (frames with a particular vlan-id will be mapped to what vrf-name), use the **vlan** command in service flow direction cs-type submode. Use the **no** form of the command to disable vrf mapping.

vlan {*2-4095* **| range** *2-4095 2-4095***} vrf** *vrf-name*

no vlan

Syntax Description

range *2-4095 2-4095*	(Optional) Specifies the range of vlan-ids mapped to a vrf-name.
vrf *vrf-name*	Specifies the vrf name.

Defaults

There are no default values.

Command Modes

Service flow direction cs-type configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

Note vlan-vrf mapping can only be configured for ethernet-cs for direction uplink.

Examples

The following example illustrates how to configure the **vlan** command:

```
router(config-gw-sf-dir-cstype)# direction uplink
  cs-type ip-cs
   pak-classify-rule isf-classifier-uplink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-uplink
   precedence 2
   vlan 2 vrf vrf_1
   vlan range 3 10 vrf vrf_2
   vrf-default vrf_1
  qos-info isf-qos-uplink
```

vrf (user group configuration submode)

To configure the VRF, use the **vrf** command in user group configuration submode. Use the **no** form of the command to delete the VRF.

vrf *vrf-name*

no vrf *vrf-name*

Syntax Description

vrf-name	Specifies the name of the vrf.

Defaults

By default, no user groups belong to any VRF.

Command Modes

User group configuration submode.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

Multiple user groups can share the VRF.

Examples

The following example illustrates how to configure a **vrf** named “cisco”:

```
Router(config-gw-ug)#vrf cisco
```

vrf-default

To specify the default vrf mapping, use the **vrf-default** command in service flow direction cs-type submode. Use the **no** form of the command to disable vrf mapping.

vrf-default *vrf-name*

no vrf-default

Syntax Description

vrf-name	Specifies the name of the vrf.

Defaults

There are no default values.

Command Modes

Service flow direction cs-type submode configuration submode.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

This is an optional configuration command that specifies the default vrf mapping. Uplink frames without a vlan-id, or with a vlan-id that is not configured under this cs-type with a vlan-vrf mapping will be mapped to the vrf-name configured using the above CLI.

Note **vrf-default** can be configured for ethernet-cs and ip-cs for direction uplink only.

Examples

The following example illustrates how to configure the **vrf-default** command:

```
router(config-gw-sf-dir-cstype)# direction uplink
  cs-type ip-cs
   pak-classify-rule isf-classifier-uplink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-uplink
   precedence 2
   vlan 2 vrf vrf_1
   vlan range 3 10 vrf vrf_2
   vrf-default vrf_1
  qos-info isf-qos-uplink
```

wimax agw

To configure various subcommand modes, use the **wimax agw** global configuration command.

wimax agw [**base-station** | **idlemode** [**entry-timout** *sec* | **update-timout** *sec*] | **maximum** | **paging-controller** *word* | **paging-group** | **pmip** | **redundancy** | **service-flow** | **sla** | **slb** | **user**]

Syntax Description

base-station	Specifies WiMAX AGW Base Station configuration commands.
idlemode	Specifies WiMAX AGW Idlemode configuration commands.
entry-timout *sec*	Specifies the timer used for the network suggested Idle mode entry. The range is 10-600 seconds, and the default value is 10 seconds.
update-timout *sec*	Specifies the timer to use for the network forced location update through paging. The range is 128-65536 seconds and the default value is 4096 seconds.
maximum	Specifies WiMAX AGW maximum configuration commands.
paging-controller *word*	Specifies WiMAX AGW Paging Controller configuration commands. *word* specifies the paging controller group name, which should be the same as the Generic Load Balancing Protocol (GLBP) group.
paging-group	Specifies WiMAX AGW Paging Group configuration commands.
pmip	Specifies Proxy Mobile IP configuration commands.
redundancy	Specifies that WiMAX AGW Session Redundancy is enabled.
service-flow	Specifies User group Service Flow configuration commands
sla	Specifies Service Level Agreement configuration commands.
slb	Specifies WiMAX AGW Session SLB configuration commands.
user	Specifies GW user configuration commands.

Defaults

The **entry-timout** default value is 10 seconds, the **update-timout** default value is 4096 seconds.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Usage Guidelines

This CLI is only necessary on a SAMI platform that is using SLB for load balancing. This CLI should not be configured for 7301 platform. This CLI can only be configured if one of the interfaces on the gateway is configured for GLBP because a valid GLBP group-name is input to this CLI. If this CLI is configured on the Cisco 7301, then (by default) GLBP is also configured on one of the interfaces and the entire feature is supported on 7301 platform as well.

wimax agw base-station group

To configure a base-station group, and to ensure that all of the individual base stations configured to belong to this base station group will use the base station group parameters, use the **wimax agw base-station group** command in global configuration mode. This command also places you in base station configuration submode. Use the **no** form of the command to delete a base station group.

wimax agw base-station group *name*

Syntax Description

name	Specifies the name of the base station group.

Defaults

The default behavior is that there are no base station groups.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Examples

The following example creates a base station group named “cisco”:

```
router(config)#wimax agw base-station group cisco
```

wimax agw hotline profile

To configure a hotline profile on the BWG, and to enter the GW hotline configuration sub mode, use the **wimax agw hotline profile** global configuration command. Use the **no** form of the command to remove the profile.

wimax agw hotline profile *profile-name* [**ip access-group** *num in* | *out* **passthru**] [**http access-group** *num* **redir-url** *url*]

no wimax agw hotline profile

Syntax Description

profile-name	Specifies the name of the profile.
ip access-group *num*	Enables an access group and specifies the access group number.
in	Upstream packet flow.
out	Downstream packet flow.
passthru	Packets passing the filter rule defined by the ACL are allowed to pass.
http access-group *num* **redirect** *url*	Packets passing the filter rule are dropped and a downstream http packet with the specified url is sent to the MS.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Usage Guidelines

A subscriber can be hot-lined at the start of their packet data service or mid-session with AAA-based CoA. The AAA Access Accept is used to hot-line the user's session at the session startup time. If the session receives a AAA CoA with the hot-lining status on in the middle of the session, the user's data traffic will be re-directed. Similarly the hot-lining status can be removed during mid-session, or at the start of a new session. Hotline profile is selected based on the hotline profile received from the AAA. To disable hot-lining, the AAA server can choose a special profile name called "hotlining-exit" (case insensitive).

Similar to SLA profile, the AAA server simply selects a hotline profile. To disable hot-lining, the AAA server can choose a special profile name called "hotlining-exit" (case insensitive). Once it receives this special profile name, the BWG resumes normal traffic for the subscriber. In order to avoid confusion, this special profile name should not be used as a normal hotline profile name.

Examples

Here is an example of the **wimax agw hotline profile** command:

```
BWG#sh run | inc hotline
wimax agw hotline profile XYZ
   ip access-group 101 in passthru
   http access-group 102 redir-url www.hotlined.com
   ip access-group 101 out passthru
```

wimax agw pmip profile

To configure a PMIP profile on the BWG, and to enter the GW PMIP configuration sub mode, use the **wimax agw pmip profile** global configuration command. Use the **no** form of the command to remove the profile.

wimax agw pmip profile *pmip-profile-name*

no wimax agw pmip profile *pmip-profile-name*

Syntax Description

pmip-profile-name	Specifies the name of the PMIP profile.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(24)YG	This command was introduced.

Usage Guidelines

The PMIP profile includes all the PMIP attributes used for establishing a PMIP call. You can associate a PMIP profile with a user-group by configuring subcommand **pmip profile** *profile name*.

PMIP attributes can be provisioned from AAA and overwrite the user-group PMIP profile defined attributes. You need to define a PMIP profile in the user-group to enable PMIP, or you can enable PMIP by getting the attributes from AAA.

Examples

Here is an example of the **wimax agw pmip profile** command:

```
wimax agw pmip profile pmip1
 home-agent
  address 14.1.1.80
  ha-rk-key ascii rootcisco spi decimal 258 lifetime 6000
 proxy-mn
  gre-tunneling-enable
  no host-config-ext-request
  mn-ha-key ascii cisco spi 102 lifetime 3000
  coa-address 14.1.1.100
```

wimax agw r6 maximum base-station

To specify the maximum number of base stations that are allowed to connect to the AGW, use the **wimax agw r6 maximum base-station** command in global configuration mode. Use the **no** form of the command to disable this feature.

wimax agw r6 maximum base-station *number*

no wimax agw r6 maximum base-station

Syntax Description

number	Specifies the maximum number of base stations that are allowed to connect to the BWG. The maximum number range is *1-16384*. The expected throughput per BS will dictate the number of BSs that can connect.

Defaults

The maximum number of base stations that are supported on the BWG platform is 500.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If you do not configure this command, the number of base stations allowed to connect to the BWG is set to the maximum number supported by the platform.

Examples

The following example allows 240 base stations to connect to the BWG:

```
wimax agw r6 maximum base-station 240
```

wimax agw r6 maximum subscriber

To specify the maximum number of subscriber sessions allowed on the BWG, use the **wimax agw r6 maximum subscriber** command in global configuration mode. Use the **no** form of the command to disable this feature.

wimax agw r6 maximum subscriber *number*

no wimax agw r6 maximum subscriber *number*

Syntax Description

number	Specifies the maximum number of subscriber sessions on the BWG. The range is 1-20000.

Defaults

The default maximum number of subscriber sessions is 20000

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

If you do not configure this command, the number of subscriber sessions supported on the BWG platform is set to its maximum value.

Examples

The following example limits the number of subscriber sessions on the BWG to 50:

```
Router(config)#wimax agw r6 maximum subscriber 50
```

wimax agw redundancy

To enable session redundancy on the BWG, use the **wimax agw redundancy** command in global configuration mode. Use the **no** form of the command to disable this feature. You must clear all subscribers to configure the **no** form of the command.

wimax agw redundancy

no wimax agw redundancy

Syntax Description

There are no keywords or arguments.

Defaults

This command is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

You must clear all subscribers to configure **no wimax agw redundancy**. Here is an example:

```
AGW-2(config)#no wimax agw redundancy
ERROR: Clear all subscribers (1) before unconfig. redundancy
AGW-2(config)#
```

Examples

The following example enables session redundancy on the BWG:

```
Router(config)# wimax agw redundancy
```

wimax agw service-flow pak-classify-rule profile

To configure a service-flow packet classification rule profile on the BWG, or to enter the service flow packet classify configuration submode, use the **wimax agw service-flow pak-classify-rule profile** global configuration command. Use the **no** form of the command to remove the profile, or exit the submode.

wimax agw service-flow pak-classify-rule profile *profile-name*

no wimax agw service-flow pak-classify-rule profile

Syntax Description

profile- name	Specifies the name of the service-flow packet classification rule profile on the BWG. The profile name is case insensitive.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

These profiles are configured under the convergence sub layer type (cs-type) in predefined service flows that are to be opened for the subscriber.

Examples

Here is an example of a pre-defined service flow classifier rule profile

```
wimax agw service-flow pak-classify-rule profile profile_name
priority number
    ipv4 --> same as before
    ethernet permit src_mac | any src_mac_mask | all dst_mac | any dst_mac_mask | all
ethernet_type
    vlan permit number | any priority number | any | range number start number end
```

wimax agw service-flow profile

To configure a service-flow profile on the BWG, and to enter the GW service flow profile configuration submode, use the **wimax agw service-flow profile** command in global configuration mode. Use the **no** form of the command to disable this feature and remove the profile.

wimax agw service-flow profile *service-flow-profile-name*

no wimax agw service-flow profile *service-flow-profile-name*

Syntax Description

service-flow-profile-name	Specifies the name of the service flow profile. The profile name is case insensitive.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

These service flows are predefined and are opened for the subscriber.

Configuring the command will open the GW service flow profile configuration submode.

The **precedence** is used as a tie-breaker when an MS can support more than one CS Type (for example, IPCS and EthCS and VLAN CS). In these scenarios, the BWG selects the CS-type based on precedence.

As an example, consider that the MS sends the CS capability in the attachment request with a bit map set to indicate it only supports eth-cs, and the precedence of the eth-cs in the BWG is 2. Then the BWG would pick CS-type of Ethernet CS. However, if the MS supports both, and the BWG configuration has ip-cs with a precedence set to 1, then the BWG would pick CS-type of IP-CS.

Examples

The following example illustrates a configuration with a predefined service flow profile named “cisco2”:

```
router(config)wimax agw service-flow pak-classify-rule profile cisco 2
direction uplink
          cs-type ip-cs|ethernet-cs
               precedence 1/2/
               pak-classify-rule classifier_profile
               vlan range 2-4095 2-4095 vrf vrf_name
               default-vrf vrf_name
          qos-info-profile name
direction downlink>
         cs-type ip-cs/ethernet-cs
               precedence 1/2
               pak-classify-rule classifier_profile
          qos-info-profile name
```

wimax agw service-flow profile qos-info

To configure a service-flow QoS information profile on the BWG, or to enter service flow qos info configuration submode, use the **wimax agw service-flow profile qos-info** command in global configuration mode. Use the **no** form of the command to remove the profile.

wimax agw service-flow profile qos-info *service-flow-qos-info-profile-name*

no wimax agw service-flow profile qos-info *service-flow-qos-info-profile-name*

Syntax Description

service-flow-qos-info-profile-name	Specifies the name of the service flow QoS information profile.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

You can configure a service-flow QoS information profile on the BWG that is associated to predefined service flows that are opened for the subscriber.

Examples

The following example specifies the service flow profile name as “upstreamprofile”:

```
Router(config)#wimax agw service-flow profile qos-info upstreamprofile
```

wimax agw sla profile

To configure the Service level agreement (SLA) on the BWG, and to enter GW SLA configuration sub mode, use the **wimax agw sla profile** command in global configuration mode. Use the **no** form of the command to remove the profile.

wimax agw sla profile *sla-profile-name*

no wimax agw sla profile *sla-profile-name*

Syntax Description

sla-profile-name	Specifies the name of the service flow profile.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL1	This command was introduced.

Usage Guidelines

The SLA profile includes all the flows. The BWG will enforce a limit for the number of service flows to 4 for each SLA profile. Attempting to exceed the limit will result in a failure.

For Cisco BWG Release 1.1, the same vlan should be configured in the same SLA profile.

Different service flows get listed under one SLA profile. You can associate an SLA with a user-group by configuring subcommand **sla profile** *profile name*. Provisioning the SLA allows you to better manage the service flows.

If not configured, there is no other provision to define flows:

```
wimax agw sla profile silver
 service-flow pre-defined isf profile isf
 service-flow pre-defined secondary 1 profile sec1
```

This command moves the ability to configure the service flow commands from the **user-group**.

You need to configure this sla profile in the user-group, to define how many flows will be allowed for that user-group.

Examples

The following example specifies the service flow profile name as “upstreamprofile”:

```
Router(config)#wimax agw sla profile gold
    service-flow pre-defined isf profile isf encap-type none vlan 10
    service-flow pre-defined secondary profile sec1 encap-type none vlan 10
```

wimax agw slb notify

To enable the BWG to send notification to the SLB, use the **wimax agw slb notify** global configuration command. Use the **no** form to disable this feature.

wimax agw slb notify {**update** | **delete**}

no wimax agw slb notify {**update** | **delete**}

Syntax Description

update	Enables sending of update notification to SLB.
delete	Enables sending of delete notification to SLB.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)YX4	This command was introduced.

Examples

Here is an example of the **wimax agw slb notify** command:

```
router(config)# wimax agw slb notify delete
```

wimax agw slb port

To use the **wimax agw slb port** global configuration command. Use the **no** form to disable this function.

wimax agw slb port *port* **vserver** *vserver* **[next-hop ip** *ip_addr* **vrf** *vrf_name***]**

no wimax agw slb port *port* **vserver** *vserver* **[next-hop ip** ***ip_addr*** **vrf** *vrf_name***]**

Syntax Description

port	Specifies the port number. The range is *49152-65535*.
vserver *vserver*	Specifies the vserver.
next-hop ip *ip_addr*	Specifies the next hop address.
vrf *vrf_name*	Specifies the vrf.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)YX4	This command was introduced.

Usage Guidelines

For session deletion/update notification, this command is required . Both, **next-hop ip** *ip address* and **vrf** *vrf name*, are optional. In the absence of next-hop ip address, you will have to input a static route to reach the virtual server.

wimax agw user group-list

To configure the User group list on the BWG, and to enter user group list configuration subcommand mode, use the **wimax agw user group-list** command in global configuration mode. Use the **no** form of the command to remove the user group lists, or to exit user group list configuration subcommand mode.

wimax agw user group-list *user-group-list-name*

no wimax agw user group-list *user-group-list-name*

Syntax Description

user-group-list-name	Specifies the name of the user group list.

Defaults

The default behavior is that there are no configured user group lists.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XL	This command was introduced.

Usage Guidelines

There can be only one user group list allowed on a single processor of the BWG.

The **no** version of command will remove the user group list. This will create a user group list sub configuration mode to create multiple user groups under the user-group list created.

The **aaa authentication method-list** *xxxx* in the example below indicates if the RADIUS Access Request is initiated from the BWG for the group. If the CLI is not configured, the AAA query is not required.

The **proxy realm** *sprint.com* **password** *ciscoway* instructs the BWG how to populate the RADIUS Access Request message. If configured, the user name is constructed as *mac@realm* (for example, *mac*@sprint.com). If the realm is not configured, the user name is simply *mac*. The *cisco* argument is used as passwd if not configured. These two CLIs are applicable for other user groups (EAP users) as well. The reply from the AAA server contains the user's real domain name, which is used for selecting a local user group. It should also be noted that the above scheme should not break EAP-authenticated users. In other words, the BWG should allow EAP and non-EAP authenticated users to coexist. For authenticated users, the user name is acquired from CPE through the EAP identity request. EAP uses NAI in Access request to the AAA. If the response from the AAA includes the SLA Profile Name and the User Domain Name for EAP users, the result from the AAA will override those determined earlier.

Examples

The following example configures a user group list named “cisco”:

```
Router(config)#wimax agw user group-list cisco
```

The **wimax agw user group-list** command supports route aggregate at per user-group level. The following example shows how to configure route aggregation:

```
AGW-1(config)#wimax agw user group-list wimax
AGW-1(config-gw-ugl)#user-group unauthenticated
AGW-1(config-gw-ug)#?
GW user group sub configuration commands
  aaa           User group AAA configuration commands
  default       Set a command to its defaults
  dhcp          User group DHCP configuration commands
  exit          Exit user group sub configuration
  ip            User group IP configuration commands
  no            Negate a command or set its defaults
  security      User group security configuration commands
  service-flow  User group service-flow configuration commands
  timeout       User group timeout configuration commands
  vrf           User group VRF configuration commands
  proxy         Proxy to enter realm and password
  sla           User group service level agreement configuration commands
  user          Allow user-autoprovisioning


AGW-1(config-gw-ug)#ip
AGW-1(config-gw-ug)#ip ?
  access-group  Specify access control for packets
  address       User group address configuration commands
  route         User group route confiugration commands

AGW-1(config-gw-ug)#ip rou
AGW-1(config-gw-ug)#ip route ?
  aggregate  Configure aggregate range

AGW-1(config-gw-ug)#ip route
AGW-1(config-gw-ug)#ip route aggregate ?
  A.B.C.D  {/nn || A.B.C.D}  IP prefix and prefix mask
  auto                       will aggregate routes automatically base on the
                             mask return by servers

AGW-1(config-gw-ug)#ip route aggregate auto
AGW-1(config-gw-ug)#
```

For un-authenticated users, we do not get the user name from the CPE. In this case, the user name, realm and password are based on the following CLI.

```
!
wimax agw user group-list wimax
 user-group unauthenticated
  aaa authentication method-list xxxx
  proxy realm sprint.com passwd ciscoway
  sla profile-name silver
 !
```

User Auto-Provisioning

There are occasions when users may be admitted into the network for a short while even if AAA does not have provisioning for them. To enable this feature, the related user group should be properly configured. When it is enabled, the session timer in the user group should be configured to a small value so that free use of the network is limited.

Auto-provisioning is not supported for EAP users. It will not take effect when configured with any user group other than the unauthenticated.

Auto-provision in not supported for hosts with static IP and IPCS.

```
!
wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
sla profile-name silver
  user auto-provisioning
  timeout session 600
 !
!
```