

Command Reference

13 September 2007

The following commands are new or changed in Cisco ASN GW 1.0 for IOS Release 12.4(15)XL:

- [aaa accounting network, page -4](#)
- [aaa accounting update, page -10](#)
- [aaa authentication, page -12](#)
- [clear wimax agw bs, page -14](#)
- [clear wimax agw redundancy statistics, page -15](#)
- [clear wimax agw subscriber, page -16](#)
- [data-delivery-service, page -17](#)
- [debug ip slb, page -19](#)
- [debug condition, page -21](#)
- [debug eap, page -22](#)
- [debug eap authenticator, page -24](#)
- [debug ip packet, page -26](#)
- [debug ip slb, page -32](#)
- [debug radius, page -34](#)
- [debug radius, page -34](#)
- [debug wimax agw aaa, page -36](#)
- [debug wimax agw message, page -38](#)
- [debug wimax agw message tlv, page -42](#)
- [debug wimax agw path, page -44](#)
- [debug wimax agw r6 flow, page -46](#)
- [debug wimax agw r6 session, page -48](#)
- [debug wimax agw r6 subscriber, page -53](#)
- [debug wimax agw redundancy, page -54](#)
- [debug wimax agw switching, page -67](#)
- [debug wimax agw vtemplate, page -71](#)
- [dhcp gateway address, page -72](#)
- [direction, page -73](#)
- [direction, page -73](#)
- [encapsulation agw, page -74](#)
- [ip access-group, page -75](#)
- [ip address allocation subscriber timeout, page -76](#)

- [maximum-latency, page -77](#)
- [maximum-traffic-burst, page -79](#)
- [maximum-traffic-rate-sustained, page -81](#)
- [media-flow-type, page -83](#)
- [minimum-traffic-rate-reserved, page -85](#)
- [pak-classify-rule, page -86](#)
- [policy-transmission-request, page -87](#)
- [priority permit, page -89](#)
- [qos-info, page -91](#)
- [radius-server vsa send accounting wimax, page -92](#)
- [radius-server vsa send authentication wimax, page -93](#)
- [reduced-resources-code, page -94](#)
- [reference-point r6, page -95](#)
- [reference-point r6 response retransmits, page -96](#)
- [reference-point r6 response timeout, page -97](#)
- [sdu-size, page -98](#)
- [security subscriber address-filtering ingress, page -100](#)
- [service-flow pre-defined profile, page -101](#)
- [set, page -102](#)
- [service wimax agw, page -104](#)
- [show ip slb sessions, page -105](#)
- [show wimax agw, page -107](#)
- [show wimax agw message, page -109](#)
- [show wimax agw path, page -112](#)
- [show wimax agw redundancy, page -114](#)
- [show wimax agw statistics, page -115](#)
- [show wimax agw subscriber, page -117](#)
- [show wimax agw tlv, page -120](#)
- [show wimax agw user-group, page -125](#)
- [subscriber redundancy rate, page -128](#)
- [timeout idle, page -130](#)
- [timeout session, page -131](#)
- [tolerated-jitter, page -132](#)
- [traffic-priority, page -134](#)
- [unsolicited-interval-grant, page -136](#)
- [unsolicited-interval-polling, page -138](#)
- [user-group \(user group list configuration subcommand\), page -140](#)
- [vrf \(user group configuration submode\), page -141](#)

- [wimax agw base-station group, page -142](#)
- [wimax agw base-station ip-addr any group, page -143](#)
- [wimax agw r6 maximum base-station, page -144](#)
- [wimax agw r6 maximum subscriber, page -145](#)
- [wimax agw redundancy, page -146](#)
- [wimax agw service-flow pak-classify-rule profile, page -147](#)
- [wimax agw service-flow profile, page -148](#)
- [wimax agw service-flow profile qos-info, page -149](#)
- [wimax agw user group-list, page -150](#)

aaa accounting network

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 might return 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.
<i>list-name</i>	Character string used to name the list of at least one of the following accounting methods: <ul style="list-style-type: none"> • 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 <i>group-name</i> argument.
vrf vrf-name	(Optional) Specifies a virtual routing and forwarding (VRF) configuration. VRF is used <i>only</i> 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 “start” accounting notice was received by the accounting server.
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.
group <i>group-name</i>	Specifies the accounting method list. Enter at least one of the following keywords: <ul style="list-style-type: none"> • auth-proxy—Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service. • commands—Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level. • connection—Creates a method list to provide accounting information about all outbound connections made from the network access server. • exec—Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • network—Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions. • resource—Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated. • tunnel—Creates a method list to provide accounting records (Tunnel-Start, Tunnel-Stop, and Tunnel-Reject) for virtual private dialup network (VPDN) tunnel status changes. • tunnel-link—Creates a method list to provide accounting records (Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject) for VPDN tunnel-link status changes.

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.

Release	Modification
12.1(5)T	The auth-proxy keyword was added.
12.2(1)DX	The vrf keyword and <i>vrf-name</i> 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 <i>vrf-name</i> 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 <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server <i>group-name</i> 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.

Command	Description
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 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 <i>number</i> .
<i>number</i>	(Optional) Integer specifying number of minutes.
jitter	(Optional) Allows you to set the maximum jitter value in periodic accounting.
maximum <i>max-value</i>	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.
<i>method1 [method2...]</i>	At least one of these keywords: <ul style="list-style-type: none"> • 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.

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.
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.

clear wimax agw bs

To clear all the subscribers that belong to this base station, and clear the base station details, use the **clear wimax agw bs** command in global configuration mode.

clear wimax agw bs *bs-ip-address*

Syntax Description	<i>bs-ip-address</i>	IP address of a specific base station.
--------------------	----------------------	--

Defaults	There are no default values.
----------	------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

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



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

For example:

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

Examples	The following example illustrates how to enable the clear wimax agw bs command:
----------	--

```
router#clear wimax agw bs bs-ip-address
```

clear wimax agw redundancy statistics

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

clear wimax agw redundancy statistics

Syntax Description This command has 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.



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

For example:

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

Examples The following example clears all ASN GW redundancy statistics:

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

clear wimax agw subscriber

To clear the subscriber on the AGW, use the **clear wimax agw subscriber** command in global configuration mode.

```
clear wimax agw subscriber [mac-id mac-id ] [local]
```

Syntax Description	mac-id <i>mac-id</i>	Specifies the MAC ID of the subscriber. If the MACID is not specified the entire subscriber list is cleared.
	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 Global configuration.

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



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

For example:

```
asngw#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
```


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		Configures 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 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.

```
debug ip slb { conns | dfp | icmp | reals | asnr6 | all }
```

```
no debug ip slb { conns | dfp | icmp | reals | asnr6 | all }
```

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.
reals	Displays debugging messages for all real servers defined to Cisco IOS SLB.
asnr6	Displays debugging messages for the packet path inside ASNLB.
all	Displays all debugging messages for Cisco IOS SLB.

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 introduced.

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 command:

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

```
SLB All debugging is on
```

```
Router#
```

The following example stops all debugging:

```
Router# no debug all
```

All possible debugging has been turned off

debug condition

To enable conditional debugging on the ASN GW, 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 <i>mac-id-of-subscriber</i>	based on the Subscriber MAC-ID
ip <i>bs-ip-address</i>	based on the BS IP address

Defaults

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 AGW related debugs, enter:

```
router#debug wimax agw
```

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

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

Examples

The following example enables conditional debugging on the ASN GW:

```
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
asn# 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
asn#
*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

<i>access-list-number</i>	(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 7](#) describes the significant fields shown in the display.

Table 7 *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 8 describes the significant fields shown in the display.

Table 8 *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
070033D0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M
070033E0: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +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 9 describes the significant fields shown in the display.

Table 9 *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 10 describes.

Table 10 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`.

```
debug ip slb {conns | dfp | icmp | asnr6 | reals | all}
```

```
no debug ip slb {conns | dfp | icmp | asnr6 | reals | all}
```

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 ASN GW 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.

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.

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
```



```
Router#
```

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 brief
Radius protocol 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>Received Absolute(session) timeout 1500 secs
*Feb 23 07:53:49.689: AGW-Auth: <1000003B0009>Received 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 ASNGW.

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#
asn#
*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 open command is run on the simulator, and the debug messages are observed on the ASNGW.

debug wimax agw message

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

debug wimax agw message [events | errors | dump]

Syntax Description	events	errors	dump
	Displays brief information on the processing of all transmitted and received messages.	Displays details of any errors encountered during message processing.	Displays details of all transmitted and received messages. Output will include the following: <ul style="list-style-type: none"> • 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.

Usage Guidelines

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 ASN GW 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	errors	dump
	Displays brief information on the encoding and decoding of all TLVs.	Displays details of any errors encountered during TLV encoding and decoding.	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 msec
*Feb 23 10:35:25.428: AGW-Path: <(SU)-10.1.1.70>Expired purge timer after 20000 msec
*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 msec
*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 msec
*Feb 23 10:34:32.392: AGW-Path: <(DG)-10.1.1.70>Expired purge timer after 20000 msec
*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 msec
*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 ASN GW 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 msec, timer type 2(16)
*Feb 23 10:18:00.996: AGW-Flow: <100022230001><F[21]>Starting pak resend timer 0x207497F0
for 10000 msec 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 msec 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 ASN GW 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.

Usage Guidelines

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 msec, timer type 1(2)
*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Starting pak resend timer 0x654986B8 for
10000 msec 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 msec 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 msec, timer type 1(8)
```



```

*Feb 23 12:55:34.715: AGW-Sess: <1000222A0001>Starting pak resend timer 0x2034967C for
10000 msec 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 msec 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, agr
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 msec, timer type 1(2)
*Feb 23 08:51:02.728: AGW-Sess: <067611141111>Starting pak resend timer 0x65AEF5B4 for
10000 msec 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 msec 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 msec, timer type 1(10)
*Feb 23 08:51:02.788: AGW-Sess: <067611141111>Starting pak resend timer 0x654986B8 for
10000 msec 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 msec 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 msec, timer type 1(11)

```

```

*Feb 23 08:54:17.556: AGW-Sess: <067622242222>Starting pak resend timer 0x65F35C00 for
10000 msec 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 msec 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 msec, timer type 1(2)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msec 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 msec 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 msec, timer type 1(8)
*Feb 23 08:56:35.700: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msec 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 msec 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
AGW-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 msec, timer type 1(2)
*Feb 23 08:59:07.448: AGW-Sess: <067611141111>Starting pak resend timer 0x65F35C00 for
10000 msec 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 msec 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 msec, timer type 1(10)
*Feb 23 08:59:07.504: AGW-Sess: <067611141111>Starting pak resend timer 0x506F3A88 for
10000 msec 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 msec 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 Dereg
Req(19) with retcode Ok(0)
*Feb 23 08:57:13.696: AGW-SessFSM:<100022230001>Deleting(8) -> Deleting(8) on event Rx
Dereg 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 msec, timer type 1(11)
*Feb 23 08:57:13.696: AGW-Sess: <100022230001>Starting pak resend timer 0x65F35C00 for
10000 msec 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 msec 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 ASN GW 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 ASN GW 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 ASN GW redundancy information:

```
debug wimax agw redundancy events
```

Output on ACTIVE ASNGW for MS Open

```
ASNGW#
*Mar 21 06:25:48.688: AGW-SR: Type AGW_MAC_ID(0), Length 6, Class Mandatory
*Mar 21 06:25:48.688: AGW-SR: Value <067611131111>
*Mar 21 06:25:48.688: AGW-SR: Type AGW_SUB_AUTH_POLICY(1), Length 2, Class Mandatory
*Mar 21 06:25:48.688: AGW-SR: Value <18>
*Mar 21 06:25:48.688: AGW-SR: Type AGW_SUB_AUTH_AK(3), Length 20, Class Optional
*Mar 21 06:25:48.688: AGW-SR: Value <32FE0D9681EBDCFCDA1ECBA65BC764B52D80E90D>
*Mar 21 06:25:48.688: AGW-SR: Type AGW_SUB_AUTH_AK_METHOD(2), Length 4, Class Optional
*Mar 21 06:25:48.688: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB_AUTH_AKID(4), Length 8, Class Optional
*Mar 21 06:25:48.692: AGW-SR: Value <90DDCD514678A29E>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB_AUTH_AKLIFETIME(5), Length 2, Class Optional
*Mar 21 06:25:48.692: AGW-SR: Value <15000>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB_AUTH_CMAC_KEY_COUNT(6), Length 2, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB
ASNGW#_AUTH_AK_SEQUENCE_NUM(7), Length 1, Class Optional
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB_AUTH_PMK_SEQUENCE_NUM(8), Length 1, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_SUB_AUTH_AK_CONTEXT_PRESENT(9), Length 1, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <1>
```

```

*Mar 21 06:25:48.692: AGW-SR: Type AGW_TID_HASH_KEY(10), Length 14, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0A01014602020202067611131111>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_TID(11), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <32777>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_TID_FT(12), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <3>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_TID_MT(13), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <12>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_PREVIOUS_TID(14), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <32776>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_PREVIOUS_TID_FT(15), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <8>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_OUR_PREVIOUS_TID_MT(16), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <5>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_TID(17), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <9>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_TID_FT(18), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <9>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_TID_MT(19), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <8>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_PREVIOUS_TID(20), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <8>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_PREVIOUS_TID_FT(21), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <8>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_PEER_PREVIOUS_TID_MT(22), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_ID_CTRL_REMOTE(0), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_ID_CTRL_LOCAL(1), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <6>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_LOCAL_ADDR_SIG(2), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <33686018>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_REMOTE_ADDR_SIG(3), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <167838022>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_LOCAL_UDPPORT_SIG(4), Length 2, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2231>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_REMOTE_UDPPORT_SIG(5), Length 2, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2231>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_FLAG_UNAUTHENTICATED(30), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_FLAG_NW_BEHIND_MS(32), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_FLAG_FRAMED_ROUTE_DOWNLOADED(34), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_MAX_FLOWS_SUPPORTED(33), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_SESSION_TIMEOUT(35), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <15000>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT(36), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_SESSION_START_TIME(37), Length 8, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0000000010B94FC4>

```

```

*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_SEQ_ENABLED_FOR_SIGNALING(38), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_IDS_REQUIRED_SIGNALING(39), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_IDLE_TIMEOUT_DIRECECTION_INBOUND(40),
Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_READY_FOR_SWITCHING_TRAFFIC(41), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_IS_SESSION_SYNCED(42), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_MASTER_SESSION_KEY(31), Length 64, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value
<F8BA755134ACE79E455CD056001967C4F29BB19A6250B8FA6CFB0981FC880D2F6D59B6419605CB94C0C2099FD
0AB405A2F8BFF0C14867E2C1FEF63D04D4F3365>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_USRGRP_USER_NAME(27), Length 20, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <7075736865747479406561702D746C732E636F6D>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_USRGRP_DOMAIN_NAME(28), Length 7, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <2A2A616E792A2A>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_SESSION_ACCT_AAA_AT_CLASS(6), Length 19, Class
Optional
*Mar 21 06:25:48.692: AGW-SR: Value <636C6173732D77696D61782D6368616E676564>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_PATH_BSID(85), Length 8, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0A01014600000000>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_INDEX(43), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ID_DATA_LOCAL(45), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <9>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ID_DATA_REMOTE(46), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <26>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_START_TIME(47), Length 8, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0000000010B950B0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_CREATE_TIME(48), Length 8, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0000000000000000>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_FASTSWITCHABLE(49), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SEQ_ENABLED_DATA(50), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_IS_FLOW_SYNCED(51), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_SENDING_ACCT_RECORD(73), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_PATH_SEND(74), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_LAST_ACCT_RECORD(75), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_TERMINATE_CAUSE(76), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_AIRLINK_STATE(77), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_ACCT_START_SENT(78), Length 1, Class
Mandatory

```



```
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_DISCARD(79), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_ACCT_SESSION_ID(84), Length 4, Class Optional
*Mar 21 06:25:48.692: AGW-SR: Value <17>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_ID(52), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <18>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(53), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(54), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <11>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(55), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(56), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(57), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(58), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <51>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(59), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <61>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(60), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <71>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(61), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(62), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <81>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(63),
Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(64), Length 4,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(65), Length 0, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(66), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(67), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(68), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(69), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(70), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(71), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_ID(52), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <17>
```

```

*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_DATA_DELIVERY_SERVICE(53), Length 1,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_LATENCY(54), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_BURST(55), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <2>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MAX_TRAFFIC_RATE_SUSTAINED(56), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <3>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MIN_TRAFFIC_RATE_RESERVED(57), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <4>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_POLICY_TRANSMISSION_REQUEST(58), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <5>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SDU_SIZE(59), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <49>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_TOLERATED_JITTER(60), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_TRAFFIC_PRIORITY(61), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_GRANT(62), Length
4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_UNSOLICITED_INTERVAL_POLLING(63),
Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <9>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_REDUCED_RESOURCES_CODE(64), Length 4,
Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_MEDIA_FLOW_TYPE(65), Length 0, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_TYPE(66), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE(67), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_VALID_CFG(68), Length 1, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_INFO_PRESENT(69), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_CLASSIFIER_PRESENT(70), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_FLOW_SF_QOS_SET_VALUE_PRESENT(71), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type AGW_FLOW_CURR_TID_USED(23), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <32777>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_ALLOCATED_ADDR(8), Length 4, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <33685507>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_TABLE_ID(9), Length 2, Class Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <0>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_ADDR_ALLOC_SOURCE(10), Length 4, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <5>

```

```

*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_ADDR_REAL_LENGTH(11), Length 2, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <1056>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_ALLOCATED_PREFIX_LENGTH(12), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <32>
*Mar 21 06:25:48.692: AGW-SR: Type UGW_HOST_AGGREGATE_PREFIX_LENGTH(13), Length 1, Class
Mandatory
*Mar 21 06:25:48.692: AGW-SR: Value <32>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_ORG_TYPE(14), Length 1, Class Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <1>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_TYPE_NUM(15), Length 1, Class Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <33>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_STATIC_ROUTE_ADDED(22), Length 1, Class
Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <1>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_TYPE_STATIC_ALLOCATED(23), Length 1,
Class Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <0>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_ALLOCATED(24), Length 1,
Class Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <1>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_ADDR_DYNAMIC_ADDR_REQUEST(25), Length 1, Class
Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <0>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_IP_KEY(26), Length 8, Class Mandatory
*Mar 21 06:25:48.696: AGW-SR: Value <0202000300000000>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_SERVER_ADDR(16), Length 4, Class Optional
*Mar 21 06:25:48.696: AGW-SR: Value <0>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_SERVER_XID(17), Length 4, Class Optional
*Mar 21 06:25:48.696: AGW-SR: Value <5142>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_TYPE(18), Length 1,
Class Optional
*Mar 21 06:25:48.696: AGW-SR: Value <1>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_HARDWARE_ADDRESS_LEN(19), Length 1, Class
Optional
*Mar 21 06:25:48.696: AGW-SR: Value <6>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_CLIENT_HARDWARE_ADDRESS(20), Length 16,
Class Optional
*Mar 21 06:25:48.696: AGW-SR: Value <06761113111100000000000000000000>
*Mar 21 06:25:48.696: AGW-SR: Type UGW_HOST_DHCP_CLIENT_ADDR_LEASE_TIME(21), Length 4,
Class Optional
*Mar 21 06:25:48.696: AGW-SR: Value <3540>
*Mar 21 06:25:48.696: AGW-SR: Attr Type: UGW_HOST_FLOW_INDEX Length: 1 Value: 0
*Mar 21 06:25:48.696: AGW-SR: Attr Type: Length: 1 Value: 1
*Mar 21 06:25:48.696: AGW-SR:
0C3535E0:          000003D0 001400A9          ...P...
0C3535F0: 00000006 06761113 11110001 00020012  ....v.....
0C353600: 00030014 32FE0D96 81EBDCFC DA1ECBA6  ...2~...k\|Z.K&
0C353610: 5BC764B5 2D80E90D 00020004 00000001  [Gd5-.i.....
0C353620: 00040008 90DDCD51 4678A29E 00050002  ....]MQF"x"....
0C353630: 3A980006 00020001 00070001 00000800  :.....
0C353640: 01000009 00010100 0A000E0A 01014602  .....F.
0C353650: 02020206 76111311 11000B00 02800900  ....v.....
0C353660: 0C000103 000D0001 0C000E00 02800800  .....
0C353670: 0F000108 00100001 05001100 02000900  .....
0C353680: 12000109 00130001 08001400 02000800  .....
0C353690: 15000108 00160001 02001500 F3000000  .....s...
0C3536A0: 04000000 00000100 04000000 06000200  .....
0C3536B0: 04020202 02000300 040A0101 46000400  .....F...
0C3536C0: 0208B700 05000208 B7001E00 01000020  ..7.....7.....
0C3536D0: 00010000 22000100 00210001 01002300  ...."!....#.
0C3536E0: 0400003A 98002400 04000000 00002500  ....:$.....%.
0C3536F0: 08000000 0010B94F C4002600 01000027  ....9OD.&....'

```

```

0C353700: 00010000 28000100 00290001 01002A00 ....(....)....*.
0C353710: 0100001F 0040F8BA 755134AC E79E455C .....@x:uQ4,g.E\
0C353720: D0560019 67C4F29B B19A6250 B8FA6CFB PV..gDr.1.bP8z1{
0C353730: 0981FC88 0D2F6D59 B6419605 CB94C0C2 ..|../mY6A..K.@B
0C353740: 099FD0AB 405A2F8B FF0C1486 7E2C1FEF ..P+@Z/.....~,o
0C353750: 63D04D4F 3365001B 00147075 73686574 cPMO3e....pushet
0C353760: 74794065 61702D74 6C732E63 6F6D001C ty@eap-tls.com..
0C353770: 00072A2A 616E792A 2A000600 13636C61 ..**any**....cla
0C353780: 73732D77 696D6178 2D636861 6E676564 ss-wimax-changed
0C353790: 0016000C 00550008 0A010146 00000000 .....U.....F....
0C3537A0: 0017017C 00000178 002B0001 00002D00 ...|...x.+....-.
0C3537B0: 04000000 09002E00 04000000 1A002F00 ...../.....
0C3537C0: 08000000 0010B950 B0003000 08000000 .....9P0.0.....
0C3537D0: 00000000 00003100 01000032 00010000 .....1....2....
0C3537E0: 33000100 00490004 00000001 004A0004 3....I.....J..
0C3537F0: 00000000 004B0004 00000001 004C0001 .....K.....L..
0C353800: 00004D00 0102004E 00010100 4F000100 ..M....N....O...
0C353810: 00540004 00000011 00340004 00000012 .T.....4.....
0C353820: 00350001 01003600 04000000 0B003700 .5....6.....7..
0C353830: 04000000 00003800 04000000 00003900 .....8.....9..
0C353840: 04000000 00003A00 04000000 33003B00 .....:.....3.;.
0C353850: 013D003C 00040000 0047003D 00010000 .=.<.....G.=....
0C353860: 3E000400 00005100 3F000400 00000000 >.....Q.?.....
0C353870: 40000400 00000000 41000000 42000100 @.....A...B...
0C353880: 00430001 00004400 01010045 00010100 .C....D....E....
0C353890: 46000101 00470001 00003400 04000000 F...G...4.....
0C3538A0: 11003500 01020036 00040000 00010037 ..5....6.....7
0C3538B0: 00040000 00020038 00040000 00030039 .....8.....9..
0C3538C0: 00040000 0004003A 00040000 0005003B .....:.....;
0C3538D0: 00013100 3C000400 00000000 3D000101 ..1.<.....=...
0C3538E0: 003E0004 00000000 003F0004 00000009 .>.....?.....
0C3538F0: 00400004 00000000 00410000 00420001 .@.....A...B...
0C353900: 00004300 01000044 00010100 45000101 ..C....D....E...
0C353910: 00460001 01004700 01000017 00028009 .F....G.....
0C353920: 00180000 00190094 00000090 00080004 .....
0C353930: 02020003 00090002 0000000A 00040000 .....
0C353940: 0005000B 00020420 000C0001 20000D00 .....
0C353950: 0120000E 00010100 0F000121 00160001 . .....!.....
0C353960: 01001700 01000018 00010100 19000100 .....
0C353970: 001A0008 02020003 00000000 00100004 .....
0C353980: 00000000 00110004 00001416 00120001 .....
0C353990: 01001300 01060014 00100676 11131111 .....v.....
0C3539A0: 00000000 00000000 00000015 00040000 .....
0C3539B0: 0DD40007 00010000 56 .T.....V
*Mar 21 06:25:48.696: AGW-SR: <067611131111><F[9]>Session (Setup) Sync to Standby

```

Output on STAND BY ASNGW 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 .....
jigarsha-asn(co.

```

```

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 C8003300 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_CMACE_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 <0A01014602020202067611121111>
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_SIGNALING(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 <7075736865747479406561702D746C732E636F6D>
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 switching

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

debug wimax agw switching [events | errors | gre events | gre errors | gre packet | gre packet detail | udp events | udp errors | udp packet | udp packet detail | dhcp events | dhcp errors]

Syntax Description

events	Displays information on bearers / signaling related events.
errors	Displays information on bearers / signaling related errors.
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 detail	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 detail	Displays information on related signaling UDP packet dump being switched.
dhcp events	Displays information on IOS DHCP interaction related events.
dhcp errors	Display information on IOS DHCP interaction 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 various ASN GW 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, procolot 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, procolot 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 ...
asn#
*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.
asn#
*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 ...
*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, procolot 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, procolot 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 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 02 02 02 02 10 00 22 27 00 01 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 02 02 00 59
    00 00 00 00 00 00 00 10 00 22 27 00 01 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
asn#
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
```

debug wimax agw vtemplate

To display ASN GW 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 ASN GW vtemplate information:

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

dhcp gateway address

To specify the IP address of the DHCP relay which the server is supposed to communicate with in the AGW, 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

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

Defaults

By default the AGW 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 AGW 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.

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
```

encapsulation agw

To clone a Virtual-Access interface of encapsulation type ASNGW, 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 ASNGW:

```
Router(config-if)#encapsulation agw
```

ip access-group

To specify IPv4 access permissions between a subscriber and an external host through the ASNGW 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**}

Syntax Description

<i>access-group-number</i>	Specifies the access group number.
in	Filters packets going to the subscriber (downstream).
out	Filters packets coming from the subscriber (upstream).

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:

```
access-group 4 in
```

ip address allocation subscriber timeout

To specify the IP address allocation timeout value for a subscriber, use the **ip address allocation subscriber timeout** command in user group configuration subcommand mode. Use the **no** form of the command to disable this feature.

ip address allocation subscriber timeout *timeout-value-in-secs*

Syntax Description	<i>timeout-value-in-secs</i>	Specifies the IP address allocation timeout value. The default value is 300 seconds.
---------------------------	------------------------------	--

Defaults	The default value is 300 seconds.
-----------------	-----------------------------------

Command Modes	User group configuration mode.
----------------------	--------------------------------

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

Usage Guidelines	After successful data-path establishment between BS and AGW, the address allocation timer is started for timeout value specified by this command[else default value is used]. If within the timeout value, the DHCP process is not successful then the subscriber is automatically de-registered by AGW.
-------------------------	--

Examples	The following example configures a timeout value of 500 seconds: <pre>Router(config-gw-ug)#ip address allocation subscriber timeout 500</pre>
-----------------	--

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 ????

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 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	<i>maximum-traffic-rate-sustained-value</i>	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

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 ????

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

no media-flow-type

Syntax Description	<i>media-flow-type-hex-string</i>	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

<i>minimum-traffic-rate-reserved-value</i>	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 direction, use the **pak-classify-rule** subcommand in service flow direction configuration submode. Use the **no** version of the command to remove the packet classification rule from the corresponding direction.

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

Syntax Description	<i>pak-classify-rule-profile-name</i>	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	<p>The following example specifies a packet classification rule profile named “uplink2”:</p> <pre>router(config-gw-sf-dir)#pak-classify-rule uplink2</pre>
-----------------	--

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 ????

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

Syntax Description	<p><i>policy-transmission-request-value</i></p> <p>Specifies the value of the policy transmission request. Range of values is 0-4294967295 32-bit bitmask.</p> <ul style="list-style-type: none"> • 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
```


priority permit

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

```
priority 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 permit
```

Syntax Description

<i>0-255</i>	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.
<i>src-address</i>	Specifies the src address.
<i>src-mask</i>	Specifies the src mask.
any	Specifies any address or mask.
host	Specifies the host src address.
<i>src-port-low</i>	Specifies the src low port value.
<i>src-port-high</i>	Specifies the src high port value.
<i>dst-address</i>	Specifies the dst address.
<i>dst-mask</i>	Specifies the dst mask.
<i>tos-low</i>	Specifies the tos low value.
<i>tos-mask</i>	Specifies the tos mask.
<i>tos-high</i>	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

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 sets the **priority** for a gre packet:

```
Router(config-gw-pak-classify-rule)#priority permit 100 gre
```

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** version of the command to remove the QoS information from the corresponding direction.

qos-info *qos-profile-name*

Syntax Description

<i>qos-profile-name</i>	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 ASNGW, 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 ASNGW:

```
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 ASNGW, 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 ASNGW 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	<i>reduced-resources-code</i> Specifies the value of the reduction in resources. <i>-value</i>
---------------------------	---

Defaults	There is no default value.
-----------------	----------------------------

Command Modes	Service flow QoS information configuration submode.
----------------------	---

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.4(15)XL</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.4(15)XL	This command was introduced.
Release	Modification				
12.4(15)XL	This command was introduced.				

Examples	<p>The following example illustrates how to configure the reduced-resources-code command:</p> <pre>router (config-gw-sf-qos-info)#reduced-resources-code <i>reduced-resources-code-value</i></pre>
-----------------	---

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**]

no reference-point r6

Syntax Description

keepalive	Enables the AGW-BS keepalive feature.
path	Specifies the WiMAX AGW BS R6 reference point base station path.
purge-timeout <i>value</i>	Specifies WiMAX AGW 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 AGW BS R6 reference point response configuration commands.

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.

Examples

The following example illustrates how to configure the **reference-point r6** command, and sets a **purge-timeout** value of 30 minutes:

```
router(config)#wimax agw base-station group default

router(config-wimax-agw-bs)#reference-point 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

router(config-wimax-agw-bs)#reference-point r6 path ?
  purge-timeout  WiMAX AGW BS R6 reference point path purge timeout

router(config-wimax-agw-bs)#reference-point r6 path purge-timeout ?
  <1-4320>  WiMAX AGW BS R6 reference point path purge timeout in minutes

router(config-wimax-agw-bs)#reference-point r6 path purge-timeout 30
```

reference-point r6 response retransmits

To specify the number of times the AGW 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	<i>retransmit value</i>	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 AGW 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

<i>timeout value</i>	Specifies the amount of time the AGW 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 AGW will retransmit the message until the maximum number of retries configured is reached.

Examples

The following example illustrates that the AGW 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

<i>sdu-size-value</i>	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

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 } profile sf-profile-name
```

Syntax Description		
isf		The service flow is assumed to be the initial service flow.
secondary <i>secondary-index</i>		Represents the auxiliary service flows for the subscriber.
profile <i>sf-profile-name</i>		Enables the service flow profile and profile name of the flow.

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 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.

Examples The following example enables the initial service flow:

```
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
```

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 | precedence} {precedence-value | dscp-value}
```

```
no set {dscp | precedence}
```

Syntax Description

dscp	Set GW service flow DSCP specific values.
precedence	Set GW service flow Precedence specific values.
<i>precedence-value</i>	Precedence value. The range is 0-7.
<i>dscp-value</i>	Differentiated services codepoint value. The range is 0-63.

Defaults

By default, no marking is done. Default values of above 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 the *precedence-value* and *dscp-value* arguments:

```
router(config-gw-sf-dir)#set dscp dscp-value

dscp-value -
<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)
```

```
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 ASN gateway functionality on the router, use the **service wimax agw** command in global configuration mode. Use the **no** version of the command to disable ASN gateway functionality; all configured ASN gateway-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.

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

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

Examples The following example enables the ASN gateway:

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


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 <i>virtual-server</i>	(Optional)	Displays information about sessions being handled by the specified virtual server.
client <i>ip-address netmask</i>	(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 session asnr6

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

```
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 wimax agw

To display various system parameters, including ASN GW software version, number of base stations allowed, number of subscribers allowed, and others, use the **show wimax agw** privilege 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.

Usage Guidelines The output of this show command contains the following information:

- Version of WiMAX AGW 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 flows currently active
- Current base station keep alive interval configured
- Current timeout value configured for R6 messages

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

```

WiMAX AGW Session Redundancy is enabled
  WiMAX AGW Session Redundancy system status
    AGW state = ACTIVE
    AGW-peer state = STANDBY HOT
  WiMAX AGW Session Redundancy Statistics Summary

      Synced to standby
Subscriber          1
Flows                2
Hosts                3

```

Display information about the AGW redundancy specific statistics.

Snapshot:

```
WiMAX AGW 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
```

show wimax agw message

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

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

Syntax Description	<i>function-type-no</i>	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)

ASNGW#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		
	<i>bs-ip-address</i>	<p>For each base station, the following information will be displayed.</p> <ul style="list-style-type: none"> 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 <p>If the base station IP address is not specified, the command will display information about all of the base stations currently connected to the AGW.</p>
	brief	<p>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</p> <ul style="list-style-type: none"> BS IP Address Number of sessions currently active Number of flows currently active

Defaults No default behavior or values.

Command Modes Privileged EXEC.

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

Usage Guidelines

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

```
router# show wimax agw path
Path type Sig-UDP
```



```
State current Ready, old Purging
Number of sessions connected 1
Number of old sessions connected 0
Address local 2.2.2.2(AF_INET), remote 10.1.1.71(AF_INET)
UDP port local 2231(0x8B7), remote 2231(0x8B7)
Identification Peer 0x0A01014700000000, Our 0x02020202
Traffic sent 5 packets, 609 bytes
Traffic received 5 packets, 482 bytes
```

```
Path type Data-GRE
Number of flows connected 1
Address local 2.2.2.2(AF_INET), remote 10.1.1.71(AF_INET)
Traffic sent 0 packets, 0 bytes
Traffic received 3 packets, 1938 bytes
```

show wimax agw redundancy

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

show wimax agw redundancy [status]

no show wimax agw redundancy

Syntax Description	status	(Optional) Displays session redundancy status on the ASN GW.
--------------------	--------	--

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Privileged EXEC.
---------------	------------------

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

Usage Guidelines

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.



Note

For Release 1.0 of the AGW, only a single reference point, R6 is supported.

show wimax agw statistics

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.

Usage Guidelines

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
```

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 AGW.

```
show wimax agw subscriber [msid macid] [brief | host | flow] [traffic]
```

Syntax Description

msid	Displays information about the mobile subscriber.
<i>macid</i>	If the subscriber <i>macid</i> is not specified, the output displays information about all the subscribers currently connected to the AGW.
brief	Displays output that contains a list of all the subscribers currently connected. Contains the following information: <ul style="list-style-type: none"> 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	
host	
traffic	

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

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

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 for all the flows
- Authentication details (i.e., unauthenticated, single-EAP, double-EAP etc.)

Examples

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

```
MSID 1000.2223.0001
Connection time 044:26:44
Auth policy 0X0(0)
Number of TIDs 1
TID Key 10.1.1.70/2.2.2.2/1000.2223.0001
Peer TID 0X2(2)
    FT MS State Change(9), MT Attachment Request(8)
Our TID 0x8002(32770)
    FT Data Path(3), MT Registration Request(12)
Subscriber address 2.2.0.87, type IPv4, organization IETF
Subscriber address method Dynamic, source DHCP relay
Subscriber address assigned on flow downlink ID 1
Subscriber address prefix len allocated 32, aggregate 32
Subscriber address traffic sent 0 packets, 0 bytes
Subscriber address traffic received 3 packets, 1812 bytes
Subscriber address DHCP XID 2097, server 11.1.1.93, htype 1
Subscriber address DHCP client ID 1000.2223.0001, length 6
Subscriber address DHCP Refresh time 86400 seconds
Number of sessions 1
Session details:
    FSM in state Ready(7) on last event Rx Attach Ack(14)
    Authentication method unauthenticated
    Associated user group **unauthenticated**
    Signalling address local 2.2.2.2, remote 10.1.1.70
    Signalling UDP port local 2231, remote 2231
    Idle for inbound 08:13:56, outbound 08:13:56
    Ingress Address filtering 0 packets, 0 bytes
    Number of flows 2
    Flow details ISF(0)
        FSM in state SF Ready(4) on last event Up(1)
        Transaction ID used 0X8001(32769)
        Data ID local 0x1(1), remote 0x1(1)
        Data address local 2.2.2.2, remote 10.1.1.70
        Data traffic sent 2 packets, 661 bytes
        Data traffic received 4 packets, 2416 bytes
        Accounting last record sent Interim(3)
        Idle for inbound 1d20h, outbound 1d20h
        Service Flow information Downlink:
            Identifier 1
            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 permit ip any any
    Service Flow information Uplink:
        Identifier 2
        QoS information:
            Data-delivery-service unsolicited-grant
            Minimum traffic-rate-reserved 0, Maximum latency 11
            Tolerated-jitter 71, SDU-size 61
            Unsolicited interval-grant 81, Request/Transmission-policy 51
            Reduced-resources-code 0
        Classifier information:
            priority 0 permit ip any any
    Flow details Secondary(1)
        FSM in state SF Ready(4) on last event Up(1)
        Transaction ID used 0X8002(32770)
        Data ID local 0x2(2), remote 0x2(2)
```

```

Data address local 2.2.2.2, remote 10.1.1.70
Data traffic sent 3 packets, 999 bytes
Data traffic received 3 packets, 1812 bytes
Accounting last record sent Interim(3)
Idle for inbound 08:14:15, outbound 08:14:15
Service Flow information Downlink:
Identifier 3
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 permit ip any any
Service Flow information Uplink:
Identifier 4
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 permit ip any any

```

asn# **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

asn# **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

Asn# **show wimax agw subscriber brief host [traffic]**

MSID	Base Station	Index	Pkts-Tx	Bytes-Tx	Pkts-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					

show wimax agw tlv

To display information about the TLVs supported by the AGW, use the **show wimax agw** command in privileged EXEC mode.

```
show wimax agw tlv [tlv-type]
```

Syntax Description	<i>tlv-type</i>	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.

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

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 Identifier(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 ASN GW, 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.

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 Recevied 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 Recevied 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 Recevied 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 ?
  brief  Brief output
  |      Output modifiers
  <cr>
```

```
router#show wimax agw user-group any
```

```
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
```

```
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 Received 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 Received 0 packets, 0 bytes
Ingress Address filtering 0 packets, 0 bytes
```

```
asn#sh wimax agw user-group unauthenticated b
asn#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
```

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 <i>percentage</i>	(Optional) Specifies CPU busy threshold value as a percentage. Range 0 to 100, default 90.
delay <i>seconds</i>	(Optional) Specifies delay in seconds before the CCM component synchronizes sessions after the CPU busy threshold is exceeded.
allow <i>value</i>	(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 <i>time</i>	(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 <i>sessions time</i>	(Optional) Specifies number of sessions per time period for bulk and dynamic synchronization. <ul style="list-style-type: none"> • 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 idle

To specify the idle timeout for a subscriber, use the **timeout idle** command in user group configuration mode. Use the **no** form of the command to disable this feature.

timeout idle *timeout value* [**inbound**]

Syntax Description	<i>timeout value</i>	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

<i>timeout value</i>	Specifies the timeout session value in seconds. The <i>timeout value</i> 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

Global configuration.

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	<i>tolerated-jitter-value</i>	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	<i>traffic-priority-value</i>	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

<i>unsolicited-interval-grant-value</i>	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.

Usage Guidelines

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	<i>unsolicited-interval-polling-value</i>	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.

Usage Guidelines

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-group (user group list configuration subcommand)

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.
<i>domain-name</i>	Specifies the domain name.

Defaults

There are no default values.

Command Modes

User group list configuration sub mode.

Command History

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

Usage Guidelines

Release 1.0 of the Cisco ASN GW supports the user-groups **any** and **unauthenticated**.

Examples

The following example illustrates how to configure unauthenticated users:

```
Router(config-gw-ugl)#user-group unauthenticated
```

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

<i>vrf-name</i>	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
```

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	<i>name</i>	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 base-station ip-addr any group

To specify the base stations that are allowed to connect to the AGW, and the base station group they belong to, use the **wimax agw base-station ip-addr any group** command in global configuration mode. Use the **no** form of the command to disable this feature.

wimax agw base-station ip-addr any group *group-name*

no wimax agw base-station ip-addr any group *group-name*

Syntax Description

<i>group-name</i>	Specifies the name of the base station group.
-------------------	---

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 base stations are configured based on the IP address of the base station. The mask parameter allows several base stations with contiguous IP addresses to be configured using a single invocation of this command.

Examples

The following example configures a base station group named *boston*:

```
Router(config)#wimax agw base-station ip-addr any group boston
```

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

<i>number</i>	Specifies the maximum number of base stations that are allowed to connect to the AGW. The maximum number range is 0-500. 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 AGW 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 AGW is set to the maximum number supported by the platform.

Examples

The following example allows 240 base stations to connect to the ASN GW:

```
wimax agw r6 maximum base-station 240
```


wimax agw r6 maximum subscriber

To specify the maximum number of subscriber sessions allowed on the AGW, 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*

Syntax Description	<i>number</i>	Specifies the maximum number of subscriber sessions on the ASN GW. The range is 0-20000.
---------------------------	---------------	--

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 AGW platform is set to its maximum value.
-------------------------	--

Examples	The following example limits the number of subscriber sessions on the ASN GW to 50:
-----------------	---

```
Router(config)#wimax agw r6 maximum subscriber 50
```

wimax agw redundancy

To enable session redundancy on the ASN GW, 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 ASN GW:

```
Router(config)# wimax agw redundancy
```

wimax agw service-flow pak-classify-rule profile

To configure a service-flow packet classification rule profile on the ASN GW, 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.

Router(config)#

wimax agw service-flow pak-classify-rule profile *service-flow-pak-classify-rule-profile-name*

no wimax agw service-flow pak-classify-rule profile

Syntax Description

<i>service-flow-pak-classify-rule-profile-name</i>	Specifies the name of the service-flow packet classification rule profile on the ASN GW. 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

The profiles are configured under the predefined service flows that are opened for the subscriber.

Examples

The following example illustrates a configuration with a service flow named “cisco2”:

```
router(config)#wimax agw service-flow pak-classify-rule profile cisco 2
```

wimax agw service-flow profile

To configure a service-flow profile on the AGW, 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.

agw service-flow profile *service-flow-profile-name*

no agw service-flow profile *service-flow-profile-name*

Syntax Description

<i>service-flow-profile-name</i>	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.

Examples

The following example illustrates a configuration with a service flow named “cisco2”:

```
agw service-flow profile cisco2
```

wimax agw service-flow profile qos-info

To configure a service-flow QoS information profile on the AGW, 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*

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 AGW 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 user group-list

To configure the User group list on the AGW router, 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 AGW.

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.

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
```

```
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 configuration 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)#
```