CHAPTER 2

Configuring the Cisco ASN Gateway

This feature module explains and discusses the feature set for the Cisco ASN Gateway. Additionally, this feature module explains how to configure those features, and provides sample configurations when appropriate.

This chapter contains information on the following features:

EAP Authentication

The Authenticator function is part of the ASN gateway. This function performs the role of an anchored authenticator for the specific subscriber for the duration of the session. During further mobility events (for example, as a subscriber moves between base stations served by the ASN gateway), the authenticator anchor remains stationary.

ASN Gateway Release 1.0 does not support inter-ASN gateway mobility. If a subscriber moves to a base station served by a new ASN gateway, the anchor authenticator is now hosted at the new ASN Gateway. A full re-authentication of the subscriber is required.

The Radius Client for Authentication and Accounting is collocated with the Authenticator function.

The supported Authentication types in Release 1.0 are EAP-TLS and unauthenticated users.

The ASN Gateway acts as an EAP relay and is agnostic to the EAP method. EAP transport is done between the ASN Gateway and the base station as a control exchange. The base station functions as an EAP-relay, converting from Pair-wise Master Key version 2 (PKMv2) to the EAP messages over to the ASN Gateway. The ASN Gateway is an EAP pass-through, and any key that generates EAP methods is supported in the system.

PKMv2 is used to perform over-the-air user authentication. PKMv2 transfers EAP over the IEEE 802.16 air interface between the MS and the base station. The base station relays the EAP messages to the Authenticator in the ASN Gateway. The AAA client on the Authenticator encapsulates the EAP message in AAA protocol packets, and forwards them through one (or more) AAA proxies to the AAA server in the CSN of the home NSP. In roaming scenarios, one (or more) AAA brokers with AAA proxies may exist between the Authenticator and the AAA server. All AAA sessions always exist between the Authenticator and AAA server, with optional AAA brokers providing a conduit for NAI realm-based routing.

Note There is no support for Fast Re-Authentication in Cisco ASN Gateway Release 1.0.

Subscriber Identities

The following three types of subscriber identities are used on the ASN Gateway:

MSID

The MSID is the 802.16 identifier used for all subscriber stations, and is used in all the messages over R6. This identifier associates all requests from a SS/MSS to the ASNGateway. Typically it is the MACID.

EAP Outer Identity

The EAP outer identifier format is *pseudo-identity@domain*. The domain portion is used to route to the correct home AAA server. The domain portion is also used to access the local configured group configuration on the ASN Gateway.

EAP Inner Identity

The EAP inner identifier is sent directly between the SS/MSS to the AAA server, and is provisioned at the SS/MSS.

Network Admission of an Authenticated User

The following series of events illustrates how the network admits an authenticated user.

1. BS sends MS Pre-attachment request with the Authorization Policy bits to indicate Authorization Method/Policy. The receipt of authorization policy other than EAP authorization (Single EAP), or Authenticated-EAP Authorization (Double EAP), or Null authentication, results in the ASN Gateway sending an MS Pre-Attachment Response with indication of “Authentication Failure”.
2. The authenticator (in ASN Gateway) initiates EAP authentication procedure with MS after receipt of Pre-Attachment-Ack message from the Base Station.
3. The authenticator sends EAP Request/ Identity message over Authentication Relay protocol (AuthRelay-EAP-Transfer) to BS.
4. The BS relays the EAP Request/ Identity payload in the PKMv2 EAP-Transfer/ PKM-RSP message to the MS.
5. The MS responds with EAP Response/ Identity message providing NAI. This message is transferred to BS over PKMv2 EAP-Transfer/ PKM-REQ message.
6. The BS relays EAP payload received in PKMv2 EAP-Transfer to the authenticator over Authentication Relay protocol (AuthRelay-EAP-Transfer message).
7. The EAP payload is forwarded to MS’ Home AAA server via Visited AAA server (authenticator analyzes the provided NAI for resolving the Home-AAA server location). Authenticator sends EAP Request/ Identity message over Authentication Relay protocol (AuthRelay-EAP-Transfer) to BS.
8. In order to deliver EAP payload received from BS, to AAA server, authenticator forwards EAP message through the collocated AAA client using RADIUS Access-Request message (EAP payload is encapsulated into RADIUS “EAP message” attribute(s).
9. The EAP authentication process (tunneling EAP authentication method) is performed between the MS and the authentication server through the authenticator in the ASN Gateway.
10. The EAP payload returned from the AAA server in a RADIUS Access-Challenge message is transferred to the base station in an AuthRelay-EAP-Transfer message. There may be multiple EAP message exchanges between the EAP supplicant, located at the Mobile Subscriber Station, and the EAP Authentication Server, located at the AAA server.
11. The authenticator sends the Key Change Directive message to the base station to indicate completion of the EAP authentication process. The key is computed by ASN Gateway using the Master Secret Key (MSK) it received from AAA (in an Access Accept). The Key Change Directive contains the MSINFO TLV with the AK Context sub-TLV, and also the EAP Payload TLV indicating EAP success.
12. In the case of an authentication failure indication is received from the AAA server the subscriber is de-registered from the network using the Normal Mode Network-Initiated Network Exit procedure.
13. The base station acknowledges receipt of Key Change Directive message with a Key Change Acknowledgement message.
14. The base station sends the result of authentication to the Mobile Subscriber Station using a PKMv2 EAP-Transfer message.

Support of Un-Authenticated User

Support of un-authenticated users is required in the following scenarios, and can be used for pre-paid systems, or emergency calls.

- The Mobile Subscriber (MS) can choose to indicate NULL Authentication. This may be a specific type of MS, such as an MS that is limited to emergency calling. This type of MS will indicate NULL Authentication support in the SBC_REQ. The BS relays this through the NetEntry MS State Change Request to the ASN Gateway.
- Based on local policy, the ASN Gateway can choose to skip authentication, and allow a subscriber to enter the network.
- When the ASN Gateway is configured to enable NULL Authentication using the CLI, any Subscriber Station (SS)/MSS requesting NULL authentication will be mapped to a NULL-AUTH user group. DHCP requests from these SS/MSS will only be sent to the configured DHCP server. This enables the operator to control address allocation to the unauthenticated users, as well as apply any restrictions for such users. In addition, Access Control Lists may be configured that would restrict the traffic from the SS/MSS only to certain destinations.

Configuring Authentication

This section provides information on how to configure authentication and authorization on the Cisco ASN Gateway. To enable authenticated calls between the ASN Gateway and a subscriber, perform the following tasks on the ASN Gateway:

- Configuring AAA for Accounting Types
- Configuring Authorization
- Configuring Authentication
- RADIUS Server

Configuring AAA for Accounting Types

To configure accounting types on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	`router(config)# aaa session-id {common	unique}`	Specifies either a common or unique session id for different accounting types.
Step 2	`router(config)# aaa new-model`	Enables the NEW access control commands and functions. (Disables OLD commands.) The **no** version of this command resumes the old commands and functions.

Configuring Authorization

To configure authorization on the ASN Gateway, perform the following task:

	Command	Purpose
Step 1	router(config)# **aaa authorization network default group {***server-group-name* **| radius}**	Specifies the server-group to download the configurations from AAA server for a particular authorization list. The **no** version of this command removes the use of server-group.

Configuring Authentication

To configure authentication on the ASN Gateway, perform the following task:

	Command	Purpose
Step 1	router(config)# **aaa authentication dot1x {***authentication-list-name* **| default} group {***server-group-name* **| radius | tacacs+}**	Specifies the authentication method to be used. The dot1x keyword will be replaced with WiMAX specific keyword.

RADIUS Server

To configure the RADIUS server host on the ASN Gateway, perform the following task:

	Command	Purpose
Step 1	router(config)# **radius-server host {***host-name* | *ip-address***} {auth-port | acct-port} key**	Configures the RADIUS Server. *ip-address* of RADIUS server **auth-port**—UDP port for RADIUS authentication server (default is 1645). **acct-port**—UDP port for RADIUS accounting server (default is 1646). **key**—per-server encryption key.

Configuring User Groups

To configure a user group on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	`router(config)#` **`wimax agw user group-list`** *`user-group-list-name`*	Configures the user group list on the ASN Gateway router. There can be only one user group list allowed on a single processor of the ASN Gateway. The **no** version of command removes the user group list. Enabling this command create a user group list sub configuration mode to create multiple user groups under the user-group list created.
Step 2	`router(config)#` **`user-group {any | unauthenticated | domain`** *`domain-name`***`}`**	Configures the **user group** under the user group list. This creates a user group sub configuration mode for configuring various parameters of the user group. Three types of user groups are supported: • Domain based user groups – In cases where the user is authenticated, the ASN Gateway discovers the user based on the domain name part of the NAI received. The NAI received uses the format *userpart@domain*. In order to match a user-group *abc@cisco.com*, you need to configure **user-group domain** *cisco.com* and put all the per domain configuration under this user-group. • Any user group – In cases where an authenticated user is not found in a user-group based on the domain, the default behavior is to place those users in this category. For example, if you receive a user with NAI *abc@cisco2.com* and do not have a user-group domain for *cisco2.com*, this user will fall into the **any** user group category. • Un-Authenticated User Group – All un-authenticated users fall into this category of user groups.The **no** version of command removes the user group. **Note** For ASN Gateway Release 1.0, the presence of user-groups **any** and **unauthenticated** is optional.
Step 3	`router(config)#` **`aaa {authentication | accounting} method-list {`***`method-list-name`*** `| default}`**	Configures the authentication or the accounting method list used for the domain. The **no** version of the command removes the user group.

Note AAA server group can be linked with the method list configurations so that different AAA servers can be configured, and thereby map to different user-groups.

Verifying the Configuration

The authentication method of a subscriber displays whether the call was authenticated with EAP, or unauthenticated for the respective user group (**any**, **unauthenticated**, **domain** specific).

For an authenticated call, the Auth Policy and AK Context is also displayed.

To verify your authentication configuration, use the following commands:

	Command	Purpose
Step 1	`router# show wimax agw subscriber msid`	Displays subscriber authentication information.

Configuration Examples

Here is sample output for subscriber information for an unauthenticated call:

```
Router>sh wimax agw subscriber msid 1000.0003.0000
 Connection time 000:01:05
 Auth policy 0X0(0)
 Number of TIDs 1
 TID Key 10.1.1.82/2.2.2.2/1000.0003.0000
  Peer TID 0X2(2)
    FT MS State Change(9), MT Attachment Request(8)
  Our TID 0x8001(32769)
 Subscriber address 2.2.0.9, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 Subscriber address assigned on flow downlink ID 17
 Subscriber address prefix len allocated 32, aggregate 32
 Subscriber address traffic sent 0 packets, 0 bytes
 Subscriber address traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 2391, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 1000.0003.0000, 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 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:10, outbound 00:01:10
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8001(32769)
     Data ID local 0x9(9), remote 0x2(2)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 656 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:10, outbound 00:01:10
     Service Flow information Downlink:
      Identifier 17
QoS information:
       Data-delivery-service real-time-variable-rate
       Minimum traffic-rate-reserved 4, Maximum latency 1
```

Here is sample output for subscriber information for an authenticated call:

```
Router>sh wimax agw subscriber msid 1000.0002.0001MSID 1000.0002.0001
 Connection time 000:01:08
 Auth policy 0X12(18), Single-EAP, CMAC
  AK Ctx method C-MAC(1), Lifetime 65535
  AK Ctx Seq No. AK 0, PMK 0
  AK Ctx C-MAC key count 1
 Number of TIDs 1
 TID Key 10.1.1.82/2.2.2.2/1000.0002.0001
  Peer TID 0X4(4)
    FT MS State Change(9), MT Attachment Request(8)
  Our TID 0x8004(32772)
 Subscriber address 2.2.0.8, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 ….
 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)
   Username eap-md5-u@eap-md5.com
   Authentication method EAP
AAA session-id length 7, 0x30313233414243
   AAA termination-action 1
   Reauthentication attempts from subscriber 0, ASNGW 0
   Associated user group **any**
   Signalling address local 2.2.2.2, remote 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:09, outbound 00:01:09
   Absolute timeout 1500, remaining 00:23:49
   Idle timeout 600 (both), remaining 00:08:50
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8004(32772)
     Data ID local 0x8(8), remote 0x1(1)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 705 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:09, outbound 00:01:09
     Service Flow information Downlink:
      Identifier 15
```

Security Key Exchange

After EAP authentication of the subscriber, the ASN Gateway computes the respective Access Keys (AKs) for each Base-Station. The ASN Gateway also caches the PMK for the duration of the authentication, and recomputes additional AKs when the SS/MSS moves to another BS.

Release 1.0 supports Re-Authentication triggered from the mobile, and generates a new PMK.

IP Address Allocation Using DHCP

Cisco ASN Gateway Release 1.0 supports external Dynamic Host Configuration Protocol (DHCP) server-based address allocation.

Note The only mechanism to assign addresses to the SS/MSS is based on DHCP.

The SS/MSS can use DHCP to allocate IP addresses. For Release 1.0 there is no MIP or PMIP, because the ASN Gateway is only targeting fixed and portable. The DHCP relay is resident in the ASN Gateway, and interacts with a DHCP server, provided when the user-groups are on different VRF.

Overlapping of addresses with usergroup is allowed only with VRF.

After successful authentication and setup of the Initial Service Flow, the MS triggers DHCP to acquire an IP address. The DHCP server is configured on the ASN Gateway per user-domain group. The DHCP messages are transported transparently over the R6 data path between the BS and the ASN Gateway. The addresses can be allocated by the corresponding DHCP server pertaining to the user-domain group. Overlapping addresses across different user-groups are supported. using loop back might be the ideal way, however if the “dhcp gateway address” is not configured the IP of Virtual Template will be used as the gi-address

The initial service flow does not permit any data traffic except DHCP packets. After address allocation is successfully completed, the appropriate classifiers are installed that correspond to the IP address assigned to the SS/MSS.

In order to support multiple hosts behind a Subscriber Station, multiple DHCP requests from subscriber stations will be supported. These requests can be received on the same or alternate service flows.

Configuring IP Address Allocation

To configure IP address allocation using an external-based DHCP server, perform the following task:

	Command	Purpose

Step 1	`router# interface Loopback102`
	`ip address 102.0.0.1 255.255.255.0`
	` !`
	` user-group domain eaptls.com2`
	`  aaa accounting method-list AAA-ACC1`
	`  aaa authentication method-list AAA-AUTHN1`
	`  dhcp gateway address 102.0.0.1`
	`  dhcp server primary 27.0.0.8`
		Configures an external DHCP server to allocate IP addresses.
		The default ip address allocation time is 300 seconds.

Here is a sample configuration:

```
interface Loopback102
  ip address 102.0.0.1 255.255.255.0
 !
 user-group domain eaptls.com2
  aaa accounting method-list AAA-ACC1
  aaa authentication method-list AAA-AUTHN1
  dhcp gateway address 102.0.0.1
  dhcp server primary 27.0.0.8
  service-flow pre-defined isf profile sf3
  service-flow pre-defined secondary 1 profile sf4
vrf VRF_2
```

The DHCP server and gateway also can be configured under User Group. If you do not configure DHCP server or gateway address under the user group, the global configuration method is used.

Multiple Host Support

Multiple hosts behind an SS can be supported for IPCS, using DHCP Relay option 82, or option 82 - subscriber ID.

Subscriber-id sub-option of Option 82 could be set to the MSID of the MS/SS and the Circuit-id sub-option can be set to the downlink service flow identifier. A remote ID could be set to the SS/MSS's username for an authenticated user, and the VPNID can be set to the user's VRF name if configured.

For example, the DHCP server can allocate a unique IP address for each MAC, to support a multi-host scenario.

Now, the subscriber ID will have the username and remote ID will have the MACID of the user.

Note For Release1.0, relay cascading is not supported.

Note The maximum number of hosts allowed behind an MS is 8.

Support of Multiple Hosts Behind a SS

Multiple hosts are also supported over a single SS/MSS

Step 1 CPE (SS) undergoes initial network entry and authentication, and a bearer path is created.

Step 2 A basic R6 bearer path between the BS and the ASN Gateway is created. The basic R6 shares a GRE key for uplink/downlink, which may be mapped to the SFID and the corresponding airlink connection.

Step 3 All uplink and downlink packets are sent and received by the CPE for all the hosts on the same service flows (R6 bearer) at the ASN Gateway.

DHCP Option 82

DHCP option 82 is applicable for subscribers as well as host. This is sent in any DHCP messages for any host or subscriber.

Multiple hosts can also be supported using the DHCP option 82. The Relay Agent Information option is inserted by the DHCP relay agent when it forwards client-originated DHCP packets to a DHCP server. Servers that recognize the Relay Agent Information option can use the information to implement IP address, or other parameter assignment policies.

DHCP options 82 appends subscriberid + remote id + circuit id. This is then sent in all DHCP messages toward the server. In case of VRF, VPN ID is also sent. If the DHCP server is not Option 82 aware, and does not echo back the option 82, the ASN Gateway drops the messages from DHCP server.

This feature is valuable because it allows you to do the following:

- Identify each subscriber
- Perform subscriber management
- Assign IP addresses based on subscriber info
- Set access control, QoS and security policies

Here is the sequence of events that occur for the DHCP Option 82 feature:

Step 1 Hosts set the client identifier field to the MAC address in the DHCP message.

Step 2 DHCP message communication is done only over ISF for procuring the CPE's IP address, and can be done on any of the flows for procuring the host's IP address. The DHCP packets from ASN Gateway are sent out on the same flow as the incoming DHCP message from the host.

Step 3 The ASN Gateway inserts the option 82 fields for use by the DHCP server. Option 82 shall be inserted into all DHCP messages towards the DHCP server. For the list of options to insert refer to Table 2-1

Step 4 The DHCP Server could allocate IP address using any of the options in the Option 82 field of the incoming DHCP packet. Once the IP address is allocated, the ASN Gateway learns the assigned IP address by monitoring the responses and maps it to the R6 bearer. This process is repeated for each host, and the address is tracked and mapped to the same R6 bearer.

Step 5 The ASN Gateway will monitor all DHCP messages, and ensure that the option 82 fields are inserted.

Table 2-1 lists the DHCP Server Options.

Table 2-1 DHCP Server Options

Sub-Option	Code	Length	Sub Value
Circuit ID	1	Variable	Downlink Service Flow ID
Subscriber ID	6	Variable	MSID (MAC-address of SS/MSS)
Remote ID	2	6	User name of the SS/MSS, for an authenticated user
VPN-ID	151	Variable	VRF name, if the user belongs to a VRF

Service Flow Creation and Management

802.16 supports multiple service flows for a given SS. The service flows are identified by mapping a set of classification rules over the packet bearer. Each service flow is a unidirectional flow and can have a different quality of service treatment, both on the airlink and on the network.

In Cisco ASN Gateway Release 1.0, service flow creation is supported only when initiated by the network. This service flow creation will provision the classifiers on the SS/MSS as well.

Additionally, pre-provisioned service flow templates are configured on the ASN Gateway locally. AAA support for downloading the Service Flow Profile ID is not supported on the ASN Gateway.

Service Flows

The ASN Gateway manages the service flows for each SS/MSS. Release 1.0 only supports network triggered service flows. The ASN Gateway allocates SFID for each service flow, and triggers service flow creation. Each service flow also has its respective datapath (for example, GRE key, and the packets corresponding to each service flow are transported accordingly).

All pre-provisioned flows are assumed to be available for the lifetime of the SS/MSS session, and are not deleted.

Multiple Service Flow Creation

When the control plane comes up, the ASN Gateway requests the creation of the Initial Service flow with the base station. Once the initial service is created and an IP address is allocated to the user with the DHCP to the subscriber over the initial service flow, a secondary service flow will be created.

Each secondary service will be created one after the previous. Only after successfully creating one secondary service will the next secondary flow be created.

For Release 1.0, the ASN Gateway supports creating 4 service flows; the initial service flow, and 3 secondary service flow.

If a secondary SF creation fails, then the next flow is attempted and session continues without the failed SF.

Configuring ASN Gateway Service

To enable ASN Gateway services, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`router(config)# service wimax agw`	Enables WiMAX ASN Gateway services.
Step 2	`router(config-if)# encapsulation agw`	Clones a Virtual-Access interface of encapsulation type “ASNGW”. Configure this command in Virtual-Template configuration mode.

Sample Configuration

Here is a sample configuration to clone the Virtual Address:

```
#
!
interface Virtual-Template1
ipaddress 2.2.2.2 255.255.0.0
encapsulation agw
no keepalive
!
```

The Gi address is picked from the Virtual Address by default. You can use the **user-group** configuration to override the Gi address.

Verifying the Configuration

To verify that ASN Gateway services are enabled, and to display MS State Change and Data Path statistics, use the **show wimax agw statistics** command in privileged EXEC mode:

```
Message type Deregistration Request(4/0x4)
   Number of messages sent 1
   Number of messages received 11
   Number of messages resent 0
  Message type Deregistration Response(5/0x5)
   Number of messages sent 6
   Number of messages received 1
   Number of messages resent 10
  Message type Deregistration Ack(6/0x6)
   Number of messages sent 1
   Number of messages received 5
   Number of messages resent 0
  Message type Registration Request(12/0xC)
   Number of messages sent 6
   Number of messages received 0
   Number of messages resent 0
  Message type Registration Response(13/0xD)
   Number of messages sent 0
   Number of messages received 6
   Number of messages resent 0
  Message type Registration Ack(14/0xE)
   Number of messages sent 6
   Number of messages received 0
   Number of messages resent 0

Message function type Context Delivery(4/0x4)
  Message type Context Delivery Request(1/0x1)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Context Delivery Report(2/0x2)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0

Message function type Auth Relay(8/0x8)
  Message type EAP Start(1/0x1)
   Number of messages sent 0
   Number of messages received 2
   Number of messages resent 0
  Message type EAP Transfer(2/0x2)
   Number of messages sent 56
   Number of messages received 56
   Number of messages resent 0
  Message type Key Change Directive(5/0x5)
   Number of messages sent 8
   Number of messages received 0
   Number of messages resent 0
  Message type Key Change Confirm(6/0x6)
   Number of messages sent 0
   Number of messages received 2
   Number of messages resent 0
Message type Key Change ACK(7/0x7)
   Number of messages sent 2
   Number of messages received 8
   Number of messages resent 0
  Message type CMAC Key Count Update(8/0x8)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type CMAC Key Count Update Ack(9/0x9)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0

Message function type MS State Change(9/0x9)
  Message type Attachment Response(7/0x7)
   Number of messages sent 6
   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 6
   Number of messages resent 0
  Message type Attachment ACK(9/0x9)
   Number of messages sent 0
   Number of messages received 6
   Number of messages resent 0
  Message type Pre Attachment Request(15/0xF)
   Number of messages sent 0
   Number of messages received 6
   Number of messages resent 0
  Message type Pre Attachment Response(16/0x10)
   Number of messages sent 6
   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 6
   Number of messages resent 0

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

Handoff Statistics
  Message type Successful Handoff
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Request
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Response
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Ack
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
Message type Handoff Deregistration Request
  Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Deregistration Response
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Deregistration Ack
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0

Undefined Message Function / Message Type
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
```

Mapping of Service Flows to DiffServ Classes

The ASN Gateway maps each individual Service flow to a Diffserv Class. The mapping rules are configured on the router. The mapping rules are designated in Table 2-2:

Table 2-2 Map of Each Individual Service Flow to a Diffserv Class

Service Flow - QoS Class	Applications	Diffserv Class on Network
UGS (Unsolicited Grant Service)	Voice/Video	EF
Real Time Polling Service	Voice/Video	EF
Non-Real Time Polling Service	Interactive Services	AF
Best Effort	Web Traffic	BE

Marking of Packets Corresponding to Service Flows

Each packet is identified and grouped according to the associated service flow. The transport headers corresponding to the packets are then marked with the associated Diffserv Code Point (DSCP) by the ASN Gateway based on the above table.

Configuring Service Flows on the ASN Gateway

To create service flows on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	router(config)# **wimax agw service-flow profile** *service-flow-profile-name*	Specifies a service-flow profile on the ASN Gateway. The **no** version of the command removes the profile. *service-flow-profile-name* is case insensitive. Configuring this command enters service flow configuration mode.
Step 2	router(config-gw-sf)# **direction {uplink | downlink}**	Specifies the direction of the service-flow the configuration is done, and enters service flow direction configuration submode. The **no** version of the command removes the corresponding configuration from the direction specified.
Step 3	router(config-gw-sf-dir)# **qos-info** *qos-profile-name*	Specifies which QoS information profile is associated under the corresponding direction. The **no** version of the command removes the QoS information from the corresponding direction.
Step 4	router(config-gw-sf-dir)# **pak-classify-rule** *pak-classify-rule-profile-name*	Specifies which packet classification rule profile is associated under the corresponding direction. The **no** version of the command removes the packet classification rule from the corresponding direction.
Step 5	router(config-gw-sf-dir)# **set {dscp | precedence}** **{***precedence-value* **|** *dscp-value***}**	Specifies what DSCP or TOS marking needs to apply for the subscriber packets in the downstream direction. By default no marking is done.

Configuration Example

The following are examples of Service Flow configuration commands:

```
Sample router configuration
#
!
wimax agw service-flow profile isf
 direction downlink
  pak-classify-rule isf-classifier-downlink
  qos-info isf-qos-downlink
 !
 direction uplink
  pak-classify-rule isf-classifier-uplink
  qos-info isf-qos-uplink
 !
!
```

```
wimax agw service-flow profile 2sf
 direction downlink
  pak-classify-rule dn-secondary-01
  qos-info downlink-qos-02
  set dscp ef
  set precedence immediate
 !
 direction uplink
  pak-classify-rule up-secondary-01
  qos-info uplink-qos-02
 !
!
```

Configuring Service Flow Packet Classification

To configure a service-flow packet classification rule profile on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	router(config)# w**imax agw service-flow pak-classify-rule profile** *service-flow-pak-classify-rule-profile-name*	Specifies a service-flow packet classification rule profile on the ASN Gateway. These are configured under the predefined service flows that are to be opened for the subscriber. When configured, this command enters into the packet classify rule configuration submode.
Step 2	router(config-gw-pak-classify-rule)# **command priority** *0-255* **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***]**	Configures a packet classification rule under the profile. Each packet classification rule should have a unique priority associated with it.

Configuration Example

Here is a sample configuration of the Service Flow Packet Classification configuration commands:

```
#
wimax agw service-flow pak-classify-rule profile isf-classifier-uplink
 priority 0 permit ip any any
!
wimax agw service-flow pak-classify-rule profile isf-classifier-downlink
 priority 0 permit ip any any
!
wimax agw service-flow pak-classify-rule profile up-secondary-01
 priority 2 permit ip any any
!
wimax agw service-flow pak-classify-rule profile dn-secondary-01
 priority 2 permit ip any any tos 8 24 10
!
```

Note The packet classifiers are looked at collectively for a given user and direction of flow for each packet, and the first matching priority rule applied (255 is highest priority). If no classifiers match, the default flow chosen is ISF in the downlink direction.

QoS Support

QoS support refers to both airlink QoS as well as mapping on the network. The ASN Gateway is responsible for sending the QoS parameters to the BS used to create the appropriate service flows.

Certain hosts can be given additional QoS parameters.

A new R6 bearer (service flow) is created that corresponds to the host's IP address. Multiple hosts can use this service flow.

Mapping of the host to the new R6 service flow is created and communicated to the BS/MS through the RR-Request.

ASN Gateway Release 1.0 offers the following support:

- Support for pre-provisioned QoS through CLI.
- Support for signaling traffic to be marked as separate class.
- Corresponding to every service flow based on the classifiers, a Diffserv Class would be mapped and used by the BS and the ASN Gateway.
- Support for all QoS class of service.

Configuring QoS

To configure QoS on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	`router(config)#` **`wimax agw service-flow profile qos-info`** *`service-flow-qos-info-profile-name`*	Allows the user to configure a service-flow QoS information profile on the ASN Gateway. These are associated to predefined service flows that are opened for the subscriber. Configuring the command opens a sub-configuration mode to configure various parameters.
Step 2	`router(config-gw-sf-qos-info)#` **`data-delivery-service {unsolicited-grant|real-time-variable-rate|non-real-time-variable-rate|best-effort| extended-real-time-variable-rate}`**	Configures data delivery service associated with certain predefined set of QoS-related service flow parameters. The default value is unsolicited-grant.
Step 3	`router(config-gw-sf-qos-info)#` **`maximum-latency`** *`maximum-latency-value`*	Configures the time period between the reception of a packet by the BS or MS on its network interface, and delivery of the packet to the RF interface of the peer device. If defined, 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. The default value is 0.

	Command	Purpose
Step 4	`router(config-gw-sf-qos-info)#` **`maximum-traffic-burst`** *`maximum-traffic-burst-value`*	Configures the parameter that defines the maximum burst size that is accommodated for the service. Since the physical speed of the ingress and 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 if the service is not currently using any of its available resources. The default value is 0.
Step 5	`router(config-gw-sf-qos-info)#` **`maximum-traffic-rate-sustained`** *`maximum-traffic-rate-sustained-value`*	Configures the parameter that defines the peak information rate of the service.
Step 6	`router(config-gw-sf-qos-info)#` **`media-flow-type`** *`media-flow-type-hex-string`*	Specifies the parameter that describes the application type, used as a hint in admission decisions; for example, VoIP, video, PTT, gaming, or others.
Step 7	`router(config-gw-sf-qos-info)#` **`policy-transmission-request`** *`policy-transmission-request-value`*	Specifies the policy transmission request value for the associated service flow. This value includes options for PDU formation, for uplink service flows, and restrictions on the types of bandwidth request options that may be used. An attribute is enabled by setting the corresponding bit position to 1.
Step 8	`router(config-gw-sf-qos-info)#` **`minimum-traffic-rate-reserved`** *`minimum-traffic-rate-reserved-value`*	Specifies (in bits per second) the minimum amount of data to be transported on behalf of the service flow when averaged over time. 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.
Step 9	`router(config-gw-sf-qos-info)#` **`sdu-size`** *`sdu-size-value`*	Specifies number of bytes in the fixed size SDU. This parameter is used 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 default value is 49.
Step 10	`router(config-gw-sf-qos-info)#` **`tolerated-jitter`** *`tolerated-jitter-value>`*	Specifies the maximum delay variation (jitter) for the connection.
Step 11	`router(config-gw-sf-qos-info)#` **`traffic-priority`** *`traffic-priority-value`*	Specifies the priority assigned to a service flow. For service flows that are identical (except priority), give the higher priority service flow a lower delay and higher buffering preference. For dissimilar service flows, the priority parameter does not take precedence over any conflicting service flow QoS parameter. The specific algorithm to enforce this parameter is not mandated here.

	Command	Purpose
Step 12	router(config-gw-sf-qos-info)# **unsolicited-interval-grant** *unsolicited-interval-grant-value*	Specifies the nominal interval between successive data grant opportunities for this service flow. This parameter is 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).
Step 13	router(config-gw-sf-qos-info)# **unsolicited-interval-polling** *unsolicited-interval-polling-value*	Specifies the maximum nominal interval between successive polling grant opportunities for this service flow.

Configuration Example

Here is a QoS configuration example:

```
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
```

Verifying the Configuration

To verify the QoS values on the ASN Gateway, use the **show wimax agw subscriber** command. Here is sample output for QoS statistics:

```
Router>sh wimax agw subscriber
MSID 1000.2228.0001
  Connection time 000:00:14
  Auth policy 0X0(0)
  Number of TIDs 1
  TID Key 10.1.1.70/2.2.2.2/1000.2228.0001
```

```
   Peer TID 0X2(2)
     FT MS State Change(9), MT Attachment Request(8)
   Our TID 0x8001(32769)
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 host 0.0.0.0 host 0.0.0.0

Service Flow information Uplink:
      Identifier 4
     QoS information:
      Data-delivery-service unsolicited-grant
      Minimum traffic-rate-reserved 41, 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 host 0.0.0.0 host 0.0.0.0
```

Table 2-3 and Table 2-4 identify the QoS Classes and Service Parameters for 802.16.

Table 2-3 QoS Classes in 802.16

QoS Parameter	BE Best Effort Service Flow	ERT-VR	UGS	RT-VR	NRT-VR
Traffic Priority 0-7 Def: 0	Optional	Optional *[a]*		Optional *[a]*	Optional *[a]*
Maximum sustained rate 0-4294967295 bits per second	Optional	Optional *[b]*		Optional *[b]*	Optional *[b]*
Minimum reserved rate 0-4294967295 bits per second		**X**	**X**	**X**	**X**
Maximum Traffic burst 0-4294967295 bits per second		Optional		Optional	Optional
Jitter Tolerance 0-4294967295 msc		Optional *[c]*	Optional *[c]*		
Maximum latency Tolerance 0-4294967295 msc		**X**	**X**	**X**	

Table 2-3 QoS Classes in 802.16 (continued)

QoS Parameter	BE Best Effort Service Flow	ERT-VR	UGS	RT-VR	NRT-VR
Unsolicited Grant Interval 0-65535 msc		**X**	**X**		
SDU Size 0-255 Bytes Def: 49			Optional *[d]*		
Unsolicited Polling Interval 0-65535 msc				**X**	
DSCP					

Table 2-4 QoS Classes and Service Parameters in 802.16

QoS Class	Application	QoS Spec Service Parameter
Unsolicited grant service (UGS)	**VoIP** For real-time, fixed size regularly transmitted packets, e.g., voice codec, ATM CBR, E1/T1 over ATM.	Maximum sustained rate Maximum latency tolerance Jitter tolerance
Real-time polling service (rtPS)	**Streaming Audio, Video** For real-time variable size regularly transmitted packets, e.g., MPEG video, VoIP, streaming.	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Traffic priority
Extended Real-Time Packet Service (ErtPS)	**VoIP (with VAD)**	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Jitter tolerance‘
Non-real-time polling service (nrtPS)	**FTP** For non-real-time service flows, requiring variable size, regular Data Grant Burst, e.g., Internet access, ATM GFR	Minimum reserved rate Maximum sustained rate Traffic priority
Best effort service flow (BE)	**Data Transfer, Web, Browsing**	Maximum sustained rate Traffic Priority

DSCP Marking Per Service Flow

Each service flow is mapped uniquely to a Diffserv Code Point (DSCP). This DSCP value is used to mark the outer IP header for downstream packets by the ASN Gateway, and by the BS for upstream packets.

The inner IP header for upstream and downstream packets is set by the ASN Gateway as per the mapping for the service flow, unless explicitly disabled by a CLI.

ACLs

ACLs are supported, and can be configured at a per-user group basis. This applies to all users that connect to the same user-group.

Source IP Address Validation

For all uplink packets, the allocated IP address for the corresponding MS or service flow is validated. If a mismatch is found, those packets are discarded.

To configure this feature, use the **security subscriber address-filtering ingress** command in gateway user group submode.

Support of Split Control and Data End Points for BS

The BS may have different end point IP addresses for the control and the data plane. Depending on the availability of the Data Path End Point ID TLV (sent in path registration response message from the BS for the flow), the ASN Gateway can create the GRE path taking the ipv4 from the available TLV.

If the specified TLV is not present, the control plane end point address is used as the remote data end point to create GRE path.

The data and control plane split is only supported for BS in Release 1.0. Depending on the requirement, the ASN Gateway may support this feature in future releases.

Bearer Accounting

Bearer volume counts are maintained for all service flows. These include the input and output packets and octet counts.

User Group Management

To configure user groups on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	router(config)#**wimax agw user group-list** *user-group-list-name*	Configures the user group list on the ASN Gateway router. The **no** version of command removes the user group list. Enabling this command enters you into user group list sub configuration mode to create multiple user groups under the user-group list created.
Step 2	router(config-gw-ug)# **service-flow pre-defined {isf | secondary** *secondary-index***} profile** *sf-profile-name*	Specifies the number of pre-defined service flows to be opened for a subscriber. If the **ISF** keyword is configured, the service flow is assumed to be the initial service flow. The **secondary** keyword represents the auxiliary service flows for the subscriber. Currently 1 initial service flow, and up to 3 secondary service flows, are allowed per subscriber.

Sample Configuration

The following example illustrates how to configure a user group:

```
#
!
wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  service-flow pre-defined isf profile isf
 !
 user-group domain eap-tls.com
  aaa accounting method-list agw
  service-flow pre-defined isf profile isf
  service-flow pre-defined secondary 1 profile 2sf
 !
 user-group unauthenticated
  aaa accounting method-list agw
  service-flow pre-defined isf profile isf
  service-flow pre-defined secondary 1 profile 2sf
```

Idle Timer Support

An idle timer is configurable on the ASN Gateway for a User group. If there is no data traffic for the duration of the timer, the SS/MSS will be de-registered. Idle timeout can be downloaded from the AAA server during the authentication phase.

Here is a sample configuration:

```
wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  dhcp server primary 11.1.1.93
  service-flow pre-defined isf profile isf
  timeout idle 30
  timeout session 30
 !
 user-group unauthenticated
  aaa accounting method-list agw
  dhcp server primary 11.1.1.93
  service-flow pre-defined isf profile isf
  service-flow pre-defined secondary 1 profile 2sf
 !
!
```

Idle timer support is available for inbound traffic in the ASN.

If an idle timer value is configured in AAA and under an ASN user-group, then AAA is given precedence.

Session Timer Support

A Session or Absolute timer is configurable on the ASN Gateway for a User group. When the timer expires, the subscriber is de-registered. Session timeout can be downloaded from the AAA server during the authentication phase.

Mobile Subscriber Station De-Registration

Cisco ASN Gateway Release 1.0 supports Network Exit as a result of Path Deregistration messaging.

There are two possible ways to deregister a Mobile Subscriber Station:

Mobile Subscriber Station Initiated De-Registration

Step 1 The SS sends DREG-REQ message to the BS, to start de-registration procedure.

Step 2 The BS sends Data Path De-Reg Request to ASN Gateway.

Step 3 ASN Gateway sends Data Path De-Reg Response to BS with the action code (set to 0x04) to authorize de-registration procedure.

Step 4 BS sends DREG-CMD to SS to de-register the SS.

Step 5 BS sends Data Path De-Reg Ack to ASN Gateway to complete the transaction.

Network-Initiated De-Registration

Step 1 The ASN Gateway sends out a Data Path De-Reg Request message to the BS indicating the MS to be deleted.

Step 2 The BS sends out a DSD-REQ over the airlink to deregister the specific Service Flows.

Step 3 BS gets DSD-RSP from SS indicating the termination of the service flow.

Step 4 BS sends Data Path De-Reg Response to ASN Gateway indicating the termination of service flow.

Step 5 ASN Gateway sends Data Path De-Reg Acknowledgement, to terminate the transaction.

AAA Accounting Start-Stop-Interim

ASN Gateway supports per service flow accounting information. Only time based Interim accounting updates are supported. The ASN Gateway supports per service flow, and generates a unique set of accounting records for each service-flow tuple (Acct-Session-Id + Acct-Multi-Session-Id + PDFID). Each service flow is uniquely identified by a GRE key. A given MS can have more than one service flow.

Note Per-session accounting is not supported in this release.

For all the accounting records sent by the ASN Gateway, the Framed-IP-Address field is set to the mobile's IP address, irrespective of which host behind the mobile the traffic is sent for.

The ASN Gateway sends the following messages to the AAA server:

- Accounting Start: The ASN Gateway sends this message to the AAA server when a new service flow is created. In case of redundant ASN Gateway configuration, a stand-by ASN Gateway sends an Accounting Start message only when it becomes active. The trigger for the Accounting Start is the successful creation of the service flows. In case of the initial service flow, the accounting start record is sent only after the IP address is allocated to the users. For the secondary service flow, the accounting record is sent as soon the flow is successfully opened with the BS.
- Accounting Interim Update: The ASN Gateway generates an Accounting Update message if periodic accounting update message is configured. The accounting updates are based on a time trigger, and when configured. The minimum permitted value for the timer is 1 minute.
- Accounting Stop: The ASN Gateway sends and Accounting Stop message when the service flow is deleted or when the MS completes the deletion.

The attributes sent in the accounting record are listed in Table 2-5:

Table 2-5 ASN Gateway-AAA Authentication Attributes

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
User-Name	1	NAI obtained from the EAP-Response Identity (Outer-NAI)	1	0	0-1	
Service-Type	6	Set to "Framed" for initial authentication and set to "Authenticate-Only" indicating Re-authentication. It may also be set to "Authorize-Only" when used to obtain prepaid quotas mid-session.	1	0	0-1	0

Table 2-5 ASN Gateway-AAA Authentication Attributes (continued)

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
Framed-MTU	12	Used by WiMAX, as per RFC3579 in an Access-Request during EAP authentication, this attribute provides the appropriate MTU size to avoid exceeding maximum payload size for PKMv2 (2008 bytes) during EAP exchange (the appropriate fragmentation is assumed in Authentication Server on the EAP application layer). The value of this attribute should be set between 1020 and 2000 bytes (the recommended value is 1400 bytes). In an Access-Accept the use is as per RFC2865.	0-1[m]	0	0-1[m]	0
EAP-Message	79	The EAP message	1-n	1-n	1-n	1-n
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [RFC3579]	1	1	1	1
WiMAX-Capability	26/1	Identifies the WiMAX Capabilities supported by the NAS. Indicates capabilities selected by the RADIUS server.	1	0	0-1[k]	0
NAS-ID	32	FQDN of the NAS	1[b]	0	0	0
NAS-Port-Type	61	Identifies the type of port the request is associated with. Set to WiMAX when coming from a WiMAX ASN. Set to MIPv4 or MIPv6 when coming from an HA.	1	0	0	0
Calling-Station-Id	31	Set to the MAC address of the Device(MS).	1	0	0	0
Device-Authentication-Indicator	26/2	Indicates whether the device authentication was performed, and the result.	0-1[i]	0	0	0
GMT Timezone-Offset	26/3	The offset in seconds from GMT at the NAS.	1	0	0	0
NAS-IP-Address	4	NAS IP Address. Either NAS-IP-Address.	0-1[b]	0	0	0
Error-Cause	101	Error Codes generated during access authentication [RFC3576].	0	0-1	0	0-1
Class	25	Opaque value set by the server used to bind authentication to accounting.	0	0	0-1[h][k]	0
Framed-IP-Address	8	The MIPv4 home address to be assigned to the MN.	0	0	0-1[c][k]	0
Session-Timeout	27	The maximum number of seconds of service to be provided to the user before termination of the session. Associated with the lifetime of the keys	0	0	0-1[d][k]	0
Termination-Action	29	Indicates what action the NAS should take when service is completed.	0	0	0-1[d][k]	0

Table 2-5 ASN Gateway-AAA Authentication Attributes (continued)

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
AAA-Session-ID	26/4	A unique identifier in the home realm for this Session.	0-1[e]	0-1	1	0
BS-ID	26/46	Indicates the NAP-ID and BS-ID at the time the message was delivered	0-1[n]	0	0	0
MSK	26/TBD	The Master Session Key derived as the result of successful EAP Authentication.	0	0	1[f]	0
Session-Timeout	27	The maximum number of seconds of service to be provided to the user before termination of the session. Associated with the lifetime of the keys derived from the EAP authentication (i.e., MSK, EMSK and keys derived from EMSK) Session-Timeout in an Access-Challenge packet is used set the EAP-retransmission timer as per RFC3579.	0	0-1	0-1[d][k]	0

[b] NAS-ID MUST appear in the Access-Request. NAS-IP-Address may also appear. NAS-ID may be configured on the CLI using the **radius-server attribute 32 include-in-access-req** command.

[c] If this attribute is present then the home address assigned to the mobile must be as specified by this attributes. If this attribute is absent then the home address is derived from MIP procedures or other means (for example, DHCP).

[d] Both Session-Timeout and Termination-Action MUST be present. Termination-Action MUST be set to "RADIUS-Request"(1). This causes the NAS to re-authenticate when the Session-Timeout expires.

[f] The attribute must be encrypted using the procedures in section 3.5 of RFC2868

[h] If more then one class attribute is found in an Access-Accept message, the NAS shall store all of them and send them back in the accounting request packets.

[i] Must appear in the Access-Request associated with the User Authentication phase of the Double EAP Device, user authentication procedure. Otherwise, the attribute MUST not be present in the Access-Request message.

[k] Attributes must not appear in the Access Accept sent associated with the Device Authentication phase of double EAP.

[m] If the Framed MTU appears in an Access-Request during Access-Authentication then it indicates the MTU on the link between the NAS and the MS. As per RFC3579, the RADIUS shall not send any subsequent packet in this EAP conversation containing EAP-Message attributes whose values, when concantenated, exceed the length specified by the Framed-MTU value.

[n] Either the BS-ID or NAP-ID SHALL be provided. If both are provided the receiver SHALL ignore the NAP-ID attribute. In Release 1.0, NAP_ID is not sent to AAA. NAP-ID is 24 (MSB) bits of 48 bit BSID (when BS will send it in future).

Configuring AAA Accounting

To enable the accounting feature on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	`router(config)# ` **`aaa accounting network {`***`accounting-list-name`***`} {none|start-stop|stop-only} {broadcast|group} {`***`server-group-name`***`|radius}`**	Enables the accounting for network services. For WiMAX, an accounting method list name is required.
Step 2	`router(config)# ` **`aaa accounting update {newinfo|periodic} {`***`periodic intervals to send accounting updates in minutes`***`}`**	Enables the accounting updates at periodic intervals. The **no** version of this command disables the sending of accounting updates.

	Command	Purpose

Step 3	`router(config)# `**`wimax agw user group-list`**
	`user-group-list-name`
		Configures the user group list on the ASN Gateway router. Only one user group list is allowed on a single processor of the ASN Gateway. The **no** version of command removes the user group list. This command enters a user group list sub-configuration mode to create multiple user groups under the *user-group list* created.

Step 4	`router(config-gw-ug)# `**`aaa accounting method-list`** **{***`method-list-name`*| **`default}`**	Specifies the accounting method list used for the domain.

Configuration Example

Here is an example of a user group configuration:

```
wimax agw user group-list wimax
  user-group any
   aaa accounting method-list agw
   aaa authentication method-list agw
!
  user-group domain cisco.com
   aaa accounting method-list agw
   aaa authentication method-list agw
!
  user-group unauthenticated
   aaa accounting method-list agw
```

Here is an example of a AAA and RADIS configuration:

```
aaa new-model
!
aaa accounting update periodic 15
aaa accounting network agw start-stop group radius
aaa authorization network default group radius
aaa authentication dot1x agw group radius
!
radius-server attribute 32 include-in-access-req format %h.%d.%i
radius-server attribute 55 access-request include
radius-server attribute 25 accounting prefer-preauth
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
radius-server host 172.19.25.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 1.8.91.8 auth-port 1645 acct-port 1646 key cisco

!
```

Verifying the Configuration

Here is an example of the **show wimax agw subscriber** command, used to verify the accounting configuration:

```
Router#sh wimax agw subscriber msid 1000.0002.0001
 Connection time 000:01:08
 Auth policy 0X12(18), Single-EAP, CMAC
 Number of TIDs 1
 TID Key 10.1.1.82/2.2.2.2/1000.0002.0001
  Peer TID 0X4(4)
```

```
    FT MS State Change(9), MT Attachment Request(8)
  Our TID 0x8004(32772)
 Subscriber address 2.2.0.8, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 Subscriber address assigned on flow downlink ID 15
 Subscriber address prefix len allocated 32, aggregate 32
 Subscriber address traffic sent 0 packets, 0 bytes
 Subscriber address traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 2390, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 1000.0002.0001, 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)
   Username eap-md5-u@eap-md5.com
   Authentication method EAP
AAA session-id length 7, 0x30313233414243
   AAA termination-action 1
   Reauthentication attempts from subscriber 0, ASNGW 0
   Associated user group **any**
   Signalling address local 2.2.2.2, remote 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:09, outbound 00:01:09
   Absolute timeout 1500, remaining 00:23:49
   Idle timeout 600 (both), remaining 00:08:50
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8004(32772)
     Data ID local 0x8(8), remote 0x1(1)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 705 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:09, outbound 00:01:09
     Service Flow information Downlink: Identifier 15
```

Here is sample RADIUS output for a AAA accounting start:

```
*Aug 11 02:27:21.143: RADIUS(00000006): Send Accounting-Request to
 1.8.91.8:1646 id 1646/61, len 165
*Aug 11 02:27:21.143: RADIUS:  authenticator C4 F4 3F A3 00 1C 01 66 - 78
 DD A4 B4 68 37 F9 5B
*Aug 11 02:27:21.143: RADIUS:  Acct-Session-Id     [44]  10  "00000006"
*Aug 11 02:27:21.143: RADIUS:  Framed-Protocol     [7]   6   noval0
 [0]
*Aug 11 02:27:21.143: RADIUS:  Called-Station-Id   [30]  9   "2.2.2.2"
*Aug 11 02:27:21.143: RADIUS:  Framed-IP-Address   [8]   6   2.2.0.76
*Aug 11 02:27:21.143: RADIUS:  Calling-Station-Id  [31]  19  "10-00-22-
 25-00-01"*Aug 11 02:27:21.143: RADIUS:  Acct-Input-Octets   [42]  6   1208
*Aug 11 02:27:21.143: RADIUS:  Acct-Output-Octets  [43]  6   666
*Aug 11 02:27:21.143: RADIUS:  Acct-Input-Packets  [47]  6   2
*Aug 11 02:27:21.143: RADIUS:  Acct-Output-Packets [48]  6   2
*Aug 11 02:27:21.143: RADIUS:  Vendor, Wimax       [26]  13
*Aug 11 02:27:21.143: RADIUS:   GMT-Time-Zone-Offse[3]   7
*Aug 11 02:27:21.143: RADIUS:   00 00 00 00 00
 [?????]
*Aug 11 02:27:21.143: RADIUS:  Vendor, Wimax       [26]  11
*Aug 11 02:27:21.143: RADIUS:   Packet-Data-Flow-ID[26]  5
*Aug 11 02:27:21.143: RADIUS:   00 00 00
 [???]
*Aug 11 02:27:21.143: RADIUS:  Acct-Session-Time   [46]  6   1630
*Aug 11 02:27:21.143: RADIUS:  Acct-Status-Type    [40]  6   start
```

```
 [3]
*Aug 11 02:27:21.143: RADIUS:  NAS-Port-Type       [61]  6   802.16e Wimax
 [27]
*Aug 11 02:27:21.143: RADIUS:  NAS-Port-Id         [87]  11  "WiMAX-AGW"
*Aug 11 02:27:21.143: RADIUS:  Service-Type        [6]   6   Framed
 [2]
*Aug 11 02:27:21.143: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Aug 11 02:27:21.143: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 11 02:27:21.175: RADIUS/ENCODE(00000007):Orig. component type = AGW
*Aug 11 02:27:21.175: RADIUS/ENCODE: NAS PORT sending disabled
*Aug 11 02:27:21.175: RADIUS(00000007): Config NAS IP: 0.0.0.0
*Aug 11 02:27:21.175: RADIUS(00000007): sending
*Aug 11 02:27:21.175: RADIUS/ENCODE: Best Local IP-Address 2.2.2.2 for
 Radius-Server 1.8.91.8
```

Here is sample RADIUS output for a AAA accounting stop:

```
*Feb 18 15:30:29.011: RADIUS(00000006): Send Accounting-Request to
 172.19.25.8:1646 id 1646/24, len 252
*Feb 18 15:30:29.011: RADIUS:  authenticator 6D FC 9B 49 59 28 56 41 - 3F 2E A5
 3C 7B 7A 3A B1
*Feb 18 15:30:29.011: RADIUS:  Acct-Session-Id     [44]  10  "00000008"
*Feb 18 15:30:29.011: RADIUS:  Framed-Protocol     [7]   6   noval0
[0]
*Feb 18 15:30:29.011: RADIUS:  Called-Station-Id   [30]  9   "2.2.2.2"
*Feb 18 15:30:29.011: RADIUS:  Framed-IP-Address   [8]   6   2.2.0.2
*Feb 18 15:30:29.011: RADIUS:  Calling-Station-Id  [31]  19  "06-76-22-24-22-22"
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  10
*Feb 18 15:30:29.011: RADIUS:   AAA-Session-ID     [4]   4
*Feb 18 15:30:29.011: RADIUS:   00 00
[??]
*Feb 18 15:30:29.011: RADIUS:  User-Name           [1]   23  "eap-md5-u@eap-
 md5.com"
*Feb 18 15:30:29.011: RADIUS:  Acct-Input-Octets   [42]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Output-Octets  [43]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Input-Packets  [47]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Output-Packets [48]  6   0
*Feb 18 15:30:29.011: RADIUS:  Multilink-Session-ID[50]  10  "30313233"
*Feb 18 15:30:29.011: RADIUS:  Class               [25]  21
*Feb 18 15:30:29.011: RADIUS:   63 6C 61 73 73 2D 77 69 6D 61 78 2D 63 68 61 6E
[class-wimax-chan]
*Feb 18 15:30:29.011: RADIUS:   67 65 64
[ged]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  13
*Feb 18 15:30:29.011: RADIUS:   GMT-Time-Zone-Offse[3]   7
*Feb 18 15:30:29.011: RADIUS:   00 00 00 00 00
[?????]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  17
*Feb 18 15:30:29.011: RADIUS:   BaseStation-ID     [46]  11
*Feb 18 15:30:29.011: RADIUS:   00 0A 01 01 46 00 00 00 00
[????F????]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  11
*Feb 18 15:30:29.011: RADIUS:   Packet-Data-Flow-ID[26]  5
*Feb 18 15:30:29.011: RADIUS:   00 05 01
[???]
*Feb 18 15:30:29.011: RADIUS:  Acct-Session-Time   [46]  6   25
*Feb 18 15:30:29.011: RADIUS:  Acct-Terminate-Cause[49]  6   none
[0]
*Feb 18 15:30:29.011: RADIUS:  Acct-Status-Type    [40]  6   Stop
[2]
*Feb 18 15:30:29.011: RADIUS:  NAS-Port-Type       [61]  6   802.16e Wimax
[27]
*Feb 18 15:30:29.011: RADIUS:  NAS-Port-Id         [87]  11  "WiMAX-AGW"
*Feb 18 15:30:29.011: RADIUS:  Service-Type        [6]   6   Framed
```

```
[2]
*Feb 18 15:30:29.011: RADIUS:  NAS-IP-Address      [4]   6   172.19.24.88
*Feb 18 15:30:29.011: RADIUS:  Acct-Delay-Time     [41]  6   0
*Feb 18 15:30:29.019: RADIUS: Received from id 1646/23 172.19.25.8:1646,
Accounting-response, len 20
*Feb 18 15:30:29.019: RADIUS:  authenticator 4D 1A 1B 4D C5 0E 39 FD - 36 6B 90 FF 96 21
66 64
*Feb 18 15:30:29.019: RADIUS: Received from id 1646/24 172.19.25.8:1646,
Accounting-response, len 20
*Feb 18 15:30:29.019: RADIUS:  authenticator EB 25 42 F1 48 2C BF 13 - 43 B0 0A 3A 7A 04
F4 1F
```

WiMAX Specific VSAs

The following VSAs are specific to WiMax:

- Wimax Capability—Indicates the WiMAX release, accounting capabilities indication, Hotlining capabilities, and Idle Mode Notification capabilities of the ASN Gateway to the AAA in an Access Request.
- GMT Time Zone Offset—The current offset in seconds of the local time at the NAS with respect to GMT time.
- Packet Data Flow-Id (PDFID)—The value of this attribute matches all records from the same packet data flow. PDFID is assigned by the CSN, and remains constant through all handover scenarios. In Release 1.0, the ASN Gateway generates the PDFID for a flow in the session.
- Base Station ID—Uniquely identifies a NAP and a base station within that NAP. The ASN Gateway forwards the R6 BS ID in this attribute.
- AAA Session ID—A unique per realm identifier assigned to the WiMAX session by the home network during network entry. The value is included in all subsequent AAA packets for that session.

Handoffs

Multiple forms of handoff are supported for WiMax, both inter-base station and inter-ASN Gateway. However, Release 1.0 of the ASN Gateway only supports inter-base station handoff.

Inter-BS handoff includes both predictive and unpredictive handoff. In the predictive case, the ASN Gateway is informed of the impending move of a mobile device to a new BS before the handoff actually occurs. Unpredictive handoff occurs when the device has already moved from the source BS before the ASN Gateway receives a handoff trigger.

Release 1.0 of the ASN Gateway only supports unpredictive handoff.

Unpredictive handoff includes two variants: controlled and uncontrolled.

Uncontrolled handoffs occur where information exchange between base stations is not possible prior to the target BS triggering a handoff at the ASN Gateway. Uncontrolled handover is treated identically to Initial Network Entry, with the addition that the ASN Gateway ensures that paths registered with the serving base station are deregistered. The only addition being that for Release 1.0, one attempt is made to send the deregistration message to the serving BS, and the handoff takes place regardless of the completion of the deregistration handshake between the ASN and SBS.

For uncontrolled handoffs, the path will not be deregistered if there are already MS available in that path—deregistration is sent to the old BS for the MS. If that is the last MS in the path, then the path is deleted.

Handoffs do not trigger interim accounting updates.

Unpredictive Handoff

An unpredictive controlled handover is signaled from the BS to the ASN Gateway using a Path Registration Request message. This message contains information for each service flow that is already established with the source BS. It also contains the DP-IDs used for downlink flows.

Note There is no need to re-authenticate the device or the subscriber, as the session is maintained at the same ASN Gateway.

Note In un-predictive handoff, the target BS will trigger a MS network entry in which the MS will get authenticated.

The ASN Gateway initiates the deregistration of the path to the old BS. This deregistration will be scheduled by the ASN Gateway. It does not necessarily occur directly after successful completion of handoff to the new BS.

There is no requirement to buffer bearer path data during handoff. Downlink data received at the ASN Gateway during the handover procedure is discarded.

Any traffic that is “in-flight” through the old path is lost because the device has already moved to the service area of the target BS before to the handoff trigger is received at the ASN Gateway.

It is possible that the device may move to a new BS while the handoff procedures between the target BS and the ASN Gateway are completed. Because the handover is uncontrolled, the handoff to the current target BS is completed (including R6 message retransmissions, if necessary) before the new handoff event is processed.

The handover exchange comprises three messages (applicable only for controlled handoff):

- Path Registration Request—sent from the Target BS to the ASN Gateway—which contains the following:
  - Registration Type
  - SF INFO(s) with SFID, Reservation Action (set to Create), Direction, QoS parameters, Data Path Info and GRE Key (for downlink flows)
  - BS INFO with BSID
- Path Registration Response—sent from the ASN Gateway to the Target BSq—which contains the following:
  - Registration Type
  - SF INFO(s) with SFID, Reservation Action (set to Success), Direction, Data Path Info & GRE Key (for uplink flows)
  - BS INFO with BSID
- Path Registration Acknowledgement—sent from the Target BS to the ASN Gateway—which contains the following:
  - Registration Type

If ASNGateway cannot accept the handover, it sends the response with “reject cause code TLV”.

If the ASN Gateway accepts the handover for only a subset of the desired Service Flows, the handover is rejected.

Handoff will not be rejected if secondary flow is missing, but if primary flow is missing it will be rejected.

The Deregistration Request and ACK sent to SBS will have the registration type as “Handover” while Deregistration response from SBS will have “Network exit”. This is an expected behavior. On receiving this, the ASN Gateway does not send the ACK with “reject cause code TLV”.

Unpredictive Controlled Handoff

An unpredictive controlled handoff occurs when the current and target BSs are able to communicate information and exchange details about service flows, classifiers, and other details, prior to the target BS triggering the handoff at the ASN Gateway. This means that the target BS has all relevant information about the mobile device prior to sending the ASN Gateway handoff trigger. This trigger occurs when the mobile device has already been connected to the target BS using 802.16e procedures. You can tell a controlled handoff occurred at the ASN Gateway by the receipt of a Path Registration Request message from the BS without a previous authentication exchange (which would be observed for a Network Entry event).

The following flow sequence illustrates the events that occur during a controlled handoff:

Step 1 The Target Base Station sends a Path Registration Request to the ASN Gateway containing the service flow information received from the Serving Base Station.

Step 2 The ASN gateway responds with a Path Registration Response accepting registration of the data path with the Target base Station.

Step 3 The Target Base Station responds with a Path Registration Acknowledgement.

Step 4 The ASN gateway sends a Path Deregistration Request to the Serving Base Station.

Step 5 The Serving Base Station responds with a Path Deregistration Response.

Step 6 The ASN Gateway acknowledges the response with a Path Deregistration Acknowledgement.

Step 7 The Target Base Station sends a Context Report to the ASN Gateway.

Step 8 The ASN Gateway acknowledges with a Context Acknowledgement.

Step 9 The target BS sends a CMAC Key Count Update message, and the ASN Gateway responds with a CMAC Key Count Ack message.

Verifying the Configuration

To view the handoff statistics for the ASN Gateway, use the **show wimax agw statistics section handoff** command.

Here is a sample configuration:

```
Router#show wimax agw statistics section handoff
Message type Successful Handoff
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Request
   Number of messages sent 0
   Number of messages received 2
```

```
 Number of messages resent 0
Message type Handoff Registration Response
 Number of messages sent 2
 Number of messages received 0
 Number of messages resent 0
Message type Handoff Registration Ack
 Number of messages sent 0
 Number of messages received 2
 Number of messages resent 0
Message type Handoff Deregistration Request
 Number of messages sent 2
 Number of messages received 0
 Number of messages resent 0
Message type Handoff Deregistration Response
 Number of messages sent 0
 Number of messages received 0
 Number of messages resent 0
Message type Handoff Deregistration Ack
 Number of messages sent 0
 Number of messages received 0
 Number of messages resent 0
```

Security Context Exchange

In order for a BS to secure the airlink, it requires keying material from the ASN Gateway. A handoff cannot be successful from the perspective of the BS and the device until the data path registration has completed, and the BS receives the keying material. The BS is responsible to initiate both procedures. The ASN Gateway treats a context exchange with the BS as an entirely separate event from handover.

A context exchange can occur at any time. The AK transfer protocol is used to transfer the keying material to the BS. This material comprises the AK, AKID, AK Lifetime, AK sequence number and EIK.

If the PMK has expired, then a new PMK must be created.

The security context exchange comprises two messages.

- Context Request—sent from the target BS to the ASN Gateway—which contains the following:
  - Context Purpose Identifier
  - BS Info
  - Target BS ID
- Context Report—sent from the ASN Gateway to the target BS—which contains the following:
  - MS Info
  - AK Context
  - AKID
  - AK lifetime
  - AK SN
  - CMAC Key count
  - Target BS Info
  - Target BS ID

Keepalive Support for R6 Interface

The keepalive mechanism is based on the periodic transmission of “keepalive” messages between the BS and the ASN Gateway.

Transmission of the keepalive messaging is configurable at the ASN gateway.

Note When a Base Station ASN Gateway receives an R6 Keepalive Request message, it must send an R6 Keepalive reply.

For each R6 instance, ASN gateway maintain the following configurable parameters:

- Tk: Keepalive timer
- N: Number of consecutive keepalive failures. Initialized to 0
- M: Permitted maximum number of consecutive keepalive failures.

The supported keepalive functionality in this release is as follows:

Step 1 The base station or ASN Gateway sends a Keepalive_Request and starts timer Tk.

Step 2 On receipt of a Keepalive_Reply, the value of N is reset to 0.

Step 3 When Tk expires, the node sends the next Keepalive_Request. N is incremented if a Keepalive_Reply for the last Keepalive_Request message was not received prior to expiry of timer Tk.

Step 4 When N equals M, N is reset to 0 and any R6 sessions established with the remote node are terminated locally (with no attempt to send any further cleanup message to remote end) and any data related to subscribers, belonging to the specific R6 interface is cleaned up.

The following two TLVs will be used in this release:

- BS ID TLV to identify the BS which is either a recipient or initiator of the request.
- ASN Gateway ID to identify the ASN Gateway which is either the recipient or initiator of the request.

Configuring Keepalive

To configure the keepalive value on the ASN Gateway, perform the following task:

	Command	Purpose
Step 1	`router(config)#` **`wimax agw base-station group`** *`name`*	Configures a base-station group, and enters user into the ASN Gateway basestation configuration submode. All of the individual base stations configured to belong to this base station group use the base station group parameters. The **no** version of this command deletes the base station group. The base station group can only be deleted if all the references to this group are also deleted.
Step 2	`router(config-wimax-agw-bs)#` **`reference-point r6 keepalive`**	Specifies if keepalive packets between the ASN Gateway and BS are enabled. Default is not enabled.
Step 3	`router(config-wimax-agw-bs)#` **`reference-point r6 keepalive timeout`** *`interval-in-minutes`*	Specifies the keepalive interval in seconds. If this command is not configured, then the keepalive interval is set to the default value (60 seconds).
Step 4	`Router(config-wimax-agw-bs)#`**`reference-point r6 path purge-timeout`**	Configures the path purge timer value in minutes. As soon as the last session associates with the BS path goes away, the path purge timer is started to remove the path after the timer expiry.

Configuration Example

Here is a sample configuration of the Keepalive configuration commands:

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

Here is a configuration example of the **reference-point r6 path purge-timeout** command:

```
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
```

Verifying the Configuration

To verify various ASN Gateway system parameters, perform the following tasks:

	Command	Purpose
Step 1	Router#**show wimax agw**	Displays various system parameters, including ASN Gateway software version, number of base stations allowed, number of subscribers allowed, number of flows, and others.
Step 2	Router#**show wimax agw path 10.1.1.70**	Displays base station information.
Step 3	Router#**show wimax agw subscriber brief**	Displays subscriber information.

Configuration Examples

Here is a sample configuration that identifies the ASN Gateway keepalive statistics:

```
Router#show wimax agw statistics | section Keepalive
Message function type Keepalive(20/0x14)
  Message type Keepalive Request(1/0x1)
   Number of messages sent 21
   Number of messages received 0
   Number of messages resent 0
  Message type Keepalive Response(2/0x2)
   Number of messages sent 0
   Number of messages received 21
   Number of messages resent 0
```

Here is a sample configuration that identifies generic ASN Gateway statistics:

```
Router#show wimax agw
Access network gateway version 1.0, service is enabled
 Signaling UDP port 2231
 Maximum Number of base station 500 allowed
 Maximum Number of subscriber 20000 allowed
  Current number of signalling paths 1
  Current number of data paths 1
  Current number of subscribers 3
  Current number of sessions 3
  Current number of flows 6
  Current number of hosts 0
  Traffic Sent 6 packets, 1998 bytes
  Traffic Rcvd 7 packets, 4228 bytes
```

Here is a sample configuration that identifies ASN Gateway base station statistics:

```
Router#show wimax agw path 10.1.1.70
Path type Sig-UDP
 State current Ready, old Idle
 Number of sessions connected 3
 Number of old sessions connected 0
 Address local 2.2.2.2(AF_INET), remote 10.1.1.70(AF_INET)
 UDP port local 2231(0x8B7), remote 2231(0x8B7)
 Identification, Our 0x02020202
 Keepalive timer expires in 00:00:25, timeout 30 secs
 Keepalive consecutive failures max allowed 5, current 0
 Keepalive Request received valid 0, invalid 0
 Keepalive Response received valid 11, invalid 0
 Keepalive Request sent success 11, fail 0
 Keepalive Response sent success 0, fail 0
 Traffic sent 29 packets, 3175 bytes
 Traffic received 28 packets, 2658 bytes


Path type Data-GRE
 Number of flows connected 6
 Address local 2.2.2.2(AF_INET), remote 10.1.1.70(AF_INET)
 Traffic sent 6 packets, 2166 bytes
 Traffic received 7 packets, 4522 bytes
```

Here is a sample configuration that identifies ASN Gateway subscriber statistics:

```
Router#show wimax agw subscriber brief

MSID           Address         Age       Flows Hosts Pkts-Tx    Pkts-Rx
1000.2223.0001 2.2.0.75        000.22.08 2     0     2          3
1111.1113.1111 2.2.0.74        000.22.05 2     0     2          2
1000.2225.0001 2.2.0.76        000.21.56 2     0     2          2
```

Session Redundancy

Note ASN Gateway Session redundancy is not supported on the Cisco 7301 Router platform.

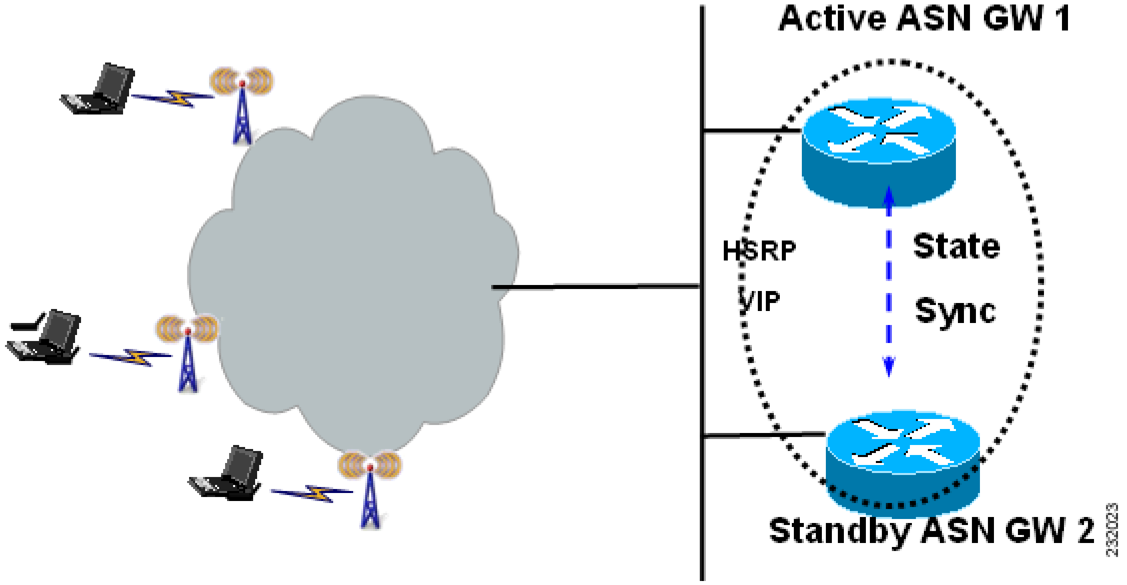
The ASN Gateway Session Redundancy architecture provides user session failover capability in a 1:1 redundancy model, with a standby present for every active ASN Gateway. The active ASN Gateway sends state information to the standby ASN Gateway for state synchronization on a as needed basis. When an active ASN Gateway failure occurs, the standby ASN Gateway has state information needed to provide service to all existing sessions. It then takes over as the active ASN Gateway and begins servicing user sessions, thus providing session redundancy. When the previously active ASN Gateway comes back online, it takes over as standby for the now active ASN Gateway, and obtains state information for all existing sessions from it.

The ASN Gateway is hosted on the SAMI blade, and only card to card redundancy will be supported. In other words, failure of a single processor unit on SAMI will result in the entire card being switched over.

ASN Gateway Session Redundancy and High Availability Infrastructure

The ASN Gateway Session Redundancy is based on the Cisco IOS Hot Standby Routing Protocol (HSRP), the Cisco IOS Check-point Facility (CF) and Redundancy Framework (RF), and Stream Control Transmission Protocol (SCTP) to provide inter-device redundancy and high availability. The Figure 2-1 shows the system view of the ASN Gateway SR with relation to the IOS HA infrastructure.

Figure 2-1 Session Redundancy on the ASN Gateway



Subscriber Management

Subscriber information includes session and flows associated with a subscriber context, and is created, updated, or eventually deleted.

Subscriber information includes the following details:

- Authentication info (method, keying info, **etc**.)
- TID
- Addressing info (MS MAC, assigned DHCP address, **etc**.)
- VRF name
- Username
- Session info (signaling address, and associated timers, **etc**.
- Flow info per session (and associated QoS info per flow)

DHCP and AAA

The ASN Gateway supports DHCP relay mode and keeps track of client IP addresses allocated by DHCP servers (and the associated server IP addresses) so that it can relay future DHCP messages from clients to the servers. The client IP address and DHCP server IP address are saved in the subscriber context and are synced to the standby. Once the standby becomes active, it continues to relay DHCP messages from a client to the right server (there can be multiple servers configured: primary/secondary).

IOS AAA is not HA-aware at the moment, so the sync of AAA-related information is part of the session replication.

Bulk Synchronization

Bulk synchronization occurs after the standby is booted up. During this stage, the stateful data of all the established sessions/flows is transferred to the standby. Additionally, all the sessions/flows are recreated to the state that a session/flow is ready to switch user traffic without losing packets (or a very minimal loss) once switchover occurs.

This process can take some time if the number of sessions/flows is big. Sessions/flows are synched to the standby one by one. Once a session/flow is synched to the standby, it is considered bulk-sync complete and is moved to the dynamic queue. It is then ready for dynamic synching upon future events on this session/flow. During this process, sessions/flows continue to be created, modified, or deleted on the active. Thus bulk synching and dynamic synching co-exist until bulk-synching for all sessions/flows is complete. But dynamic synching for a session/flow will not start until its bulk synching is complete first.

Dynamic synching is given priority over bulk synching to maintain consistency and same state for a session/flow between active and standby. This also optimizes the bulk-sync process due to a session/flow state change. For example, a session is established when bulk-sync starts, but is deleted before bulk-sync is initiated for it. As a result, the bulk-sync for this session is not needed anymore as the bulk-sync proceeds.

Dynamic Synchronization

In order for the standby to take over processing from the active in case of a failure, information regarding all sessions and flows on the active are dynamically synchronized to the standby at well defined synchronization points. Separate TLVs are used to synchronize session, flow, and path related information. Dynamic syncing happens for new session/flow events after the standby is at hot-standby state, and after bulk-sync is complete.

The following list identifies current synchronization points:

- During initial network entry, session and flow information is synched to standby only after the Initial Service Flow (ISF) is created.
- After the ISF is up, each new flow created on the active is separately synched to the standby.
- Any updates to the TFT will cause the flow to be synched to the standby.
- Every time an address allocation happens, the flow will be synched to the standby.
- Any changes to the path on the active are synchronized to the standby
- During handoff, flow information is synchronized to the standby only after the handoff is complete. Cloned flows are not synched. New flows created on the active as a result of handoff are synchronized to standby by a FLOW UPDATE message that carries modified parameters as result of handoff.
- Flow synchronization after the transmission of an interim accounting request from the active. This causes FLOW UPDATE messages to be sent from active to standby, and the necessary message carries accounting counters that are sent to AAA as a part of interim accounting update.

Configuring Session Redundancy

The following configuration tasks are required before you can configure session redundancy:

- Configure HSRP on the interface.
- Configure redundancy inter-device
- Configure SCTP for RF Check pointing
- Configure Network Time Protocol (NTP) server
- Configure AAA on the active ASN Gateway and standby ASN Gateway

To configure session redundancy on the ASN Gateway, perform the following tasks:

	Command	Purpose

Step 1	`Router#interface FastEthernet0/1`
	`description BS-If`
	`ip address 9.11.44.147 255.255.255.0`
	`standby 100 ip 9.11.44.100`
	`standby 100 name CORE`
		Configures HSRP on the interface.

Step 2	`Router# redundancy inter-device`
	`scheme standby CORE`
		Enters inter-device configuration mode, which allows you to enable and protect Stateful Switchover (SSO) traffic.

Step 3	`Router#ipc zone default`
	`association 1`
	`no shutdown`
	`protocol sctp`
	`local-port 5000`
	`local-ip 9.11.44.147`
	`remote-port 5000`
	`remote-ip 9.11.44.159`
		Configures SCTP for RF Check pointing.

Step 4	`Router#config terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Router(config)#ntp server 129.237.32.2`
	`Router(config)#^Z`
		(Recommended) - The command **ntp server**, followed by the IP address or hostname of the NTP server, is used to configure your router to use an existing NTP server

Step 5	`Router(config)#ip radius source-interface Loopback` *`Loopback number`*
	and configure the loopback interface on your router as follows:
	`interface Loopback0`
	`ip address 192.168.0.250 255.255.255.255`
		Configuring **ip radius source-interface Loopback** on both ASN Gateways enables a AAA server to view two ASN Gateways as a single entity.

Step 6	`Router(config)#` **`wimax agw redundancy`**	Enables session redundancy on the ASN Gateway.
Step 7	`Router(config)#` **`subscriber redundancy rate 500 1`**	Specifies the sync rate for SR.

Configuration Example

This configuration is for AAA only.

On the Active ASN Gateway

```
--------------------------------------------------------------

!
interface Loopback192
```

```
 ip address 192.168.0.70 255.255.255.255
!
!
aaa group server radius car-sg
 server 1.8.70.99 auth-port 1812 acct-port 1813
!
aaa authentication dot1x car_auth_list group car-sg
aaa accounting network car_acct_list start-stop group car-sg
!
!
ip radius source-interface Loopback192
radius-server host 1.8.70.99 auth-port 1812 acct-port 1813
radius-server key r6AAA
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
!
```

On the Standby ASN Gateway

```
!
interface Loopback192
 ip address 192.168.0.70 255.255.255.255
!
!
aaa new-model
!
!
aaa group server radius car-sg
 server 1.8.70.99 auth-port 1812 acct-port 1813
!
aaa authentication dot1x car_auth_list group car-sg
aaa accounting network car_acct_list start-stop group car-sg
!
!
ip radius source-interface Loopback192
radius-server host 1.8.70.99 auth-port 1812 acct-port 1813
radius-server key r6AAA
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
```

Sample Configuration of ASN Gateway: Active

```
           interface GigabitEthernet0/0.70
              description to AAA/DHCP
 encapsulation dot1Q 70
 ip address 1.8.70.147 255.255.255.0
 standby 70 ip 1.8.70.70
 standby 70 follow P7_REDUNDANCY
```

Note Please reload the ASN Gateway if it suffers a time-zone change.

This configuration example includes information about DHCP:

```
interface Loopback102
    ip address 102.0.0.1 255.255.255.0
  !
   user-group domain eaptls.com2
   aaa accounting method-list AAA-ACC1
   aaa authentication method-list AAA-AUTHN1
   dhcp gateway address 102.0.0.1
   dhcp server primary 27.0.0.8
   service-flow pre-defined isf profile sf3
   service-flow pre-defined secondary 1 profile sf4
   vrf VRF_2
```

Authentication

A subscriber is authenticated using EAP on the active before the sessions/flows are recreated on the standby. The associated MSK, AK context and other credentials need to be transferred to the standby, along with the session stateful data. If geographic redundancy is deployed, this data must be protected. If the standby becomes active after a switchover, and if the same subscriber is re-authenticated on the new active, it follows the same authentication procedure as on the previous active.

Accounting

The accounting start, stop and interim update are only sent from the active. The standby never sends accounting records until it becomes active.

As part of the session/flow recreation on the standby, the IOS AAA database is populated with accounting records for each session/flow. For example, the “class” attribute and accounting session ID are synched from the active to the standby, and are saved to the related accounting record. This ensures that once the standby becomes active, it can send accounting records with the right info.

Synchronization of accounting counters is a function of the AAA interim accounting update feature. If the AAA interim accounting update feature is enabled, then the active ASN Gateway sends accounting records to AAA server. And the same event is used as a trigger to initiate a FLOW UPDATE event (which carries accounting counters the same as were sent to AAA server). Conversely, if this feature is disabled on the active, since there is not going to be an accounting update to AAA, there is an absence of triggers to send the accounting update synchronization message to standby. By itself, the ASN Gateway SR feature does not implement triggers to synchronize accounting counters.

The accounting session ID is a key attribute used in accounting events (start, stop, interim) and is used to collaborate records on the AAA server. It is a 4-byte unassigned integer, and is assigned uniquely within a ASNWG and increased sequentially until it rolls over. To ensure the new active can continue to generate unique accounting session IDs upon switchover, the new accounting session ID starts from the latest accounting session ID on the prior active.

Subscriber IP Address

Currently, the subscriber IP address is assigned by the DHCP server and a host route is inserted for it. When the standby recreates the subscriber session, the same host route is also inserted on the standby. The standby will not relay any DHCP messages between the DHCP client and the server until it becomes active.

QoS

For ASN Gateway Release 1.0, after a flow is created and the QoS parameters for the flow are sent to the BS, the ASN Gateway active synchronizes all the QoS parameters to the standby. Out of all of the parameters, the DSCP code for a flow synched to the standby is used to mark the packets once it becomes active.

Statistics and Counters

Statistics and counters are not synched to the standby. Instead, the standby rebuilds them as it processes stateful data from the active to create, modify, and delete sessions/flows. For example, the number of sessions/flows on the standby is updated as the standby processes session/flow creation and deletion. The number of received R6 messages on the standby is accumulated from the moment it becomes active and starts to receive R6 messages.

ASN Gateway Load Balancing

When a load balancer is running, it uses the loading information of all the ASN Gateways to select one of them, and forwards an incoming NetEntry message from the BS (with regard to a SS/MS) to the selected ASN Gateway.

When Dynamic Feedback Protocol (DFP) is configured, an active ASN Gateway periodically sends its loading information to the load balancer. A standby ASN Gateway does not send feedback and does not have accurate loading information because it does not process R6 messages and handle user traffic. Once a standby becomes active, it gradually builds accurate load as it processes R6 messages and handles user traffic. So there is an adjusting period before it can send back feedback about its current accurate load.

Data Path and GRE

The data path for a flow is recreated on the standby. The GRE keys for both the upstream and downstream of a flow are synched to the standby. Upon switchover, the new active ensures that any new GRE key allocated locally must not collide with any in-use GRE keys allocated by the previous active.

Version Control

Upgrading from the immediate lower software version to a higher version is supported. Downgrading of software version is not supported. For example, if a redundant pair of ASN Gateways runs on version A and the next immediate software version is version B, then upgrading from version A to B is supported (but not from B to A). This requires that the higher version understands the stateful data synched from a lower version.

Limitations

The following limitations exist in the Session Redundancy feature on the ASN Gateway:

- Synchronization of Accounting Counters

  This is configurable, and depends upon the AAA interim accounting update feature to be enabled. If the AAA interim accounting feature is disabled, then the default behavior of ASN Gateway SR is to not synchronize accounting data/payload counters. This may lead to under charging. For example, if a switchover occurs between two consecutive interim updates, the counts accumulated on the active after the previous interim update are lost, since the new interim update sends only the counts that are accumulated on the new active. Additionally, a STOP could be lost right before the switchover.

  Note Signaling counters are not synched.

Note For a standalone system, current AAA/Radius counters work accurately. However, when Session Redundancy is enabled, the flow (or session in terms of radius) age can be incorrect if relied upon the current counters. An additional attribute will now be sent from the ASN-GW called "session_elapsed_time" which will reflect the number of seconds since the particular flow started.

- Missing of a Session on the Standby

  Although SCTP provides reliable transport, the stateful data used to replicate a session can be lost due to congestion or max retrials. In this case, the session is not recreated on the standby. In case there is a switchover, this session is lost.

- Stale Session on the Standby

  For the same reason as above, if a stateful data for a session deletion is lost, then the session is not deleted from the standby while it's gone on the active.

  - If there is no switchover before the next session creation of the same subscriber, it's expected that the next synching of creation of a new session for the same subscriber will clean up the stale session.
  - If there is a switchover, then the stale session hangs until cleanup by manual intervention or by features like idle/session timeout.

- Mid-call Abort

  If a call setup is in progression but before reaching the first synching point and if there is a switchover, the call setup is aborted, and the subscriber has to retry the call.

Switchover

When switchover occurs, a trap is generated and sent to the NMS system to indicate that the active unit has failed, and the standby has taken over as active. The following behavior is expected:

- Any new GRE key allocated locally must not collide with any in-use GRE keys allocated by the previous active.
- Any new accounting session ID allocated locally must not collide with any in-use accounting session ID allocated by the previous active.
- DHCP relay for a new session is forwarded to a configured DHCP server.

- Some of the statistics will have a fresh start.
- DFP load is rebuilt and sent to the load balancer.

The following list identifies events which will cause a switchover:

- Router reload/crash because of reasons like software crash, CPU hogging, etc.
- HSRP tracks interfaces based on the configuration. On detecting interface flap <on-off transition> HSRP will enforce reload current active which will cause switchover of activity
- Manual intervention to switch activity from current active router to redundant hot standby. This can be accomplished using the following commands:
  - **redundancy switch-activity force**

    This command is used to switch activity from current active to current hot standby. Issuing the command causes the current router to reload, the current hot standby to become active, and when the current active router comes back up it assumes the role of hot standby.
  - **reload**

    This is normal router reload command that causes switchover. The current active router will reload, and the current hot standby will become active.

ASN Gateway Load Balancing

The purpose of load balancing is scalability of the ASN Gateway without distributing intelligence across base stations. This scalability is provided by load balancing across a set of ASN Gateways, while representing the cluster as a single ASN Gateway from the perspective of the BS. Thus, the base station will have a single point of contact. And any new ASN Gateway that is added to the system will not impact the base station provisioning.

Note Server Load Balancing and Session Redundancy are only available on Cisco 7600 SAMI platform. They are not available on the Cisco 7301 router platform.

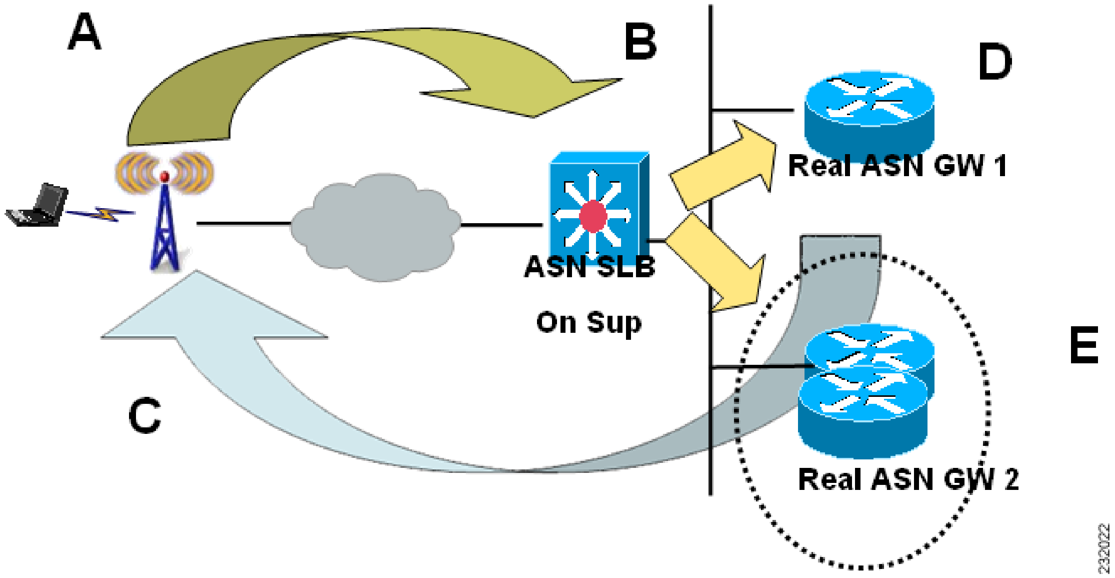
ASN Gateway Load Balancing is based on the IOS Server Load Balancing (SLB) feature. BSs are configured with the virtual IP address of the SLB as the ASN Gateway ID. The ASN Gateway selection flow for load balancing is illustrated below. Both dispatch mode and directed mode are supported. DFP is supported for the SLB to discover the load on the real ASN Gateways.

Note In Release 1.0, the SLB sticky feature and ASN Gateway handover call flows are not supported.

The session created on SLB, when the initial context request is processed, is maintained for a configurable time period to handle the re-transmission. During this period, if a re-transmission of context request is detected for a given MS/SS, SLB directs the re-transmission request to the same real ASN Gateway, that was selected for the first context request.

DFP is supported for the SLB to discover the load on the real ASN Gateways. Each real ASN Gateway has a limit on the number of maximum sessions it supports. Real ASN Gateway calculated load on itself is based on the existing number of sessions versus the maximum sessions that it can support, memory usage, and bandwidth usage and reports the load to SLB. SLB directs the initial context request to one of the real ASN Gateways based on either the round robin or least connections method. An ASN Gateway will not accept any more sessions if its load as calculated by DFP is 100%. Thus, this mechanism also supports CAC.

Figure 2-2 Server Load Balancing on the ASN Gateway



ASN Gateway Selection

- During Initial Network Entry phase, the BS sends the NetEntry MS Pre-Attachment Request corresponding to the SS/MSS to the ASN Gateway configured as the default.
- This ASN Gateway sends the NetEntry MS Pre-Attachment Response to the BS. The response may contain the IP address of an alternate Authenticator ID that can handle subsequent transactions corresponding to the SS/MSS. The BS, on receiving the NetEntry MS Pre-Attachment Response, sends the NetEntry MS State Change Ack to complete the transaction.
- All subsequent transactions corresponding to the SS/MSS occur between the BS and the ASN Gateway specified in the NetEntry MS Pre-Attachment Response Message.

Modes of Operation

There are two operation modes on the ASN Gateway:

- Dispatched Mode— In this mode packets are sent to the real server without any change to the original packet. A loopback is configured in the real server with an IP equal to virtual IP, and it replies back with virtual IP address as the source address.
- Directed Mode—The packet's destination IP address is rewritten to choose the ASN Gateway's IP address, and no loopback with the virtual ip address is configured on the ASN Gateway.

In both modes the selected ASN Gateway sends the pre-attachment response.

Configuring Load Balancing

This section lists configuration details regarding server load balancing. These configuration details are mainly for Directed Mode unless otherwise specified.

Load Balancing Configuration Task List

This section lists the tasks used to configure load balancing. Required and optional tasks

are indicated.

1. On the Cisco IOS SLB, complete the following tasks:
   a. Configuring a Server Farm and Real Server, (Required)
   b. Configuring a Virtual Server, (Required)
   c. Configuring DFP Support, (Optional, but recommended)
2. On the real ASN Gateway, complete the following tasks:
   a. Configuring a Loopback Interface for SLB, (Required if using dispatched mode)
   b. Configuring DFP Support on the ASN Gateway, (Optional, but recommended)

Configuring Cisco IOS SLB for Load Balancing

This section describes how to configure a Server Farm and a Real Server. To configure a Cisco IOS SLB server farm, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router-SLB(config)# **ip slb serverfarm** serverfarm-name Router(config-slb-sfarm)#	Adds a server farm definition to the Cisco IOS SLB configuration, and enters server farm configuration mode.
Step 2	Router-SLB(config-slb-sfarm)# **nat server**	Configures NAT server address translation mode on the server farm.
Step 3	Router-SLB(config-slb-sfarm)# **real** *ip-address* [*port*]	Identifies a real ASN Gateway as a member of a server farm, using the IP address of the ASN Gateway's virtual template interface, and enters real server configuration mode.
Step 4	Router-SLB(config-slb-real)# **weight** *weighting-value*	(Optional) Specifies the real server's workload capacity relative to other servers in the server farm. **Note** If you use DFP, the static weights you define using the **weight (server farm)** command are overridden by the weights calculated by DFP. If DFP is removed from the network, Cisco IOS SLB reverts to the static weights.
Step 5	Router-SLB(config-slb-real)# **in service**	Enables the real server for use by Cisco IOS SLB.

Sample Configuration

```
ip slb serverfarm ASNGW-SR-SF
       nat server
 probe PINGPROBE
         !
 real 11.11.11.50
   weight 0
          inservice
         !
        real 11.11.11.70
          weight 0
              inservice
```

Configuring Real ASN Gateway

Configuring the ASN Gateway for Load Balancing

To configure load balancing on the ASN Gateway, complete the tasks in the following sections:

- Configuring a Loopback Interface for SLB,
- Configuring the ASN Gateway as a DFP Agent, (Optional, but recommended)

Configuring a Loopback Interface for SLB

To enable load balancing, a loopback interface must be configured with the same IP address as thevirtual server on the Cisco IOS SLB on each ASN Gateway in a farm.

To create a loopback interface, use the following commands, beginning in global configuration mode:

	Command	Description
Step 1	`Router(config)#` **`interface loopback`** *`number`*	Creates a loopback interface. A loopback interface is a virtual interface that is always up
Step 2	`Router(config-if)# ip address ip-address mask`	Assigns an IP address to the loopback interface.

Configuring the ASN Gateway as a DFP Agent

To define the port number to be used by the DFP manager (the Cisco IOS SLB in this instance) to connect to the DFP agent; enter the following commands in order, beginning in global configuration mode:

	Command	Description
Step 1	`Router-ASNGW(config)# ip dfp agent agw`	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
Step 2	`Router- ASNGW(config-dfp)# port` *`port-number`*	Defines the port number to be used by the DFP manager to connect to the DFP agent.
Step 3	`Router- ASNGW(config-dfp)# inservice`	Enables the DFP agent for communication with a DFP manager. A DFP agent is inactive until both of the following conditions are met: • The DFP agent has been enabled using the inservice (DFP agent) command. • The client subsystem has changed the DFP agent

Sample Configuration

```
ip dfp agent agw
    port 5555
    inservice
```

To configure load balancing on the ASN Gateway, perform the following task:

	Command	Purpose
Step 1	`Router#` **`virtual`** *`x.y.z.m`* **`udp`** *`port no`* **`service asnr6`**	Enables load balancing on the ASN Gateway. The virtual server configuration commands are extended for ASN support.
Step 2	`Router#` **`idle asnr6 request`** *`timer value in seconds`*	Sets the idle timer request for the ASN Gateway.

ASN Gateway Configuration Example

Please note that following sample configuration applies only to SAMI platform.

SLB Related Configuration of Supervisor Card

```
7606-R6-sup720#show running-configuration | section slb
ip dfp agent slb
 port 5555
ip slb probe PINGPROBE ping
 interval 3
 faildetect 3
ip slb serverfarm ASNGW-SR-SF
 nat server
 probe PINGPROBE
 !
 real 11.11.11.50
  weight 0
  inservice
 !
 real 11.11.11.70
  weight 0
  inservice
ip slb vserver V-ASNGW-SR
 virtual 50.70.80.100 udp 2231 service asn r6
 serverfarm ASNGW-SR-SF
 idle asn r6 request 90
 inservice
ip slb dfp
 agent 11.11.11.50 5555 10 0 5
 agent 11.11.11.70 7777 10 0 5
7606-R6-sup720#
```

Sample configuration of real ASN Gateway for above configuration of Supervisor card.

```
asngw-real-s4p5# show running-configuration | section dfp
ip dfp agent agw
 port 5555
 inservice
asngw-real-s4p5#

asngw-real-s4p7#sh runn | section dfp
ip dfp agent agw
 port 7777
 inservice
asngw-real-s4p7#
```

Verifying the Configuration

To verify that load balancing is enabled on the ASN Gateway, perform the following tasks:

	Command	Purpose
Step 1	`Router# show ip slb session asnr6 [detail]`	Displays statistics related to load balancing R6 sessions.
Step 2	`Router# show ip slb vserver detail`	Displays vserver statistics in detail.

Configuration Example

Here is a sample configuration for SLB **show** commands on the ASN Gateway:

```
7606-R6-sup720#show ip slb sessions asn r6

vserver         MSID             Base Station     real             state
----------------------------------------------------------------------------
7606-R6-sup720#show ip slb sessions asn r6

vserver         MSID             Base Station     real             state
----------------------------------------------------------------------------
V-ASNGW-SR      0000AAAAC38ECCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC392CCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC396CCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC39ACCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC39ECCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
< S N I P P E D >

7606-R6-sup720#show ip slb vserver detail

V-ASNGW-SR, state = OPERATIONAL, v_index = 7, interface(s) = <any>
  virtual = 50.70.80.100/32:2231, UDP, service = ASNR6, advertise = TRUE
  server farm = ASNGW-SR-SF, delay = 10, idle = 3600
  asnr6: request idle = 90, Parse error pkt drops= 56,
         Number of reject responses = 0
  sticky: <none>
  sticky: group id = 0
  synguard counter = 0, synguard period = 0
  conns = 101, total conns = 509069, syns = 0,  syn drops = 0
  standby group = None
7606-R6-sup720#show ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
11.11.11.50           ASNGW-SR-SF      92      OPERATIONAL    83
11.11.11.70           ASNGW-SR-SF      92      OPERATIONAL    18
7606-R6-sup720#show ip slb serv
7606-R6-sup720#show ip slb serverfarms

server farm      predictor           nat   reals   bind id  interface(s)
--------------------------------------------------------------------------
ASNGW-SR-SF      ROUNDROBIN          S     2       0        <any>
7606-R6-sup720#show ip slb sessions asn r6 de
7606-R6-sup720#show ip slb sessions asn r6 detail

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC38ECCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
```

```
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC392CCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC396CCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC39ACCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC39ECCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50

< S N I P P E D >
7606-R6-sup720#
```

Configuring a Virtual Server

To configure a Cisco IOS SLB virtual server, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router-SLB(config)# **ip slb vserver** virtual_server-name	Identifies a virtual server, and enters virtual server configuration mode.
Step 2	Router-SLB(config-slb-vserver)# **virtual** *ip-addr* [*netmask* [**group**]] {**esp** | **gre** | *protocol*} or Router(config-slb-vserver)# **virtual** *ip-addr* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]	Specifies the virtual server IP address, type of connection, and optional TCP or UDP port number, Internet Key Exchange (IKE) Internet Security Association and Key Management Protocol (ISAKMP) or Wireless Session Protocol (WSP) setting, and service coupling.

Step 3	Router-SLB(config-slb-vserver)# **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id* **priority** *priority*]	Associates a real server farm with a virtual server. • **backup—**(Optional) Configures a backup server farm • **backup** *backup-farm* [**sticky**]—(Optional) Configures a backup server farm and optionally specifies that sticky connections are to be used in the backup server farm. • **map** *map-id* **priority** *priority—*(Optional) Associates an IOS SLB protocol map to a server farm and defines the priority for that map. Maps are searched based on priority. The lower the number, the higher the priority. **Note** Multiple instances of the **serverfarm** command are allowed if configured with the **map** keyword option. The default server farm (without the **map** keyword option) is limited to a single instance. **Note** To change map configurations the virtual server must be taken out of service. **Note** The NAT modes on the primary and backup server farms for each map must match.
Step 4	Router-SLB(config-slb-vserver)# **idle** [**request**] *duration*	(Optional) Specifies the minimum amount of time that Cisco IOS SLB maintains connection context in the absence of packet activity.
Step 5	Router-SLB(config-slb-vserver)# **inservice**	Enables the virtual server for use by Cisco IOS SLB.

Sample Configuration

```
Router-SLB(config)# ip slb vserver V-ASNGW-SR
Router-SLB(config-slb-vserver)# virtual 50.70.80.100 udp 2231 service asn r6
Router-SLB(config-slb-vserver)#serverfarm ASNGW-SR-SF
Router-SLB(config-slb-vserver)# idle asn r6 request 90
Router-SLB(config-slb-vserver)#inservice
```

Configuring DFP Support

You can define Cisco IOS SLB as a DFP manager, as a DFP agent for another DFP manager (such as DistributedDirector), or as both at the same time. Depending on your network configuration, you might enter the commands for configuring Cisco IOS SLB as a DFP manager and the commands for configuring Cisco IOS SLB as a DFP agent on the same device or on different devices.

To configure Cisco IOS SLB as a DFP manager, and to identify a DFP agent with which Cisco IOS SLB can initiate connections, use the following commands, beginning in global configuration mode:

	Command	Description
Step 1	`Router-SLB(config)#` **`ip slb dfp`** `[`**`password`** `[`**`0`**`|`**`7`**`]` *`password`* `[`*`timeout`*`]]`	Configures DFP, supplies an optional password, and enters DFP configuration mode.
Step 2	`Router-SLB(config-slb-dfp)#` **`agent`** *`ip_address port-number`* `[`*`timeout`* `[`*`retry_count`* `[`*`retry_interval`*`]]]`	Identifies a DFP agent to which Cisco IOS SLB can connect.

Sample Configuration

```
Router-SLB(config) # ip slb dfp
Router-SLB(config-slb-dfp)# agent 11.11.11.50 5555 10 0 5
Router-SLB(config-slb-dfp)# agent 11.11.11.70 7777 10 0 5
```

Configuring the ASN Gateway

This section describes various other configuration tasks that you need to perform to make the ASN Gateway function properly. It includes the following topics:

- Configuring SNMP on the ASN Gateway
- MIB Support

Configuring SNMP on the ASN Gateway

This section provides information on how to configure Simple Network Management Protocol (SNMP) on the ASN Gateway. It contains the following configuration tasks:

- Configuring SNMP Access in Routers
- Configuring SNMP-Server Host
- Configuring SNMP-Server Trap-Source
- Configuring SNMP Traps

Configuring SNMP Access in Routers

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), perform the following tasks:

	Command	Purpose
Step 1	ASNGW(config)# **snmp-server community string [view** *view-name*] **[ro | rw] [ipv6** *nacl*] [*access-list-number*]	Sets up the community access string to permit access to the Simple Network Management Protocol (SNMP). To remove the specified community string, use the **no** form of the command.
	string	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.
	view	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
	view-name	(Optional) Name of a previously defined view.
	ro	(Optional) Specifies read-only access. Authorized management stations can only retrieve MIB objects.
	rw	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
	ipv6	(Optional) Specifies a IPv6 named access list. (Optional) IPv6 named access list.
	nacl	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent.
	access-list-number	Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

Configuring SNMP-Server Host

To specify the recipient of an Simple Network Management Protocol notification operation, perform the following tasks:

	Command	Purpose
Step 1	`ASNGW(config)# snmp-server host host-addr [traps	informs] [version {1	2c	3 [auth	noauth	priv]}] community-string [udp-port port] [notification-type]`	Specifies the recipient of an Simple Network Management Protocol notification operation. To remove the specified host, use the **no** form of this command.

This command is disabled by default. No notifications are sent. If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

host-addr	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the **version** keyword, one of the following must be specified: **1 —**SNMPv1. This option is not available with informs. **2c** —SNMPv2C. **3** —SNMPv3. The following three optional keywords can follow the version 3 keyword: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	UDP port of the host to use. The default is 162.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: • **bgp—**Sends Border Gateway Protocol (BGP) state change notifications. • **config—**Sends configuration notifications. • **dspu—**Sends downstream physical unit (DSPU) notifications. • **entity—**Sends Entity MIB modification notifications. • **envmon—**Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • **frame-relay—**Sends Frame Relay notifications. • **hsrp—**Sends Hot Standby Routing Protocol (HSRP) notifications. • isdn—Sends Integrated Services Digital Network (ISDN) notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • **repeater—**Sends standard repeater (hub) notifications. • rsrb—Sends remote source-route bridging (RSRB) notifications. • **rsvp—**Sends Resource Reservation Protocol (RSVP) notifications. • **rtr—**Sends SA Agent (RTR) notifications. • **sdlc—**Sends Synchronous Data Link Control (SDLC) notifications. • sdllc—Sends SDLLC notifications. • **snmp—**Sends Simple Network Management Protocol (SNMP) notifications (as defined in RFC 1157). • **stun—**Sends serial tunnel (STUN) notifications. • **syslog—**Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. • **tty—**Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • **x25—**Sends X.25 event notifications.

Configuring SNMP-Server Trap-Source

To specify the interface (and hence the corresponding IP address) that an Simple Network Management Protocol trap should originate from, perform the following task:

	Command	Purpose
Step 1	`ASNGW(config)#` **`snmp-server trap-source`** *`interface`*	Specifies the interface (and hence the corresponding IP address) that an Simple Network Management Protocol trap should originate from. Use the no form of the command to remove the source designation. The default setting is that no interface is specified.
	`interface`	Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax.

Configuring SNMP Traps

To enable the router to send Simple Network Management Protocol traps or informs (SNMP notifications), perform the following task:

	Command	Purpose
Step 1	`ASNGW(config)#` **`snmp-server enable traps`** `[`*`notification-type`*`] [`*`notification-option`*`]`	Enables the router to send Simple Network Management Protocol traps or informs (SNMP notifications). The **no** form of this command disables SNMP notifications. This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command. If you enter this command with no *notification-type* keywords, the default is to enable all notification types controlled by this command (Exception: ATM PVC notifications are not enabled unless the atm pvc keywords are used.)

notification- type	(Optional) Type of notification to enable. If no type is specified, all notifications available on your device are sent. The notification type can be one of the following keywords: • **atm pvc—**Enables ATM permanent virtual circuit (PVC) notifications. When the **atm pvc** keywords are used, you can specify additional *notifcation-option* values (see below). The ATM PVC failure notifictiaon is defined as "enterprise 1.3.6.1.4.1.9.10.29.2.1; 1 atmIntfPvcFailuresTrap" in the CISCO-IETF-ATM2-PVCTRAP-MIB. ATM PVC failure notifications are sent when a PVC on an ATM interface fails or leaves the UP operational state. Only one trap is generated per hardware interface, within the specified interval defined by the interval keyword (stored as the atmIntfPvcNotificationInterval in the MIB). If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the fail-interval has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN. No notifications are generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router. • **bgp—**Enables Border Gateway Protocol (BGP) state change notifications. • **config—**Enables configuration notifications. • **entity—**Enables Entity MIB modification notifications. • envmon—Enables Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the **envmon** keyword is used, you can specify a *notification-option* value. • **frame-relay—**Enables Frame Relay notifications. • **hsrp—**Enables Hot Standby Routing Protocol (HSRP) notifications. • isdn—Enables Integrated Services Digital Network (ISDN) notifications. When the **isdn** keyword is used, you can specify a *notification-option* value. • repeater—Enables Ethernet hub repeater notifications. When the **repeater** keyword is selected, you can specify a *notification-option* value. • **rsvp—**Enables Resource Reservation Protocol (RSVP) notifications. • **rtr—**Enables Service Assurance Agent / Response Time Reporter (RTR) notifications.

notification- type	• **snmp [authentication]—**Enables RFC 1157 SNMP notifications. Note that use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command will globally enable (or, if using the **no** form, disable) the following SNMP traps: – authentication Failure – linkUp – linkDown – coldstart (This behavior is corrected in Cisco IOS Release 12.1(3)T and 12.0(20)S.) • **syslog—**Enables error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
notification- option	(Optional) • **atm pvc [interval** *seconds*] [**fail-interval** *seconds*]— The optional **interval** *seconds* keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30. —The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0. • **envmon** [**voltage | shutdown | supply | fan | temperature**]—When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**. • **isdn** [**call-information | isdn u-interface**]—When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdnu-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem. • **repeater** [**health | reset**] —When the **repeater** keyword is used, you can specify the repeater option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords: • **health—**Enables IETF Repeater Hub MIB (RFC 1516) health notification. • **reset—**Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

Configuration Examples

The following example enables the router to send all traps to the host specified by the name “myhost.cisco.com”, using the community string defined as “public”:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host “myhost.cisco.com” using the community string “public”:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
snmp-server enable traps bgp
snmp-server host bob public isdn

ASNGW(config)# [no] logging snmp-authfail
```

Note Using the **logging snmp-authfail** command enables all SNMP authentication failure logging messages. The **no** version of this command will disable the logging of authentication failure messages.

Note If you do not use the SNMP management tools of the router to monitor PPP sessions, you can prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory by using the no virtual-template snmp command. For example:
ASNGW(config)# [**no**] **virtual-template snmp**

SNMP Configuration Examples on the ASN Gateway

Logging

```
=========

!
logging snmp-authfail
logging queue-limit 100
logging buffered 1000000
enable password lab
!
```

Virtual Template

```
=============

!
no virtual-template snmp
!
```

SNMP Traps

```
==========

snmp-server community private RW
snmp-server trap-source GigabitEthernet0/2
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps cnpd
snmp-server enable traps pw vc
snmp-server enable traps syslog
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds3
snmp-server enable traps atm subif
snmp-server enable traps channel
snmp-server enable traps ima
snmp-server enable traps srp
snmp-server enable traps flash insertion removal
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps envmon
snmp-server enable traps aaa_server
snmp-server enable traps agw
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps dlsw
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps ipmobile
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps event-manager
```

```
snmp-server enable traps alarms informational
snmp-server host 171.71.129.34 public
```

MIB Support

The ASN Gateway supports a Management Information Base (MIB) that describes objects that enable users and network management to remotely monitor the ASN Gateway using SNMP commands. The ASN Gateway supports two separate MIBs:

One contains global system information and parameters, base-station information, subscriber, flow, traffic and trap notification information.

The second contains information about the R6 signaling protocol information used between the base-station and the ASN Gateway. This includes overall gateway R6 information, and information per base-station.

The ASNGateway MIB variables are not synchronized across a fail-over. Many MIB variables can be recreated on the standby from the synchronized state data. The NMS attempts to handle such a situation, and any inconsistencies in MIB data that result from this approach. The existing RF/CF MIB is also available.

Note The R6 MIB is not supported in the initial release of the ASN Gateway on the Cisco 7301 router platform.

Verifying MIB Support

To display various MIB parameters, perform the following tasks:

	Command	Purpose
Step 1	router# **show wimax agw**	Displays various system parameters, including ASN Gateway software version, number of base stations allowed, number of subscribers allowed, and others.
Step 2	router# **show wimax agw stat internal**	Displays ASN Gateway internal statistics.
Step 3	router# **show wimax agw stat dhcp**	Displays ASN Gateway DHCP statistics.
Step 4	router# **show wimax agw stat**	Displays ASN Gateway statistics.
Step 5	router# **show wimax agw user-group**	Displays ASN Gateway user group statistics.
Step 6	router# s**how wimax agw path**	Displays ASN Gateway path statistics.

Configuration Examples

Here is sample output for the **show wimax agw** command:

```
router# show wimax agw
Access network gateway version 0.1, service is enabled

 AGW listening on UDP control port 2231
 Maximum Number of base station 500 allowed
 Maximum Number of subscriber 20000 allowed
  Number of signalling paths created 0
  Number of brearer paths created 0
  Number of subscribers connected 0
  Number of sessions created 0
  Number of flows created 0
  Traffic Sent 0 packets, 0 bytes
  Traffic Rcvd 0 packets, 0 bytes
```

Here is samle output for the **showwimax 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 Recevied 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 Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


router#show wimax agw user-group name cisco brief ?
  |  Output modifiers
  <cr>

router#show wimax agw user-group name cisco brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
cisco 0         0         0         0         0


router#show wimax agw user-group unauthenticated ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group unauthenticated

User group domain name unauthenticated
--------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes

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
```

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

```
router# show wimax agw statistics
AGW Statistics
Message function type Undefined(0/0x0)

Message function type Data Path(3/0x3)
  Message type Deregistration Request(4/0x4)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Deregistration Response(5/0x5)
   Number of messages sent 0
   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 0
   Number of messages resent 0
  Message type Registration Request(12/0xC)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Registration Response(13/0xD)
   Number of messages sent 0
   Number of messages received 0
…
```

Here is sample output for the **show wimax agw statistics dhcp-relay** command:

```
router# show wimax agw statistics dhcp-relay
AGW DHCP Statisitics
   Tx to DHCP server Discover 0, Request 0
   Tx to DHCP server Release 0, Decline 0
   Tx to DHCP server Inform 0
   Rx from DHCP server Offer 0, Ack 0
   Rx from DHCP server Nak 0, Unknown 0
```

This output gives the statistics of DHCP messages that are relayed through the ASN Gateway. If the ASN GW happened to initiate any DHCP messages, these counters are not incremented.

Here is sample output for the **show wimax agw statistics internal** command:

```
Router# show wim agw statistics internal
Last clearing of "show wimax agw statistics internal" counters never
 Signalling plane related statistics
    Signal packets dropped service not ready 0

 Configuration related statistics
  Service flow profile not found 0
  QoS profile not found 0
  Classifier profile not found 0
 Handoff related statistics
  Total handoffs succeeded 0
  Total handoff failed 0
  Total cmac key update succeeded 0
  Total cmac key update failed 0
  Total security key exchange succeeded 0
  Total security key exchange failed 0

Router#
```

Features Not Supported

The following features are not supported in this release:

- The R6 MIB is not supported in the initial release of the ASN Gateway on the Cisco 7301 router platform.
- Configuration synchronization: ASN Gateway relies on manual configurations to ensure identical feature configuration on the active and standby.
- In-Service-Software-Upgrade (ISSU): Upgrading from the immediate lower software version to a higher version is supported.

Data Plane

The data plane is started after successful completion of the EAP authentication phase. GRE tunnel exists between the BS and ASN Gateway, and a unique GRE key is used for the data path corresponding to each service flow. There is a GRE key allocated in each direction.

The following data plane features are supported on the ASN Gateway:

GRE Keying

A GRE key is allocated per service flow in each direction. The GRE keys are exchanged using the RR-Request used to create the Data Path bearer. The GRE keys that correspond to the ASN Gateway are allocated by the ASN Gateway and sent to the BS during creation of the service flow using the RR-Request. Similarly, the GRE key values corresponding to the BS are allocated by the BS and sent to the ASN Gateway using the RR-Response message.

During Inter-BS mobility, new keys are allocated by the Base-station. The ASN Gateway keeps the same GRE keys.

The ASN Gateway allocates the GRE keys such that the values are not assigned immediately upon release.

VRF Support

A user-group can be configured with virtual route forwarding (VRF) support. This allows you to create an internal VRF entity to connect all traffic to/from the specific user-group.

Restrictions

The following restriction apply in Cisco ASN Gateway Release 1.0:

- To avoid issues with high CPU usage, we recommend the following configurations:
  - To reduce the CPU usage during bootup, disable logging to the console terminal by configuring the **no logging console** global configuration command.
  - To ensure that the HSRP interface does not declare itself active until it is ready to process a peers Hello packets, configure the delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100 interface** configuration command under the HRSP interface.
  - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), disable the notification of interface data link status changes on all virtual template interfaces of the ASN Gateway using the **no logging event link-status** interface configuration command.

```
!
interface Virtual-Template1
description ASNGW-VT
ip unnumbered Loopback0
encapsulation agw
no logging event link-status
access-point-list wimax
end
```