CHAPTER 3

Proxy Mobile IP

This chapter explains and discusses the Proxy Mobile IP feature for the Cisco Broadband Wireless Gateway (BWG). Additionally, this chapter explains how to configure those features and provides sample configurations when appropriate.

Overview

Previous BWG releases implemented the basic functionality of ASN anchored mobility. ASN-anchored mobility occurs when the MS moves between Data Path Functions while maintaining the same anchor FA (BWG) sitting at the northbound edge of the ASN network. The data flow between the CSN and Data Path Functions pivots at the anchor FA/BWG. The CSN is unaware of any mobility that occurs between the ASN Data Plane Functions. A typical example for ASN anchored mobility is inter-BS handover controlled by the same BWG.

CSN anchored mobility mainly addresses the macro-mobility between the ASN and CSN across the R3 reference point. Specifically, in the case of mobile IPv4, this implies re-anchoring the current FA to a new FA, and the consequent binding updates (or MIP re-registration) to update the upstream and downstream data forwarding paths.

BWG Release 2.0 introduces the Proxy Mobile IP (PMIP) feature. In PMIP, the MIP client is implemented in the BWG instead of being in the MS.

The fundamental function for the BWG (PMIP client) is to generate a Mobile IP Registration Request (RRQ) on behalf of the user, send it to the HA and establish the tunnel between FA and HA. In order to accomplish this task, the PMIP client needs to collect the related MIP attributes through an EAP authentication (or Cisco invented AAA access for unauthenticated users) mechanism. The AAA server returns to the BWG with a set of standard Mobility Service attributes. With this info, BWG/PMIP client initiates a MIP RRQ to HA. The HA sends back a Registration Reply (RRP), which contains an assigned IP address (HoA - Home Address) for the MS, back to the PMIP client. As a result of the MIP RRQ/RRP operation, the PMIP client interacts with FA to establish a data path with reversing tunneling capability between FA and HA.

If the MIP registration is successful, BWG further notifies the MS the assigned IP address through the DHCP or ARP mechanism.

The BWG PMIP feature has the following functionality:

- A simplified DHCP proxy server
- Support for Multiple Home Agents (HAs)
- IP-in-IP and GRE tunneling between BWG/FA and HA
- PMIP client to inter-work with different address allocation mechanisms (DHCP, AAA)
- MIP Revocation from HA

- FA Relocation (Network re-entry)
- A hybrid (co-existence) approach of PMIP and simple IP for multiple hosts behind MS
- Support of Radius Attributes (IPv4 PMIP related) for Mobility Service (PMIP IPv4) as specified in WiMAX NWG 1.2.2
- PMIP support for L3-L3 (IPCS) and L2-L3 (Ethernet CS)
- Stateful redundancy for PMIP client/FA

DHCP Proxy Server

With MIP, the client's IP address assignment is from the HA instead of a DHCP server. This requires the BWG to terminate (instead of relay) the DHCP protocol. The following DHCP messages and their options are supported:

DHCP Discover

- 53: DHCP Message Type
- 57: Maximum DHCP Message Size
- 61: Client Identifier
- 50: Requested IP Address
- 12: Host name
- 55: Parameter Request List (Subnet Mask, DNS, DN)

DHCP Offer

- 53: DHCP Message Type
- 54: Server Identifier
- 51: IP Address Lease Time
- 1: Subnet Mask (goes before Router option)
- 3: Router
- 6: DNS
- 12: Hostname

DHCP Request:

- 53: DHCP Message Type
- 57: Maximum DHCP Message Size
- 61: Client Identifier
- 54: Server Identifier
- 50: Requested IP Address
- 51: IP Address Lease Time
- 12: Host name
- 55: Parameter Request List (Subnet Mask, DNS, DN)

DHCP Ack

- 53: DHCP Message Type
- 54: Server Identifier
- 51: IP Address Lease Time
- 1: Subnet Mask
- 12: Hostname

DHCP Release

- 53: DHCP Message Type
- 61: Client Identifier
- 54: Server Identifier

DHCP Decline

- 53: DHCP Message Type
- 61: Client Identifier
- 54: Server Identifier

DHCP NAK

- 53: DHCP Message Type
- 61: Client Identifier
- 54: Server Identifier

Proxy DHCP Server Interacts with PMIP

In BWG Release 2.0, only DHCP Proxy is supported. The following data flow shows the interactions between the DHCP Proxy server and the PMIP client.

1. When an MS enters into the network, the BS and BWG exchange info for the Pre-Attachment Req/Rsp/Ack procedure. The MS/BS can indicate whether Authorization is required.
2. If authorization is required, the BWG initiates the Identity Request procedure.
3. The BWG sends a AAA Access Request.
4. The AAA and the MS start the EAP exchange, if required.
5. The BWG and BS finish the Attachment Procedure.
6. AAA Access Accept is received in the BWG. The message may include the following WiMAX attributes: hHA-IP-MIP4, vHA-IP-MIP4, MN-hHA-MIP4-KEY, MN-vHA-MIP4-KEY, MN-HA-MIP4-SPI, HA-RK-KEY, HA-RK-SPI, and HA-RK-Lifetime. Home attributes are preferred over the visiting ones.
7. If MSK is received, the BWG further derives AK context from MSK and distributes into BS, where the keys are further exchanged with MS through PKMv2. FA-HA AE derivation is based on NWG stage 3, choosing the correct SPI.
8. The BWG starts the DHCP/PMIP protocol state machine, and formulates a MIP RRQ towards the HA. The information for the RRQ message comes from the AAA server and/or the user group configuration, and includes the following information:
   - Flags: user group configuration or default value
   - Lifetime: session timeout from AAA or user-group configuration

  - HoA: from AAA's Framed IP address or zero
  - Home Agent: from AAA or user group configuration
  - Care-of Address: Interface configuration on BWG
  - NAI extension included
  - Revocation Support extension (I-bit = 0)
  - Host-Config. extension if configured in the user group
  - MN-HA AE
  - GRE-key extension (not in this release)
  - FA-HA AE

  The virtual access IDB for reverse tunneling for the HA should also be created if it has not been created.

9. The HA interacts with AAA to obtain the MIP keys.
10. The HA validates the MN-HA AE and FA-HA AE with MIP keys from AAA.
11. On successful authentication at the HA, the HA uses it address scheme (local pool, DHCP, AAA, etc.) and assigns a home address for this mobile user. This address is included in the Registration Reply (RRP) message to the BWG. The BWG checks the Identification field and calculates the Mobile-Home Authentication Extension for integrity check. Foreign-Home Authentication Extension is also validated if present. If all validation is successful, a reverse-tunnel is created between the BWG and HA to transport user data.
12. The BWG and BS set up GRE data path. Note that this step should go in parallel with the MIP RRQ/RRP.
13. The MS/Host tries to acquire an IP address by initiating a DHCP DISCOVER.
14. The BWG sends DHCP OFFER to MS/Host.
15. The MS/Host further sends DHCP REQUEST.
16. The BWG sends back DHCP Ack.

Note This procedure deviates slightly from the NWG specification, where the MIP RRQ is triggered by the DHCP Discover message. As long as the MIP RRQ message does not need any info from DHCP Discover, this scenario should operate correctly.

PMIP Authenticated Network Identifier (PANI)

From BWG Release 2.2, BWG supports PMIP Authenticated Network Identifier (PANI). Details of a PANI may be received from a AAA server as part of the Access Accept message. If details of PANI is received, then BWG will use PANI as the Network Access Identifier (NAI) while generating the RRQ to a Home Agent (HA).

The following table provides the AAA-Authentication Attributes for PANI:

Table 3-1 AAA-Authentication Attributes for PANI

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
PMIP Authenticated Network Identifier	26/78	Authenticated identity of the MS as returned by AAA.	0	0	0-1	0

Multiple HA Support

The BWG is designed to communicate with multiple HAs. For each MS, the AAA can provide an HA IP address, or if not available, an IP address from the user-group configuration.

Here is a sample configuration:

```
router(config)#wimax agw pmip profile verizon
       home-agent
          address <home-agent-ip>

router(config)#wimax agw user group-list wimax
 user-group cisco.com
  aaa accounting method-list agw
  sla profile-name silver
    pmip profile-name verizon
 !
```

Only one HA can be configured per user group.

Tunneling Between FA (BWG) and HA

From BWG Release 2.0, both IP-in-IP and GRE tunneling (without GRE key) are supported. IP-in-IP tunneling is the default method (G bit not set in RRQ). If GRE tunneling is desired (with G bit set in RRQ), it can be configured on per user-group basis.

Here is the configuration example:

```
wimax agw pmip profile verizon
       proxy-mn
          gre-tunneling-enable

wimax agw user group-list wimax
 user-group cisco.com
  aaa accounting method-list agw
  sla profile-name silver
    pmip profile-name verizon
```

MIP Host Configuration Extension

The MIP Host Configuration Extension is described in RFC 4332. The default is enabled. It can be disabled explicitly with **no host-config-ext-request** command under the proxy-mn section.

The following parameters from the HA can be passed as DHCP options to the client:

- MIP home network prefix length => DHCP subnet mask (1)
- MIP default gateway => DHCP router (3)
- MIP DNS server => DHCP DNS (6)

To enable this feature, perform the following tasks:

	Command	Purpose

Step 1	`router(config)# wimax agw pmip profile verizon`
	`proxy-mn`
	`host-config-ext-request // RFC 4332`
		Enables Proxy Mobile IP profile on the BWG.

Step 2	`router(config)# wimax agw user group-list wimax`
	`user-group cisco.com`
	`aaa accounting method-list agw`
	`sla profile-name silver`
	`pmip profile-name verizon`
		Configures the User group list on the BWG

Configuring DNS and Default Gateway

BWG allows you to configure the DNS and Default Gateway locally or download from a AAA server.

If the Home Agent does not support RFC4332 (Host Configuration Extensions), you can configure the DNS and Default Gateway in BWG through CLI or configure BWG to download DNS and Default Gateway details from a AAA server. The DNS and Default Gateway details are sent to the CPE as part of the DHCP proxy response.

The order of precedence is:

1. DNS and Default Gateway details received as part of RRP from the HomeAgent.
2. DNS and Default Gateway details received from AAA to the BWG.
3. DNS and Default Gateway configured locally in the BWG.

Use the following commands to configure DNS and Default Gateway:

- [no] dns-server primary <ip address> secondary <ip address>
- [no] default-gateway <ip_address>

The following is an example of the DNS and Default Gateway configuration:

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

Table 3-2 AAA-Authentication Attributes for DNS and Default Gateway configuration

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
Default Gateway	Cisco AVP	The IPv4 address of the default Gateway.	0	0	1	0
DNS	26/52	The IPv4 address of the DNS server.	0	0	1-n	0

Client IP Address Allocation

PMIP supports both dynamic and static IP address allocation mechanisms. For a static IP address, the BWG learns the pre-configured IP address in the Mobile Station through ARP. In this case, the BWG authorizes the IP address by verifying that it is in the IP address pool range downloaded from the AAA server. Another static IP address method is based on the BWG obtaining the IP address from the AAA server and leasing it to the MS through DHCP. In both scenarios, the BWG provides the IP address in the MIP registration to the HA, and allows the MS to use the IP address when HA accepts the registration. For dynamic IP address, the BWG does not provide an IP address in the MIP registration and the HA assigns an IP address to the MS/Host based on its own address allocation scheme (AAA, DHCP, local pool, etc.) in the registration reply.

If the BWG has already obtained the IP address before invoking the MIP operation through the means such as from DHCP relay mechanism or from AAA through Framed IP address. In all these cases, the BWG will treat them as if a static IP scenario, i.e., the MIP RRQ will carry the assigned IP to HA as HoA.

MIP Registration Revocation from HA

A MIP revocation from HA is supported. After security associations are verified in the RRP message, the subscriber session is torn down.

Co-Existence of PMIP and Simple IP Hosts

Due to the protocol limitations, a MIP subscriber can only get one IP address. This is a sharp contrast to the current BWG capability of multi-hosts behind a MS. When this happens, only the subscriber's (default) host is assigned the MIP HoA. The rest of hosts will continue to work as a simple IP hosts as if no PMIP has ever existed for the subscriber.

FA Relocation

FA relocation can be triggered when an MS re-enters the network through a different FA/BWG. When this occurs, the PMIP client in the new BWG initiates an RRQ as usual, and the HA revokes the MS’s registration from the old FA/BWG.

The following flow illustrates how FA relocation works:

1. An active session is established between the MS, BS-1, BWG-1 and HA.
2. The MS moves to BS-2, where a network re-entry is needed.
3. As part of network re-entry, the BGW-2 initiates MIP RRQ toward the HA.
4. The HA detects a binding already exists for the MS, so it revokes the MS's old MIP registration.
5. BWG-1 starts to clean up its session for the MS, if it still exists.

6. BWG-1 replies the MIP revocation.
7. MIP RRP with the same HoA to the BGW-2.
8. The MS sends DHCP Discover.
9. BWG-2 offers the HoA as the MS's IP address.
10. The MS sends DHCP Request.
11. The BWG sends back DHCP Ack to confirm the IP address assigned.

Due to mobile IP, the subscriber host will always be assigned to the same IP address by the same HA during macro-mobility. However, the multiple simple IP hosts behind the MS may not be assigned to the same IP address during the macro-mobility. This is determined by the arrangement between the two service providers involved. If the BWG-1 and BWG-2 shares the same DHCP server, the DHCP server may have a mechanism to ensure the same IP address for the simple hosts after the macro-mobility event. On the other hand, if the BWG-1 and BWG-2 uses different DHCP servers, the IP address for the simple IP host can not be ensured to be the same after the macro-mobility event.

Note R4-based FA relocation in idle mode is not supported in this release.

Ethernet CS L2-L3 or IPCS

MIP protocol dictates that the packet tunneled between HA and FA must be an IP packet. In BWG case, either Ethernet CS L2-L3 or IPCS will result in layer 3 IP packets towards CSN (HA). Hence BWG's PMIP support is designed to work with both Ethernet CS L2-L3 and IPCS.

On the other hand, when Ethernet CS L2-L2 bridging is enabled for a user group, the PMIP feature will be automatically disabled for those users. In other words, L2 bridging takes a higher priority than the PMIP feature.

WiMAX RADIUS Attributes

WiMAX Forum NWG 1.2.2 standard attributes will be supported. The following table provides details of the supported WiMAX RADIUS attributes.

Table 3-3 WiMAX RADIUS Attributes

Attribute	Description
hHA-IP-MIP4 (26/6)	HomeAgent Address.
MN-hHA-MIP4-KEY (26/10)	Attribute used to create the Mobile Node—HomeAgent authentication Extension.
MN-HA-MIP4-SPI (26/11)	The SPI associated with MN-HA-MIP4 key.
Session-Timeout	The session timeout (32 bits) is converted to registration lifetime (16 bits) with maximum value of 65534 in time unit of seconds.
Framed-IP address	If present, this attribute is used as HoA in the MIP RRQ.

Table 3-3 WiMAX RADIUS Attributes

Attribute	Description
HA-RK-KEY (26/15)	The key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. This key is used by the NAS to generate BWG-HA keys.
HA-RK-SPI (26/16)	The SPI used for the HA-RK.
HA-RK-Lifetime (26/17)	The lifetime of the HA-RK and derived keys. Value is between 0 and 65535.

Stateful Session Redundancy

Since the PMIP client/FA does not have its own scheme to perform session redundancy. Its stateful data will be synced as part of BWG's session data. The goal is that when a switchover occurs, the newly active BWG is able to continue the session with a minimal packet loss.

The **ip mobile foreign-agent redundancy** CLI needs to be enabled so that the PMIP stateful session information is synced along with the BWG session data.

PMIP Profile Configuration

In addition to HA address and GRE tunneling, the following is an example for other parameters:

```
router(config)#wimax agw pmip profile verizon
       home-agent
          address <home-agent-ip>
          ha-rk-key <key> spi <spi> lifetime <value>
       proxy-mn
          gre-tunneling-enable
          host-config-ext-request       // RFC 4332
          mn-ha-key <key> spi <spi>
          coa <ip_address>
        local-timezone <tz>
```

Each user group can optionally link to the PMIP profile configured:

```
router(config)#wimax agw user group-list wimax
 user-group cisco.com
  aaa accounting method-list agw
  sla profile-name silver
    pmip profile-name verizon !
```

Note The IP mobile configuration is optional. As long as AAA server has enough per-subscriber provisioning info, the PMIP function can be performed for the subscriber. All (except for gre-tunneling-enable) the user-group configuration serves as default when the corresponding configuration from AAA for a subscriber is not available.

On the BWG side, some basic Mobile IP configuration is required to activate the PMIP support. For example to turn on PMIP service via interface Ethernet 1/3, the following Mobile IP commands is needed:

```
interface Ethernet1/3
  ip address 14.1.1.30 255.255.255.0

ip mobile foreign-agent care-of Ethernet1/3
ip mobile foreign-service reverse-tunnel
ip mobile foreign-service revocation retransmit 3
ip mobile foreign-agent redundancy
```

Note **ip mobile foreign-agent redundancy** CLI is configured for PMIP redundancy.

After PMIP service is enabled through the global commands, MIP can be configured on a per WiMAX user-group basis using the **pmip profile**, and/or configuring the attributes that are provided by the AAA server.

L2-L2 bridging in the BWG does not work with MIP. When the established session is PMIP, L2 bridging is disabled if configured. If the session is PMIP, the L2-L3 option is done for Ethernet CS.

To enable L2-L2 bridging, perform the following tasks:

	Command	Purpose

Step 1	`router(config)# wimax agw user group-list wimax`
	`user-group cisco.com`
	`aaa accounting method-list agw`
	`sla profile-name silver`
	`bridge-group 1    ! Enable L2-L2 for Ethernet CS`
		Enables L2-L2 bridging on the BWG.

For IPCS or L2-L3 users, the PMIP feature for a user is indicated through its AAA attributes, or if the AAA attributes are absent, the user-group configuration using **pmip profile**.

The following is a sample configuration of the PMIP profile and the user-group:

```
router(config)#wimax agw pmip profile pmip1
 home-agent
  address 14.1.1.80
  ha-rk-key ascii rootcisco spi decimal 258 lifetime 6000
 proxy-mn
  gre-tunneling-enable
  no host-config-ext-request
  mn-ha-key ascii cisco spi 102 lifetime 3000
  coa-address 14.1.1.100
 !
```

The “host-config-ext-request” is enabled by default.

```
router(config)#wimax agw user group-list wimax
 user-group cisco.com
  aaa accounting method-list agw
  sla profile-name silver
    pmip profile-name pmip1
 !
```

The default flag is:

S-bit = 0

B-bit = 0

d-bit = 0

M-bit = 0

G-bit = configured through gre-tunneling-enable

r-bit = 0

T-bit = 1

x-bit = 0

I-bit = RFC 3543

Note The GRE tunnel should be configured through FA CLIs. Provided that the AAA server supplies enough information for a PMIP subscriber, all the user-group configuration is optional.

The registration lifetime for the session can be obtained in one of the following ways:

- Mn-ha-key lifetime is not configured, session_timeout is not configured, AAA does not send session_timeout:

  In this case, reg_lifetime is assumed to be infinite (65535).
- Mn-ha-key lifetime is not configured, session_timeout is configured > 65535:

  In this case, the session_timeout value is truncated to 65535 and used as reg_lifetime
- Mn-ha-key lifetime is configured > 0 and < 65536 and session_timeout is also configured > 0 and < 65536

  In this case, the configured mn-ha-key lifetime is used as reg_lifetime
- AAA sends session-timeout:

  If it is > 0 and < 65536, then it is used as reg_lifetime. If it is > 65535, then the truncated value of 65535 is used.

NAI Configuration

EAP Authenticated Call

The BWG obtains through the MS's NAI during the initial phase of authentication.

Here is an example of FA interface redundancy configuration through loopback

```
BWG #1

interface Loopback0
 ip address 16.1.1.100 255.255.255.255
!
! HSRP redundancy interface
!
interface Ethernet0/0
 description WiMAX Simulator Interface
 ip address 14.1.1.30 255.255.255.0
 standby 2 ip 14.1.1.100
 standby 2 name AGW-IOU
!
```

BWG PMIP Configuration

```
wimax agw pmip profile <name>
 home-agent
     address 14.1.1.80
     ha-rk-key ascii rootcisco spi decimal 258 lifetime 7200
```

```
   proxy-mn
     host-config-ext-request
     mn-ha-key ascii cisco spi 102 lifetime 7200
     coa-address 16.1.1.100

wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
  sla profile-name silver
  proxy realm cisco.com
  ip static-allowed
  pmip profile-name <name>
```

Mobile IP Configuration

```
router mobile
! tell FA about the loopback interface
ip mobile foreign-agent care-of Loopback0
!
ip mobile foreign-agent redundancy
ip mobile foreign-service revocation
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
```

BWG #2

!

The configuration for PMIP is identical on both the active and standby BWGs except that the physical interface is different for HSRP.

HSRP Redundancy Interface

```
interface Ethernet0/0
 description WiMAX Simulator Interface
 ip address 14.1.1.32 255.255.255.0
 standby 2 ip 14.1.1.100
 standby 2 name AGW-IOU
```

Here is an example of the FA interface redundancy configuration via HSRP group address

HSRP Redundancy Interface

```
BWG #1
interface Ethernet0/0
 description WiMAX Simulator Interface
 ip address 14.1.1.30 255.255.255.0
 standby 2 ip 14.1.1.100
 standby 2 name AGW-IOU
```

BWG PMIP Configuration

```
wimax agw pmip profile <name>
  home-agent
     address 14.1.1.80
     ha-rk-key ascii rootcisco spi decimal 258 lifetime 7200
   proxy-mn
     host-config-ext-request
     mn-ha-key ascii cisco spi 102 lifetime 7200
     coa-address 14.1.1.100
wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
  sla profile-name silver
  proxy realm cisco.com
  ip static-allowed
  pmip profile-name <name>
!
```

Mobile IP Configuration

```
router mobile
! tell FA about the loopback interface
ip mobile foreign-agent care-of Ethernet0/0
!
ip mobile foreign-agent redundancy
ip mobile foreign-service revocation
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
```

BWG #2

The configuration for PMIP is identical on both the active and standby BWGs except that the physical interface is different for HSRP.

HSRP Redundancy Interface

```
interface Ethernet0/0
 description WiMAX Simulator Interface
 ip address 14.1.1.32 255.255.255.0
 standby 2 ip 14.1.1.100
 standby 2 name AGW-IOU
```

Verifying the Configuration

Perform the following tasks to verify and troubleshoot PMIP information on the BWG:

	Command	Purpose
Step 1	`router#` **`show wimax agw`**	Displays various system parameters, including BWG software version, number of base stations allowed, number of subscribers allowed, and others. The following information has been added: • Current number of subscribers PMIP enabled
Step 2	`router#` **`show wimax agw subscriber`**	The output is enhanced to reflect the PMIP context information in the BWG. The PMIP tunnel and registry information can be obtained from the standard proxy mobile ip commands. The following information has been added: • Subscriber capability of using PMIP • MIP information such as: – HA Address – Home Address – //if host-config exists, – Home Network Prefix Length – Default Gateway – Primary DNS – Secondary DNS • Details Host – Host PMIP status (whether address allocated using PMIP) • Number of packets dropped due to MIP registration incomplete
Step 3	`router#` **`show wimax agw subscriber internal`**	In addition to the above information the following information has been added to this CLI: • MIP information such as: – MN-HA Key – MN-HA-Spi – HA-RK-Key – HA-RK-Key-Spi – Lifetime Requested – Mip-Flag – AAA-Pmip-Flag – Pmip-Cli-Conf-Flag

	Command	Purpose
Step 4	`router# show wimax agw statistics internal`	The following information has been added: • Number of packets dropped due to Static IP Host not authorized by AAA (previously - Number of packets dropped due to Static IP Host not allowed) • Number of packets dropped due to Static IP Host not authorized by HA • Data packets dropped DHCP packets received during MIP registration • Data packets dropped ARP packets received during MIP registration • Data packets dropped non-ARP and non-DHCP packets received during MIP registration • Total subscriber PMIP enabled created • Total subscriber PMIP enabled deleted • Number of packets dropped due to MIP registration incomplete
Step 5	`router# show wimax agw statistics dhcp-relay`	This command was formerly known as **show wimax agw statistics dhcp**. It displays the number for DHCP messages transmitted and received to/from DHCP server when the BWG acts as a DHCP relay.
Step 6	`router# show wimax agw statistics dhcp-proxy`	This command displays the number for DHCP messages transmitted and received to/from DHCP client when the BWG acts as a DHCP proxy.
Step 7	`router# show wimax agw fsm dhcp-proxy`	This command displays the number of elements currently in the different states of the proxy state machine.

Step 8	`router#show wimax agw statistics internal | inc SLB`
	`  Total SLB sticky update notifications succeeded 0`
	`  Total SLB sticky update notifications failed 0`
	`  Total SLB sticky delete notifications succeeded 0`
	`  Total SLB sticky delete notifications failed 0`
		4 counters have been added as part of SLB stickiness support. These counters will keep track of the number of Update and Delete notifications that were sent successfully and that failed.

The following debug commands were added to BWG Release 2.0:

	Command	Purpose
Step 1	**`router# debug wimax agw switching pmip`**	Displays PMIP switching debugs.
Step 2	**`router# debug wimax agw switching pmip errors`**	Displays PMIP switching error debugs.
Step 3	**`router# debug wimax agw switching pmip events`**	Displays PMIP switching event debugs.
Step 4	**`router# debug wimax agw switching pmip fsm`**	Displays PMIP switching fsm debugs.
Step 5	**`router# debug wimax agw switching pmip packet`**	Displays PMIP switching packet debugs.
Step 6	**`router# debug wimax agw switching pmip fsm errors`**	Displays PMIP switching fsm error debugs.
Step 7	**`router# debug wimax agw switching pmip fsm events`**	Displays PMIP switching fsm event debugs.
Step 8	**`router# debug wimax agw switching pmip packet detail`**	Displays PMIP switching packet details.

	Command	Purpose
Step 9	**router# debug wimax agw switching pmip packet brief**	Displays PMIP switching packet information.
Step 10	**router# debug ip slb sticky asn msid**	Logs debugs for SLB sticky information.

To Verify the PMIP Registry Table on FA:

```
BWG#show ip mobile proxy registration
Proxy Mobile Node Registrations:

100022240001@cisco.com:
    Registration accepted 06/13/08 05:18:59
    Next Re-registration 00:01:29
    Registration sequence number 1
    Care-of addr 14.1.1.30, HA addr 14.1.1.80, Home addr 5.1.0.2
    Flags sbdmg-T-, Identification CBFC81C3.1108C374
 Lifetime requested 00:50:00 (3000), granted 00:50:00,       remaining 00:26:29
    Revocation negotiated
```

To Verify HA’s Binding Table:

```
HA#sho ip mob bind
Mobility Binding List:
Total 4
Total VPDN Tunnel'ed 0
100022230001@cisco.com (Bindings 1):
    Home Addr 5.1.0.1
    Care-of Addr 14.1.1.30, Src Addr 14.1.1.30
    Lifetime granted 00:50:00 (3000), remaining 00:45:16
    Flags sbdmg-T-, Identification CBFC8713.59B6D7F8
    Tunnel0 src 14.1.1.80 dest 14.1.1.30 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Proxy registration, sequence number 1
    Revocation negotiated - I-bit not set
    Acct-Session-Id: 0x00000004
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

To Verify the Mobile IP Tunnel between HA and FA:

```
BWG#sho ip mobile tunnel
Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 14.1.1.30, dest 14.1.1.80
    encap IP/IP, mode reverse-allowed, tunnel-users 4
    Input ACL users 0, Output ACL users 0
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/3
    FA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    23106 packets input, 2772720 bytes, 0 drops
    23106 packets output, 2772720 bytes
```

To Verify HA Routing Table for Mobile Node:

```
HA#show ip route mobile
     5.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
M    5.1.0.0/16 is directly connected, Mobile0
M    5.1.0.1/32 [3/1] via 14.1.1.30, 06:24:02, Tunnel0
```

```
M    5.1.0.2/32 [3/1] via 14.1.1.30, 06:21:43, Tunnel0
M    5.1.0.3/32 [3/1] via 14.1.1.30, 06:21:40, Tunnel0
```

Here is a complete sample configuration for the BWG PMIP feature:

```
!
ip vrf voice
 rd 200:1
!
ip vrf sales
 rd 200:1
!
radius-server host 12.12.22.12
radius-server key cisco
! ! Start mobile IP process
router mobile

Specify an interface as the COA used by the MN
ip mobile foreign-agent care-of Ethernet1/3
ip mobile foreign-service reverse-tunnel
ip mobile foreign-service revocation retransmit 3
!
interface Ethernet1/0
Description Interface towards voice switch
 ip vrf forwarding voice
 ip address 15.9.9.1 255.255.0.0
!
interface Ethernet1/3
  ip address 14.1.1.30 255.255.255.0
!
interface Ethernet2/0
 description Interface towards sales department
 ip vrf forwarding sales
 ip address 15.9.9.2 255.255.0.0
!
interface Ethernet3/0
  description VLAN 10 for Voice
   ip address 4.2.4.4 255.255.0.0
   encapsulation dot1q 10
  !
interface Ethernet4/0
  description this interface to be used for FA
  ip address 4.3.4.4 255.255.0.0
!
!
Interface VirtualTemplate1
  ip address 4.4.4.4 255.255.0.0
  encapsulation agw
!
wimax agw service-flow pak-classify-rule profile sec1-classifier-uplink
  priority 1
     ipv4 permit gre 2.2.2.2 224.0.0.0 any
     ethernet permit any all 0032.00AE.0023 ffff.0000.0000 ethernet-type qinq
     vlan permit any priority 0 7
   !
!
wimax agw service-flow pak-classify-rule profile sec1-classifier-downlink
 priority 1
     ipv4 permit gre 2.2.2.2 224.0.0.0 any
     ethernet permit any all 0032.00AE.0023 all ethernet-type qinq
     vlan permit any priority any
    !
!
wimax agw service-flow profile sec1
```

```
    direction downlink
      cs-type eth-cs
          pak-classify-rule sec1-classifier-downlink
     cs-type ip-cs
          pak-classify-rule sec2-classifier-downlink
     qos-info isf-qos-downlink
 !
   direction uplink
      cs-type <eth-cs/ip-cs/vlan-cs>
          pak-classify-rule sec1-classifier-uplink
     qos-info isf-qos-uplink
     set vlan-priority 5
 !
!
wimax agw sla profile silver
    service-flow pre-defined isf profile isf
    service-flow pre-defined secondary 1 profile sec1
!
wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name silver
  proxy realm cisco.com
  ip mobile
   home-agent
     address 14.1.1.80
     ha-rk-key ascii rootcisco spi 102 lifetime 36000
   proxy-mn
     host-config-ext-request
     mn-ha-key ascii cisco spi 102 lifetime 36000
!
```