Proxy-Mobile IP

This chapter describes system support for Proxy Mobile IP and explains how it is configured. The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model before using the procedures in this chapter.

Proxy Mobile IP provides a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

This chapter includes the following sections:

Overview

Proxy Mobile IP provides mobility for subscribers with MNs that do not support the Mobile IP protocol stack.

Important Proxy Mobile IP is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The Proxy Mobile IP feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Table 1: Applicable Products and Relevant Sections

Applicable Product(s)	Refer to Sections
PDSN	• Proxy Mobile IP in 3GPP2 Service, on page 3 • How Proxy Mobile IP Works in 3GPP2 Network, on page 4 • Configuring FA Services, on page 30 • Configuring Proxy MIP HA Failover, on page 31 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 31 • RADIUS Attributes Required for Proxy Mobile IP, on page 32 • Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN, on page 33 • Configuring Default Subscriber Parameters in Home Agent Context, on page 34
GGSN	• Proxy Mobile IP in 3GPP Service, on page 4 • How Proxy Mobile IP Works in 3GPP Network, on page 11 • Configuring FA Services, on page 30 • Configuring Proxy MIP HA Failover, on page 31 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 31 • RADIUS Attributes Required for Proxy Mobile IP, on page 32 • Configuring Default Subscriber Parameters in Home Agent Context, on page 34 • Configuring APN Parameters, on page 34

Applicable Product(s)	Refer to Sections
ASN GW	• Proxy Mobile IP in WiMAX Service, on page 4 • How Proxy Mobile IP Works in WiMAX Network, on page 16 • Configuring FA Services, on page 30 • Configuring Proxy MIP HA Failover, on page 31 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 31 • RADIUS Attributes Required for Proxy Mobile IP, on page 32 • Configuring Default Subscriber Parameters in Home Agent Context, on page 34
PDIF	• How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication, on page 22 • Configuring FA Services, on page 30 • Configuring Proxy MIP HA Failover, on page 31 • *Configuring HA Services* • Configuring Subscriber Profile RADIUS Attributes, on page 31 • RADIUS Attributes Required for Proxy Mobile IP, on page 32 • Configuring Default Subscriber Parameters in Home Agent Context, on page 34

Proxy Mobile IP in 3GPP2 Service

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions get established between the MN and the PDSN as they would for a Simple IP session. However, the PDSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP PPP session with PDSN).

The MN is assigned an IP address by either the PDSN/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single PPP link, Proxy Mobile IP allows only a single session over the PPP link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP in 3GPP Service

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, a AAA server, or on a static-basis. The address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

Proxy Mobile IP in WiMAX Service

For subscriber sessions using Proxy Mobile subscriber sessions get established between the MN and the ASN GW as they would for a Simple IP session. However, the ASN GW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the Simple IP subscriber session with ASN GW).

The MN is assigned an IP address by either the ASN GW/FA or the HA. Regardless of its source, the address is stored in a mobile binding record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Note that unlike Mobile IP-capable MNs that can perform multiple sessions over a single session link, Proxy Mobile IP allows only a single session over the session link. In addition, simultaneous Mobile and Simple IP sessions will not be supported for an MN by the FA that is currently facilitating a Proxy Mobile IP session for the MN.

How Proxy Mobile IP Works in 3GPP2 Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the PDSN allocates an IP address to the MN. Note that the PDSN does not allocate an address from its IP pools.

- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and PDSN/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and PDSN/FA.

Figure 1: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow

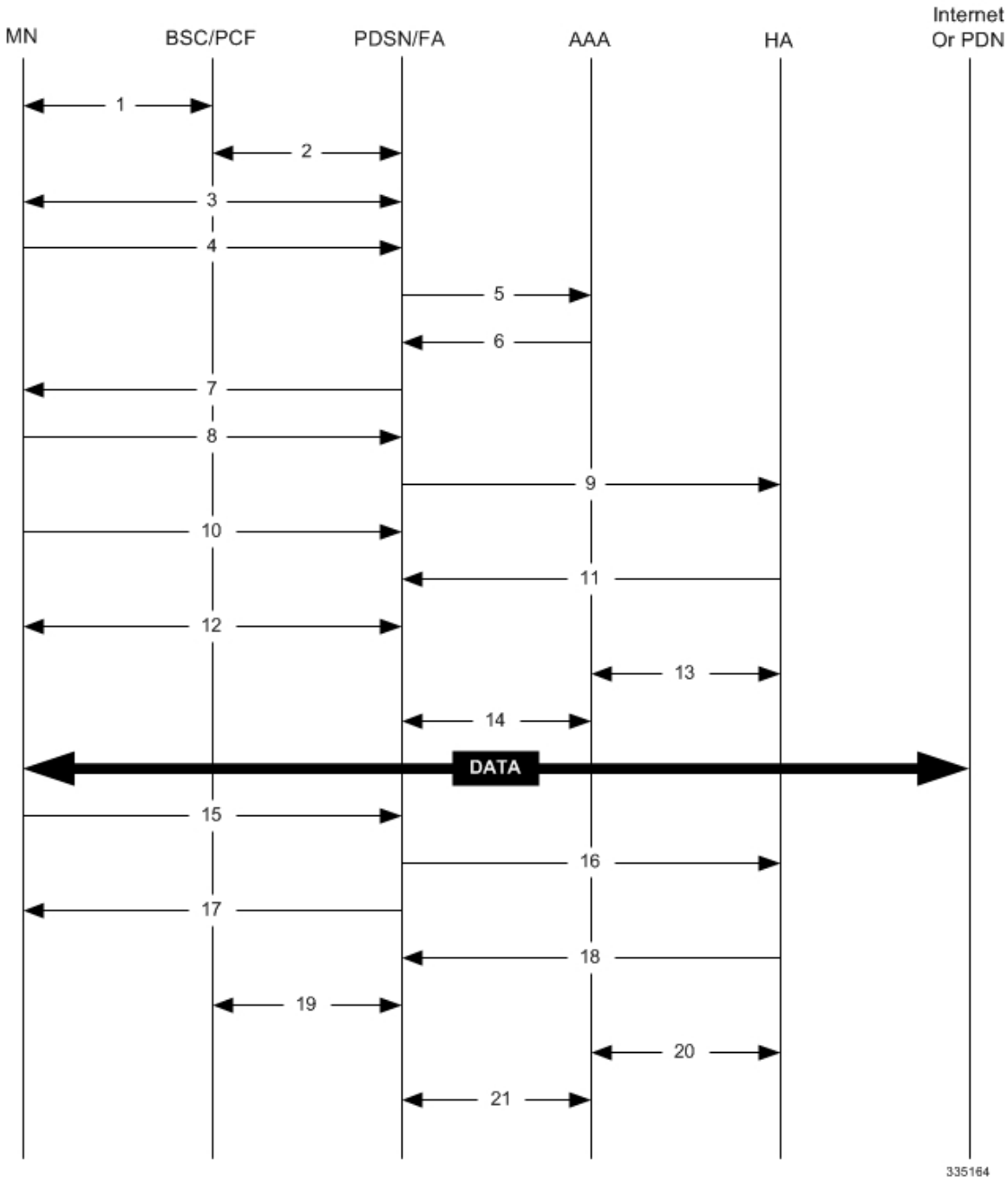

Table 2: AAA/PDSN Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.

Step	Description
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.

Step	Description
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 2: HA Assigned IP Address Proxy Mobile IP Call Flow

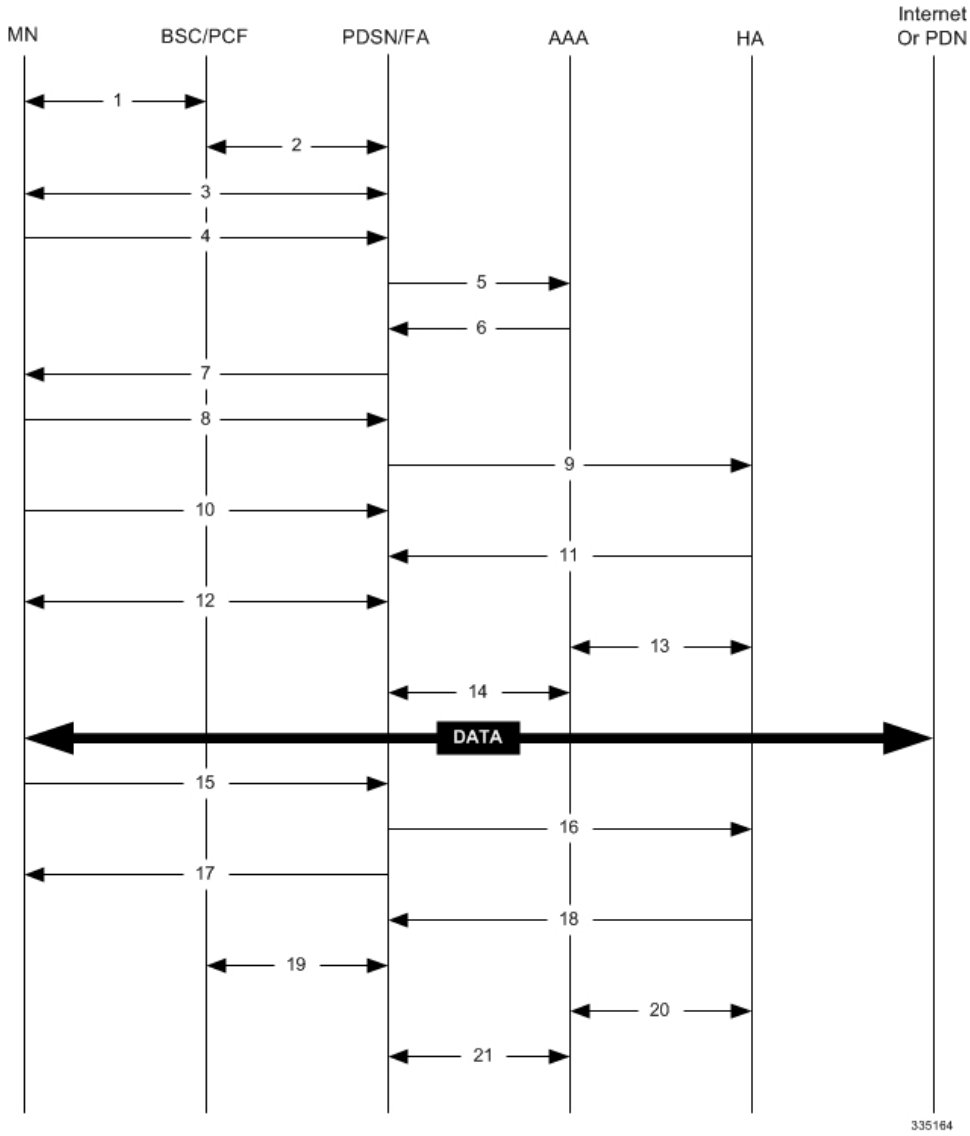

Table 3: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the RAN through the BSC/PCF.
2	The PCF and PDSN/FA establish the R-P interface for the session.
3	The PDSN/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the PDSN/FA.
5	The PDSN/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the PDSN/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The PDSN/FA sends a PPP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the PDSN/FA with an MN address of 0.0.0.0.
9	The PDSN/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the PDSN/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and PDSN/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the PDSN/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the PDSN to end the PPP session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The PDSN/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the Pi interface
19	The PDSN/FA and the PCF terminate the R-P session.
20	The HA and the AAA server stop accounting for the session.
21	The PDSN and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in 3GPP Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios in 3GPP network.

The following figure and the text that follows describe a a sample successful Proxy Mobile IP session setup call flow in 3GGP service.

Figure 3: Proxy Mobile IP Call Flow in 3GPP

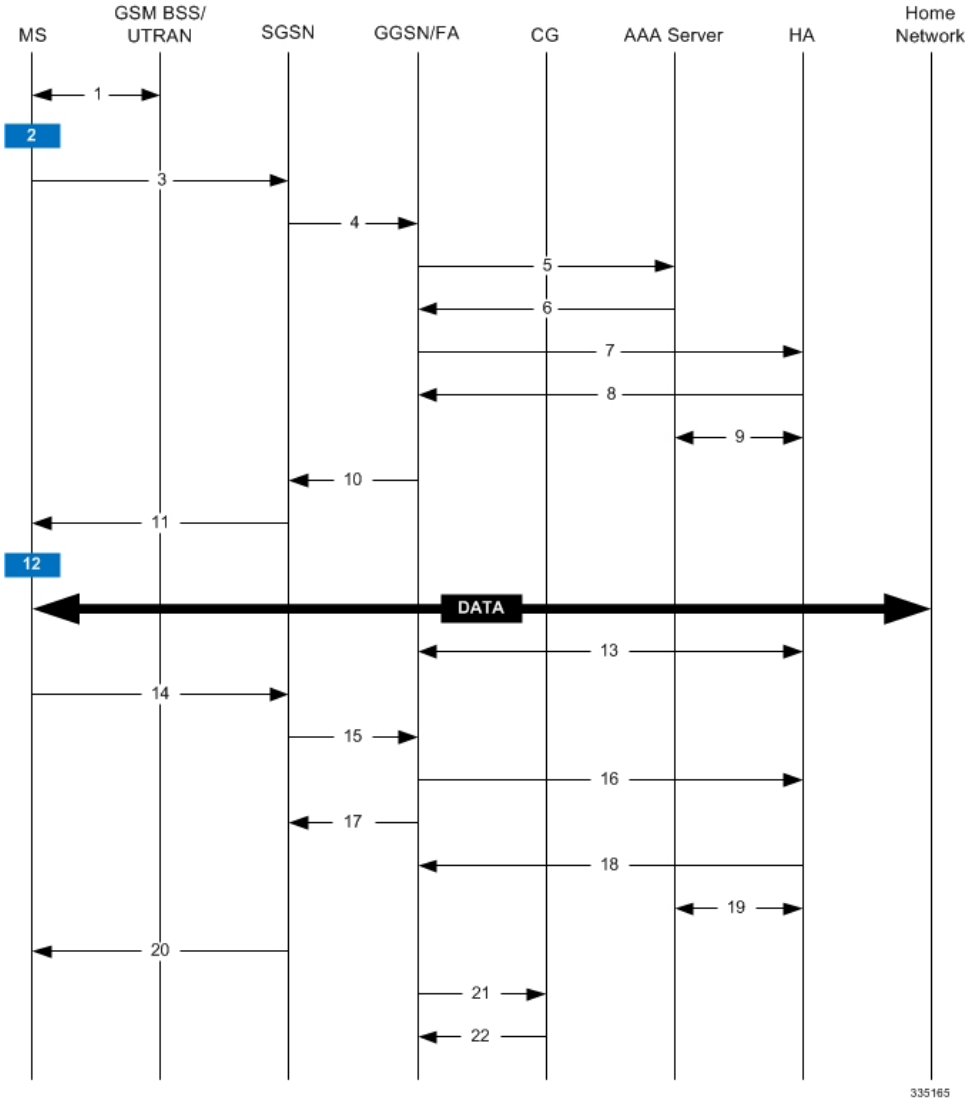

Table 4: Proxy Mobile IP Call Flow in 3GPP Description

Step	Description
1	The mobile station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

Step	Description
2	The terminal equipment (TE) aspect of the MS sends AT commands to the mobile terminal (MT) aspect of the MS to place it into PPP mode. The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information. Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.
3	The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), quality of service (QoS) requested, and PDP configuration options.
4	The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signalling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).

Step	Description
5	The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact. Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings. If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to a AAA server.
6	If the GGSN authenticated the subscriber to a AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.
7	If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
8	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
9	The HA sends an RADIUS Accounting Start request to the AAA server which the AAA server responds to.
10	The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

Step	Description
11	The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
12	The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
13	The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.
14	The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
15	The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
16	The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.
17	The GGSN returns a Delete PDP Context Response message to the SGSN.
18	The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19	The HA sends an RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20	The SGSN returns a Deactivate PDP Context Accept message to the MS.
21	The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a charging gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.

Step	Description
22	For each accounting message received from the GGSN, the CG responds with an acknowledgement.

How Proxy Mobile IP Works in WiMAX Network

This section contains call flows displaying successful Proxy Mobile IP session setup scenarios. There are multiple scenarios that are dependant on how the MN receives an IP address. The following scenarios are described:

- **Scenario 1:** The AAA server that authenticates the MN at the ASN GW allocates an IP address to the MN. Note that the ASN GW does not allocate an address from its IP pools.
- **Scenario 2:** The HA assigns an IP address to the MN from one of its locally configured dynamic pools.

Scenario 1: AAA server and ASN GW/FA Allocate IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the AAA server and ASN GW/FA.

Figure 4: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow

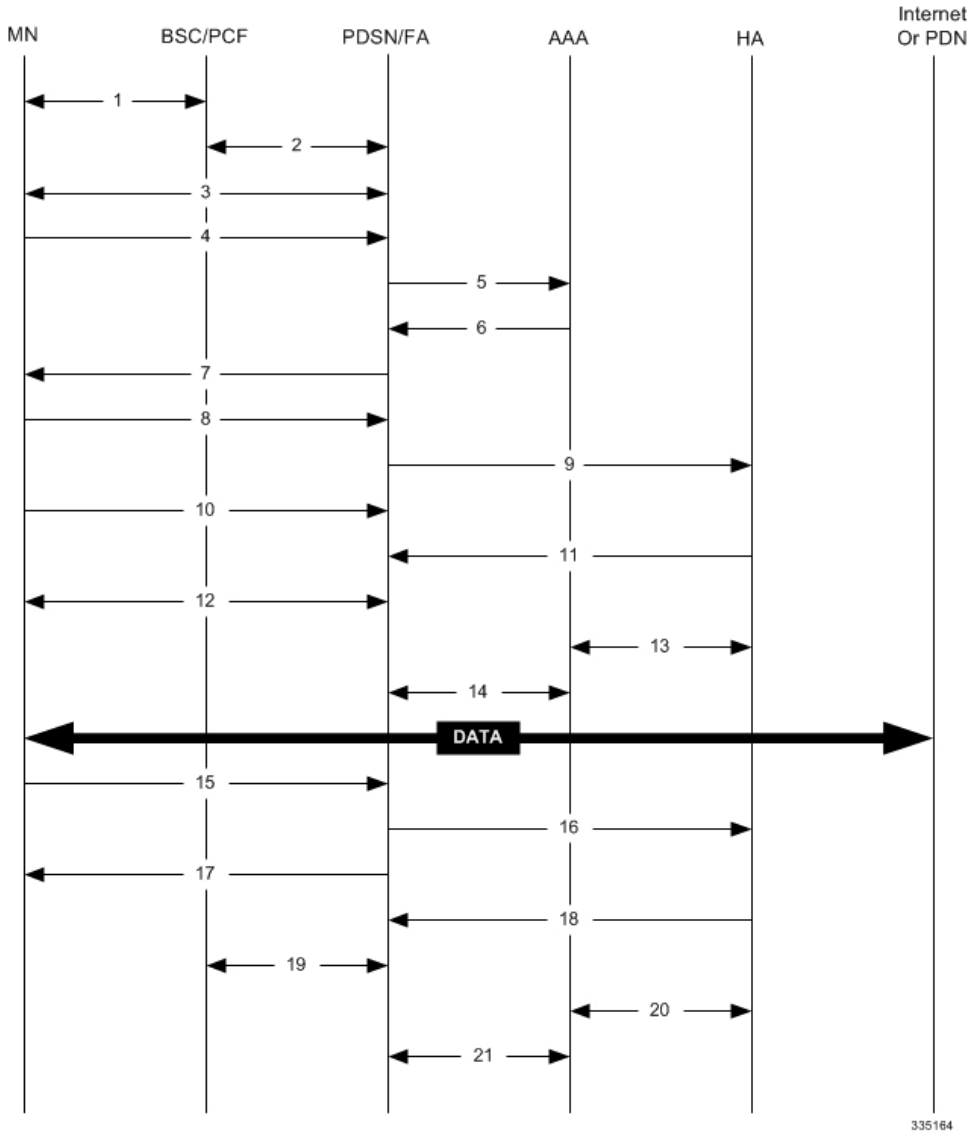

Table 5: AAA/ASN GW Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends a PPP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the MN's Home Address (IP address) and the IP address of the HA to use.
7	The ASN GW/FA sends a EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as the MN's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response after validating the home address against it's pool. The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.

Step	Description
16	The PDSN/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the subscriber session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

Scenario 2: HA Allocates IP Address

The following figure and table display and describe a call flow in which the MN receives its IP address from the HA.

Figure 5: HA Assigned IP Address Proxy Mobile IP Call Flow

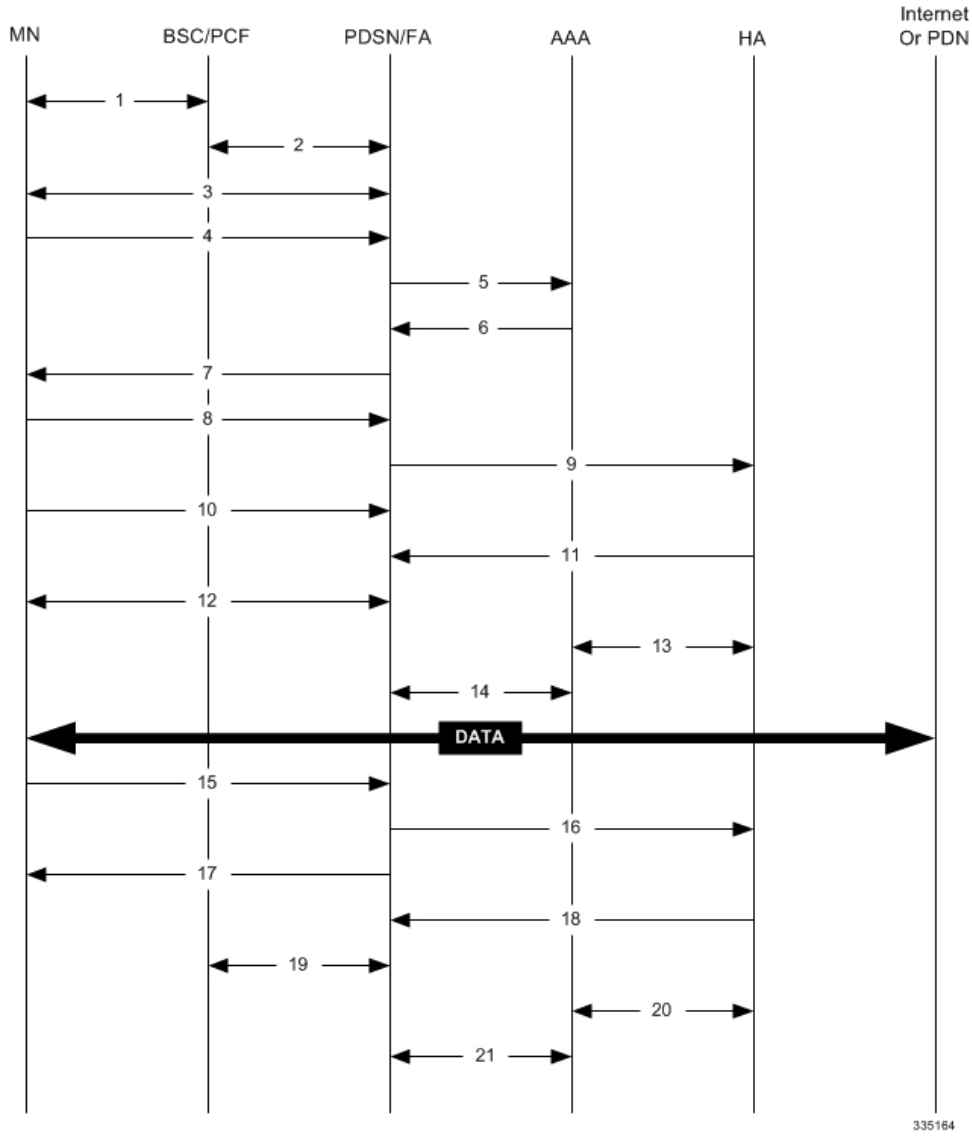

Table 6: HA Assigned IP Address Proxy Mobile IP Call Flow Description

Step	Description
1	Mobile Node (MN) secures a traffic channel over the airlink with the BS.
2	The BS and ASN GW/FA establish the R6 interface for the session.
3	The ASN GW/FA and MN negotiate Link Control Protocol (LCP).

Step	Description
4	Upon successful LCP negotiation, the MN sends an EAP Authentication Request message to the ASN GW/FA.
5	The ASN GW/FA sends an Access Request message to the RADIUS AAA server.
6	The RADIUS AAA server successfully authenticates the subscriber and returns an Access Accept message to the ASN GW/FA. The Accept message may contain various attributes to be assigned to the MN including the IP address of the HA to use.
7	The ASN GW/FA sends an EAP Authentication Response message to the MN.
8	The MN sends an Internet Protocol Control Protocol (IPCP) Configuration Request message to the ASN GW/FA with an MN address of 0.0.0.0.
9	The ASN GW/FA forwards a Proxy Mobile IP Registration Request message to the HA. The message includes fields such as a Home Address indicator of 0.0.0.0, the IP address of the FA (the care-of-address), the IP address of the FA (the care-of-address), and the FA-HA extension (security parameter index (SPI)).
10	While the FA is communicating with the HA, the MN may send additional IPCP Configuration Request messages.
11	The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MN (its Home Address). The HA also creates a mobile binding record (MBR) for the subscriber session.
12	The MN and the ASN GW/FA negotiate IPCP. The result is that the MN is assigned the home address originally specified by the AAA server.
13	While the MN and ASN GW/FA are negotiating IPCP, the HA and AAA server initiate accounting.
14	Upon completion of the IPCP negotiation, the ASN GW/FA and AAA server initiate accounting fully establishing the session allowing the MN to send/receive data to/from the PDN.
15	Upon completion of the session, the MN sends an LCP Terminate Request message to the ASN GW to end the subscriber session.

Step	Description
16	The ASN GW/FA sends a Proxy Mobile IP De-registration Request message to the HA.
17	The ASN GW/FA send an LCP Terminate Acknowledge message to the MN ending the PPP session.
18	The HA sends a Proxy Mobile IP De-Registration Response message to the FA terminating the R3 interface
19	The ASN GW/FA and the BS terminate the R6 session.
20	The HA and the AAA server stop accounting for the session.
21	The ASN GW and the AAA server stop accounting for the session.

How Proxy Mobile IP Works in a WiFi Network with Multiple Authentication

Proxy-Mobile IP was developed as a result of networks of Mobile Subscribers (MS) that are not capable of Mobile IP operation. In this scenario a PDIF acts a mobile IP client and thus implements Proxy-MIP support.

Although not required or necessary in a Proxy-MIP network, this implementation uses a technique called Multiple Authentication. In Multi-Auth arrangements, the device is authenticated first using HSS servers. Once the device is authenticated, then the subscriber is authenticated over a RADIUS interface to AAA servers. This supports existing EV-DO servers in the network.

The MS first tries to establish an IKEv2 session with the PDIF. The MS uses the EAP-AKA authentication method for the initial device authentication using Diameter over SCTP over IPv6 to communicate with HSS servers. After the initial Diameter EAP authentication, the MS continues with EAP MD5/GTC authentication.

After successful device authentication, PDIF then uses RADIUS to communicate with AAA servers for the subscriber authentication. It is assumed that RADIUS AAA servers do not use EAP methods and hence RADIUS messages do not contain any EAP attributes.

Assuming a successful RADIUS authentication, PDIF then sets up the IPSec Child SA tunnel using a Tunnel Inner Address (TIA) for passing control traffic only. PDIF receives the MS address from the Home Agent, and passes it on to the MS through the final AUTH response in the IKEv2 exchange.

When IPSec negotiation finishes, the PDIF assigns a home address to the MS and establishes a CHILD SA to pass data. The initial TIA tunnel is torn down and the IP address returned to the address pool.The PDIF then generates a RADIUS accounting START message.

When the session is disconnected, the PDIF generates a RADIUS accounting STOP message.

The following figures describe a Proxy-MIP session setup using CHAP authentication (EAP-MD5), but also addresses a PAP authentication setup using EAP-GTC when EAP-MD5 is not supported by either PDIF or MS.

Figure 6: Proxy-MIP Call Setup using CHAP Authentication

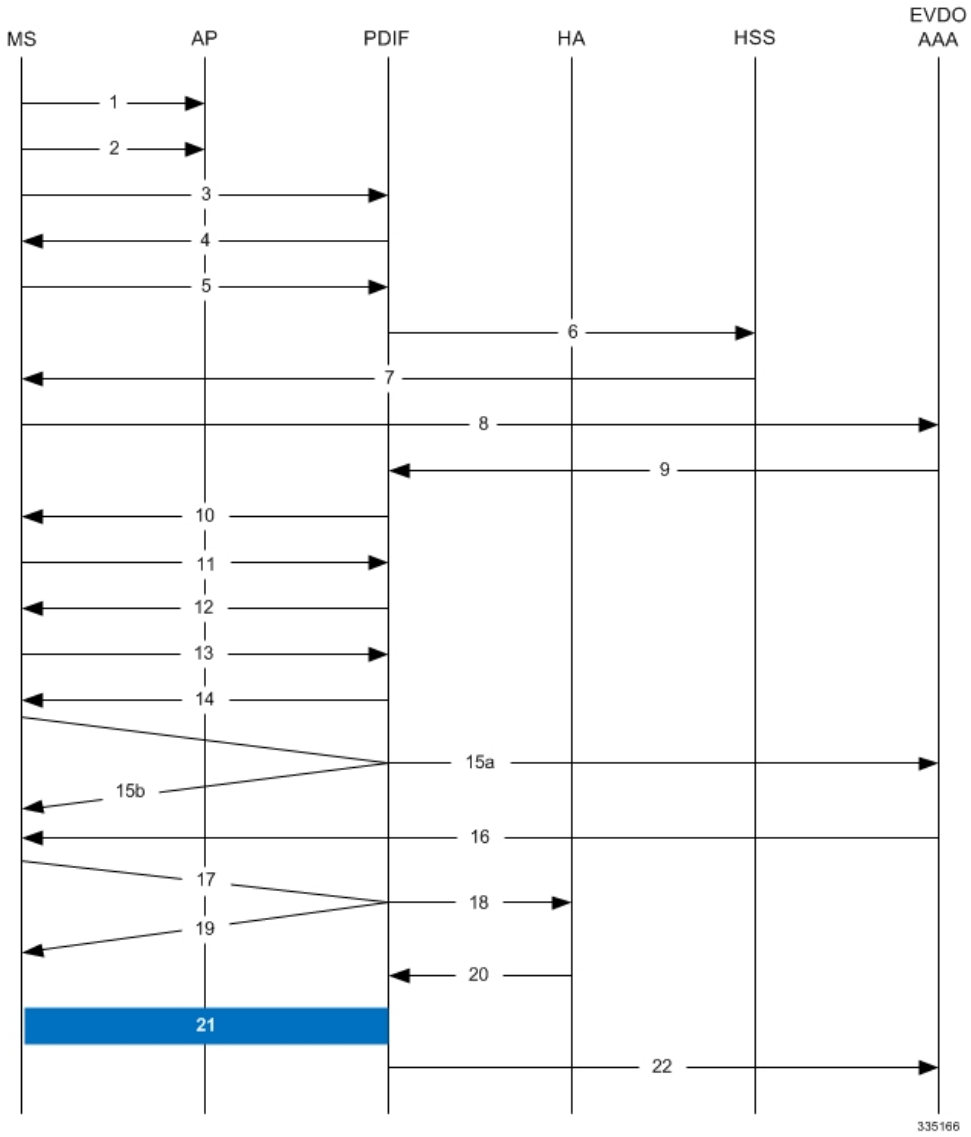

Table 7: Proxy-MIP Call Setup using CHAP Authentication

Step	Description
1	On connecting to WiFi network, MS first send DNS query to get PDIF IP address
2	MS receives PDIF address from DNS

Step	Description
3	MS sets up IKEv2/IPSec tunnel by sending IKE_SA_INIT Request to PDIF. MS includes SA, KE, Ni, NAT-DETECTION Notify payloads in the IKEv2 exchange.
4	PDIF processes the IKE_SA_INIT Request for the appropriate PDIF service (bound by the destination IP address in the IKEv2 INIT request). PDIF responds with IKE_SA_INIT Response with SA, KE, Nr payloads and NAT-Detection Notify payloads. If multiple-authentication support is configured to be enabled in the PDIF service, PDIF will include MULTIPLE_AUTH_SUPPORTED Notify payload in the IKE_SA_INIT Response. PDIF will start the IKEv2 setup timer after sending the IKE_SA_INIT Response.
5	On receiving successful IKE_SA_INIT Response from PDIF, MS sends IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it will include MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes IDi payload which contains the NAI, SA, TSi, TSr, CP (requesting IP address and DNS address) payloads. MS will not include AUTH payload to indicate that it will use EAP methods.
6	On receiving IKE_AUTH Request from MS, PDIF sends DER message to Diameter AAA server. AAA servers are selected based on domain profile, default subscriber template or default domain configurations. PDIF includes Multiple-Auth-Support AVP, EAP-Payload AVP with EAP-Response/Identity in the DER. Exact details are explained in the Diameter message sections. PDIF starts the session setup timer on receiving IKE_AUTH Request from MS.
7	PDIF receives DEA with Result-Code AVP specifying to continue EAP authentication. PDIF takes EAP-Payload AVP contents and sends IKE_ AUTH Response back to MS in the EAP payload. PDIF allows IDr and CERT configurations in the PDIF service and optionally includes IDr and CERT payloads (depending upon the configuration). PDIF optionally includes AUTH payload in IKE_AUTH Response if PDIF service is configured to do so.

Step	Description
8	MS receives the IKE_AUTH Response from PDIF. MS processes the exchange and sends a new IKE_AUTH Request with EAP payload. PDIF receives the new IKE_AUTH Request from MS and sends DER to AAA server. This DER message contains the EAP-Payload AVP with EAP-AKA challenge response and challenge received from MS.
9	The AAA server sends the DEA back to the PDIF with Result-Code AVP as "success." The EAP-Payload AVP message also contains the EAP result code with "success." The DEA also contains the IMSI for the user, which is included in the Callback-Id AVP. PDIF uses this IMSI for all subsequent session management functions such as duplicate session detection etc. PDIF also receives the MSK from AAA, which is used for further key computation.
10	PDIF sends the IKE_AUTH Response back to MS with the EAP payload.
11	MS sends the final IKE_AUTH Request for the first authentication with the AUTH payload computed from the keys. If the MS plans to do the second authentication, it will include ANOTHER_AUTH_FOLLOWS Notify payload also.

Step	Description
12	PDIF processes the AUTH request and responds with the IKE_AUTH Response with the AUTH payload computed from the MSK. PDIF does not assign any IP address for the MS pending second authentication. Nor will the PDIF include any configuration payloads. a. If PDIF service does not support Multiple-Authentication and ANOTHER_AUTH_FOLLOWS Notify payload is received, then PDIF sends IKE_AUTH Response with appropriate error and terminate the IKEv2 session by sending INFORMATIONAL (Delete) Request.b. If ANOTHER_AUTH_FOLLOWS Notify payload is not present in the IKE_AUTH Request, PDIF allocates the IP address from the locally configured pools. However, if **proxy-mip-required** is enabled, then PDIF initiates Proxy-MIP setup to HA by sending P-MIP RRQ. When PDIF receives the Proxy-MIP RRP, it takes the Home Address (and DNS addresses if any) and sends the IKE_AUTH Response back to MS by including CP payload with Home Address and DNS addresses. In either case, IKEv2 setup will finish at this stage and IPSec tunnel gets established with a Tunnel Inner Address (TIA).
13	MS does the second authentication by sending the IKE_AUTH Request with IDi payload to include the NAI. This NAI may be completely different from the NAI used in the first authentication.

Step	Description
14	On receiving the second authentication IKE_AUTH Request, PDIF checks the configured second authentication methods. The second authentication may be either EAP-MD5 (default) or EAP-GTC. The EAP methods may be either EAP-Passthru or EAP-Terminated. a. If the configured method is EAP-MD5, PDIF sends the IKE_AUTH Response with EAP payload including challenge.b. If the configured method is EAP-GTC, PDIF sends the IKE_AUTH Response with EAP-GTC.c. MS processes the IKE_AUTH Response: • If the MS supports EAP-MD5, and the received method is EAP-MD5, then the MS will take the challenge, compute the response and send IKE_AUTH Request with EAP payload including Challenge and Response. • If the MS does not support EAP-MD5, but EAP-GTC, and the received method is EAP-MD5, the MS sends legacy-Nak with EAP-GTC.
15(a)	PDIF receives the new IKE_AUTH Request from MS. If the original method was EAP-MD5 and MD5 challenge and response is received, PDIF sends RADIUS Access Request with corresponding attributes (Challenge, Challenge Response, NAI, IMSI etc.).
15(b)	If the original method was EAP-MD5 and legacy-Nak was received with GTC, the PDIF sends IKE_AUTH Response with EAP-GTC.
16	PDIF receives Access Accept from RADIUS and sends IKE_AUTH Response with EAP success.
17	PDIF receives the final IKE_AUTH Request with AUTH payload.
18	PDIF checks the validity of the AUTH payload and initiates Proxy-MIP setup request to the Home Agent if **proxy-mip-required** is enabled. The HA address may be received from the RADIUS server in the Access Accept (Step 16) or may be locally configured. PDIF may also remember the HA address from the first authentication received in the final DEA message.

Step	Description
19	If **proxy-mip-required** is disabled, PDIF assigns the IP address from the local pool.
20	PDIF received proxy-MIP RRP and gets the IP address and DNS addresses.
21	PDIF sets up the IPSec tunnel with the home address. On receiving the IKE_AUTH Response MS also sets up the IPSec tunnel using the received IP address. PDIF sends the IKE_AUTH Response back to MS by including the CP payload with the IP address and optionally the DNS addresses. This completes the setup.
22	PDIF sends a RADIUS Accounting start message.

Important For Proxy-MIP call setup using PAP, the first 14 steps are the same as for CHAP authentication. However, here they deviate because the MS does not support EAP-MD5 authentication, but EAP-GTC. In response to the EAP-MD5 challenge, the MS instead responds with legacy-Nak with EAP-GTC. The diagram below picks up at this point.

Figure 7: Proxy-MIP Call Setup using PAP Authentication

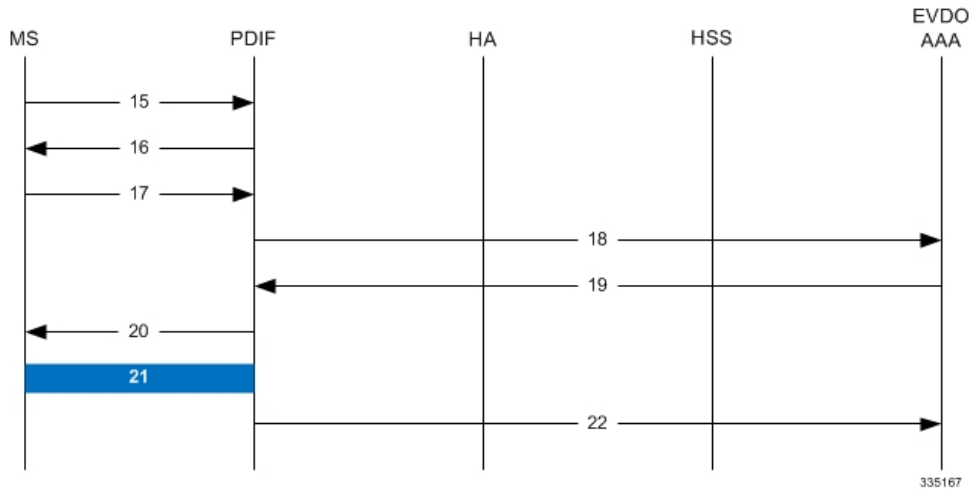

Table 8: Proxy-MIP Call Setup using PAP Authentication

Step	Description
15	MS is not capable of CHAP authentication but PAP authentication, and the MS returns the EAP payload to indicate that it needs EAP-GTC authentication.

Step	Description
16	PDIF then initiates EAP-GTC procedure, and requests a password from MS.
17	MS includes an authentication password in the EAP payload to PDIF.
18	Upon receipt of the password, PDIF sends a RADIUS Access Request which includes NAI in the User-Name attribute and PAP-password.
19	Upon successful authentication, the AAA server returns a RADIUS Access Accept message, which may include Framed-IP-Address attribute.
20	The attribute content in the Access Accept message is encoded as EAP payload with EAP success when PDIF sends the IKE_AUTH Response to the MS.
21	The MS and PDIF now have a secure IPSec tunnel for communication.
22	Pdif sends an Accounting START message.

Configuring Proxy Mobile-IP Support

Support for Proxy Mobile-IP requires that the following configurations be made:

Important Not all commands and keywords/variables may be supported. This depends on the platform type and the installed license(s).

- **FA service(s):** Proxy Mobile IP must be enabled, operation parameters must be configured, and FA-HA security associations must be specified.
- **HA service(s):** FA-HA security associations must be specified.
- **Subscriber profile(s):** Attributes must be configured to allow the subscriber(s) to use Proxy Mobile IP. These attributes can be configured in subscriber profiles stored locally on the system or remotely on a RADIUS AAA server.
- **APN template(s):** Proxy Mobile IP can be supported for every subscriber IP PDP context facilitated by a specific APN template based on the configuration of the APN.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a core network service and/or an HA according to the instructions described in the respective product administration guide.

Configuring FA Services

Use this example to configure an FA service to support Proxy Mobile IP:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip allow
 proxy-mip max-retransmissions <integer>
 proxy-mip retransmission-timeout <seconds>
 proxy-mip renew-percent-time percentage
 fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number
 { encrypted secret enc_secret | secret secret } [ description string ][
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | replay-protection {
timestamp | nonce } | timestamp-tolerance tolerance ]
authentication mn-ha allow-noauth
 end
```

Notes:

- The **proxy-mip max-retransmissions** command configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.
- **proxy-mip retransmission-timeout** configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.
- **proxy-mip renew-percent-time** configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

Example

If the advertisement registration lifetime configured for the FA service is 900 seconds and the renew-time is configured to 50, then the FA requests a lifetime of 900 seconds in the Proxy MIP registration request. If the HA grants a lifetime of **600** seconds, then the FA sends the Proxy Mobile IP Registration Renewal Request message after **300** seconds have passed.

- Use the **fa-ha-spi remote-address**command to modify configured FA-HA SPIs to support Proxy Mobile IP. Refer to the *Command Line Interface Reference* for the full command syntax.

Important Note that FA-HA SPIs **must** be configured for the Proxy-MIP feature to work, while it is optional for regular MIP.

- Use the **authentication mn-ha allow-noauth** command to configure the FA service to allow communications from the HA without authenticating the HA.

Verify the FA Service Configuration

Use the following command to verify the configuration of the FA service:

```
show fa-service name <fa_service_name>
```

Notes:

- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Proceed to the optional Configuring Proxy MIP HA Failover, on page 31 to configure Proxy MIP HA Failover support or skip to the *Configuring HA Services* to configure HA service support for Proxy Mobile IP.

Configuring Proxy MIP HA Failover

Use this example to configure Proxy Mobile IP HA Failover:

Important This configuration in this section is optional.

When configured, Proxy MIP HA Failover provides a mechanism to use a specified alternate Home Agent for the subscriber session when the primary HA is not available. Use the following configuration example to configure the Proxy MIP HA Failover:

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip ha-failover [ max-attempts <max_attempts> |
num-attempts-before-switching <num_attempts> | timeout <seconds> ]
```

Notes:

- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

Important Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

Configuring Subscriber Profile RADIUS Attributes

In order for subscribers to use Proxy Mobile IP, attributes must be configured in their user profile or in an APN for 3GPP service. As mentioned previously, the subscriber profiles can be located either locally on the system or remotely on a RADIUS AAA server.

This section provides information on the RADIUS attributes that must be used and instructions for configuring locally stored profiles/APNs in support of Proxy Mobile IP.

Important Instructions for configuring RADIUS-based subscriber profiles are not provided in this document. Please refer to the documentation supplied with your server for further information.

RADIUS Attributes Required for Proxy Mobile IP

The following table describes the attributes that must be configured in profiles stored on RADIUS AAA servers in order for the subscriber to use Proxy Mobile IP.

Table 9: Required RADIUS Attributes for Proxy Mobile IP

Attribute	Description	Values
SN-Subscriber- Permission OR SN1-Subscriber- Permission	Indicates the services allowed to be delivered to the subscriber. For Proxy Mobile IP, this attribute **must** be set to Simple IP.	• None (0) • Simple IP (0x01) • Mobile IP (0x02) • Home Agent Terminated Mobile IP (0x04)
SN-Proxy-MIP OR SN1-Proxy-MIP	Specifies if the configured service will perform compulsory Proxy-MIP tunneling for a Simple-IP subscriber. This attribute **must** be enabled to support Proxy Mobile IP.	• Disabled - do not perform compulsory Proxy-MIP (0) • Enabled - perform compulsory Proxy-MIP (1)
SN-Simultaneous- SIP-MIP OR SN1-Simultaneous- SIP-MIP	Indicates whether or not a subscriber can simultaneously access both Simple IP and Mobile IP services. **Note** Regardless of the configuration of this attribute, the FA facilitating the Proxy Mobile IP session will **not** allow simultaneous Simple IP and Mobile IP sessions for the MN.	• Disabled (0) • Enabled (1)

Attribute	Description	Values
SN-PDSN-Handoff- Req-IP-Addr OR SN1-PDSN-Handoff- Req-IP-Addr	Specifies whether or not the system should reject and terminate the subscriber session when the proposed address in IPCP by the mobile does not match the existing address that was granted by the chassis during an Inter-chassis handoff. This can be used to disable the acceptance of 0.0.0.0 as the IP address proposed by the MN during the IPCP negotiation that occurs during an Inter-chassis handoff. This attribute is disabled (do not reject) by default.	• Disabled - do not reject (0) • Enabled - reject (1)
3GPP2-MIP-HA-Address	This attribute sent in an Access-Accept message specifies the IP Address of the HA. Multiple attributes can be sent in Access Accept. However, only the first two are considered for processing. The first one is the primary HA and the second one is the secondary (alternate) HA used for HA Failover.	IPv4 Address

Configuring Local Subscriber Profiles for Proxy-MIP on a PDSN

This section provides information and instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDSN.

```
configure
 context <context_name>
 subscriber name <subscriber_name>
 permission pdsn-simple-ip
 proxy-mip allow
 inter-pdsn-handoff require ip-address
 mobile-ip home-agent <ha_address>
 <optional> mobile-ip home-agent <ha_address> alternate
 ip context-name <context_name>
 end
```

Verify that your settings for the subscriber(s) just configured are correct.

```
show subscribers configuration username <subscriber_name>
```

Notes:

- Configure the system to enforce the MN\'s use of its assigned IP address during IPCP negotiations resulting from inter-PDSN handoffs. Sessions re-negotiating IPCP will be rejected if they contain an address other than that which was granted by the PDSN (i.e. 0.0.0.0). This rule can be enabled by entering the **inter-pdsn-handoff require ip-address** command.
- Optional: If you have enabled the Proxy-MIP HA Failover feature, use the **mobile-ip home-agent** *ha_address* alternate command to specify the secondary, or alternate HA.
- Repeat this example as needed to configure additional FA services to support Proxy-MIP.
- Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring Local Subscriber Profiles for Proxy-MIP on a PDIF

This section provides instructions for configuring local subscriber profiles on the system to support Proxy Mobile IP on a PDIF.

```
configure
 context <context-name>
 subscriber name <subscriber_name>
 proxy-mip require
```

Note

subscriber_name is the name of the subscriber and can be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Configuring Default Subscriber Parameters in Home Agent Context

It is very important that the subscriber default, configured in the same context as the HA service, has the name of the destination context configured. Use the configuration example below:

```
configure
 context <context_name>
 ip context-name <context_name>
 end
```

Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring APN Parameters

This section provides instructions for configuring the APN templates to support Proxy Mobile IP for all IP PDP contexts they facilitate.

Important This is an optional configuration. In addition, attributes returned from the subscriber's profile for non-transparent IP PDP contexts take precedence over the configuration of the APN.

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name
```

Step 1 Enter the configuration mode by entering the following command:

configure

The following prompt appears:

`[local]host_name(config)`

Step 2 Enter context configuration mode by entering the following command:

context *<context_name>*

context_name is the name of the system destination context designated for APN configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.The following prompt appears:

`[<context_name>]host_name(config-ctx)`

Step 3 Enter the configuration mode for the desired APN by entering the following command:

apn *<apn_name>*

apn_name is the name of the APN that is being configured. The name must be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-).The following prompt appears:

`[<context_name>]host_name(config-apn)`

Step 4 Enable proxy Mobile IP for the APN by entering the following command:

proxy-mip required

This command causes proxy Mobile IP to be supported for all IP PDP contexts facilitated by the APN.

Step 5 *Optional.* GGSN/FA MN-NAI extension can be skipped in MIP Registration Request by entering following command:

proxy-mip null-username static-homeaddr

This command will enables the accepting of MIP Registration Request without NAI extensions in this APN.

Step 6 Return to the root prompt by entering the following command:

end

The following prompt appears:

`[local]host_name`

Step 7 Repeat *step 1* through *step 6* as needed to configure additional APNs.

Step 8 Verify that your APNs were configured properly by entering the following command:

show apn { all | name *<apn_name>* }

The output is a detailed listing of configured APN parameter settings.

Step 9 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.