Cisco ASR 5000 Series Home Agent Administration

Version 10.0

Last Updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22980-01

Cisco ASR 5000 Series Home Agent Administration

CONTENTS

About this Guide v
Conventions Used vi
Contacting Customer Support viii
HA Overview 9
System Components 10
ASR 5000 Platform: 10
Supported Standards 11
Requests for Comments (RFCs) 11
Network Deployment Configurations 15
Standalone PDSN/FA and HA Deployments 15
Interface Descriptions 15
Co-Located Deployments 16
Mobile IP Tunneling Methods 17
How Mobile IP Works 20
Understanding Mobile IP 24
Session Continuity Support for 3GPP2 and WiMAX Handoffs 24
Mobile IP Configuration Examples 25
Example 1: Mobile IP Support Using the System as an HA 26
Information Required 27
Source Context Configuration 28
Destination Context Configuration 31
How This Configuration Works 32
Example 2: HA Using a Single Source Context and Multiple Outsourced Destination Contexts 35
Information Required 36
Source Context Configuration 36
Destination Context Configuration 39
System-Level AAA Configuration 41
How This Configuration Works 42
Simple IP and Mobile IP in a Single System Configuration Example 45
Using the System as Both a PDSN/FA and an HA 46
Information Required 47
Source Context Configuration 47
AAA Context Configuration 49
Mobile IP Destination Context Configuration 50
Simple IP Destination Context 54
System-Level AAA Parameter Configuration 55
How This Configuration Works 56
Service Configuration Procedures 59
Creating and Configuring HA Services 60
Creating and Configuring an HA Service 60
Verifying HA Service Configuration 61
Session Continuity Support 64
Hybrid HA Service Configuration 66
Configuring WiMAX HA for WiMAX Calls only 66

Configuring WiMAX HA to Accept 3GPP2/Static MIP Key 67
Configuring Hybrid HA for WiMAX and 3GPP2 Calls 67
WiMAX-3GPP2 Interworking at HA 69
Mobile Node Requirement 69
H-AAA Requirements 69
FA and HA Function for 3GPP-WiMAX Interworking at HA 70
Configuring WiMAX FA Service 70
Configuring 3GPP2 FA Service 71
Configuring Common HA Service 71
Verifying and Saving Your Configuration 73
Verifying the Configuration 74
Feature Configuration 74
Service Configuration 75
Context Configuration 76
System Configuration 76
Finding Configuration Errors 76
Saving the Configuration 78
Saving the Configuration on the Chassis 79
Monitoring the Service 81
Monitoring System Status and Performance 82
Clearing Statistics and Counters 83
Engineering Rules 85
Interface and Port Rules 86
Pi Interface Rules 86
HA to FA 86
Subscriber Rules 87
Service Rules 88
Supported Registration Reply Codes 89
HA Service Reply Codes 90
Mobile-IP and Proxy-MIP Timer Considerations 93
Call Flow Summary 94
Timer Values and Recommendations 95
Controlling the Mobile IP Lifetime on a Per-Domain Basis 96

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
HA Overview

The Home Agent (HA) allows mobile nodes to be reached, or served, by their home network through its home address even when the mobile node is not attached to its home network. The HA performs this function through interaction with a Foreign Agent (FA) that the mobile node is communicating with using the Mobile IP (MIP) standard. Such transactions are performed through the use of virtual private networks that create MIP tunnels between the HA and FA.

When functioning as an HA, the system can either be located within the carrier's 3G network or in an external enterprise or ISP network. Regardless, the FA terminates the mobile subscriber's PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

This chapter includes the following sections:

- System Components and Capacities
- Network Deployment Configurations
- Understanding Mobile IP

System Components

The following application and line cards are required to support CDMA2000 wireless data services on the system:

ASR 5000 Platform:

- **System Management Cards (SMCs):** Provides full system control and management of all cards within the ASR 5000 platform. Up to two SMC can be installed; one active, one redundant.
- **Packet Processing Cards (PSC, PSC2, PPC):** Within the ASR 5000 platform, packet processing cards provide high-speed, multi-threaded PPP processing capabilities to support HA services. Up to 14 packet processing cards can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIO):** Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, Central Office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Ethernet 10/100 and/or Ethernet 1000/Quad Ethernet 1000 Line Cards:** Installed directly behind processing cards, these cards provide the RP, AAA, PDN, and Pi interfaces to elements in the data network. Up to 26 line cards should be installed for a fully loaded system with 13 active processing cards, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant processing cards do no not require line cards.
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000/Quad Ethernet 1000 line cards and every processing card in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and processing cards.


Important: Additional information pertaining to each of the application and line cards required to support CDMA2000 wireless data services is located in the Product Overview Guide.

Supported Standards

The system supports the following industry standards for 1x/CDMA2000/EV-DO devices.

Requests for Comments (RFCs)

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for Managing Asynchronously Generated Alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1771, A Border Gateway Protocol 4 (BGP-4)
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996

- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC-2401, Security Architecture for the Internet Protocol, November 1998
- RFC-2402, IP Authentication Header (AH), November 1998
- RFC-2406, IP Encapsulating Security Payload (ESP), November 1998
- RFC-2408, Internet Security Association and Key Management Protocol (ISAKMP), November 1998
- RFC-2409, The Internet Key Exchange (IKE), November 1998
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999

- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC2598 - Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol “L2TP”, August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3095, Robust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed, July 2001
- RFC-3101, OSPF NSSA Option, January 2003.
- RFC-3141, CDMA2000 Wireless Data Requirements for AAA, June 2001
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3241 Robust Header Compression (ROHC) over PPP, April 2002
- RFC-3409, Lower Layer Guidelines for Robust (RTP/UDP/IP) Header Compression, December 2002
- RFC-3519, NAT Traversal for Mobile IP, April 2003
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3576 - Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3759, Robust Header Compression (ROHC): Terminology and Channel Mapping Examples, April 2004
- RFC-3588, Diameter Based Protocol, September 2003

- RFC-4005, Diameter Network Access Server Application, August 2005
- RFC-4006, Diameter Credit-Control Application, August 2005
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

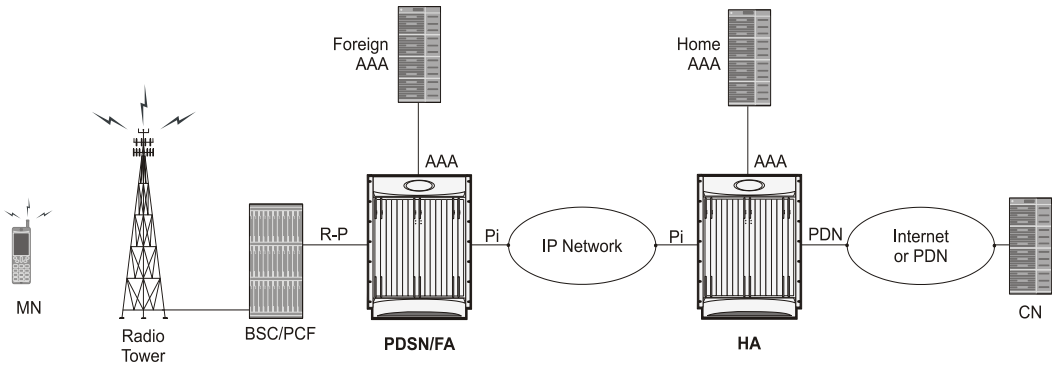
Network Deployment Configurations

This section provides examples of how the system can be deployed within a wireless carrier's network. As noted previously in this chapter, the system can be deployed in standalone configurations, serving as a Home Agent (HA) and a Packet Data Serving Node/Foreign Agent (PDSN/FA), or in a combined PDSN/FA/HA configuration providing all services from a single chassis.

Standalone PDSN/FA and HA Deployments

The following figure depicts a sample network configuration wherein the HA and the PDSN/FA are separate systems.

Figure 1. PDSN/FA and HA Network Deployment Configuration Example



The HA allows mobile nodes to be reached, or served, by their home network through its home address even when the mobile node is not attached to its home network. The HA performs this function through interaction with an FA that the mobile node is communicating with using the Mobile IP protocol. Such transactions are performed through the use of virtual private networks that create Mobile IP tunnels between the HA and FA.

Interface Descriptions

This section describes the primary interfaces used in a CDMA2000 wireless data network deployment.

Pi Interfaces

The Pi interface provides connectivity between the HA and its corresponding FA. The Pi interface is used to establish a Mobile IP tunnels between the PDSN/FA and HA.

PDN Interfaces

PDN interface provide connectivity between the PDSN and/or HA to packet data networks such as the Internet or a corporate intranet.

AAA Interfaces

Using the LAN ports located on the Switch Processor I/O (SPIO) and Ethernet line cards, these interfaces carry AAA messages to and from RADIUS accounting and authentication servers. The SPIO supports RADIUS-capable management interfaces using either copper or fiber Ethernet connectivity through two auto-sensing 10/100/1000 Mbps Ethernet interfaces or two SFP optical gigabit Ethernet interfaces. User-based RADIUS messaging is transported using the Ethernet line cards.

While most carriers will configure separate AAA interfaces to allow for out-of-band RADIUS messaging for system administrative users and other operations personnel, it is possible to use a single AAA interface hosted on the Ethernet line cards to support a single RADIUS server that supports both management users and network users.

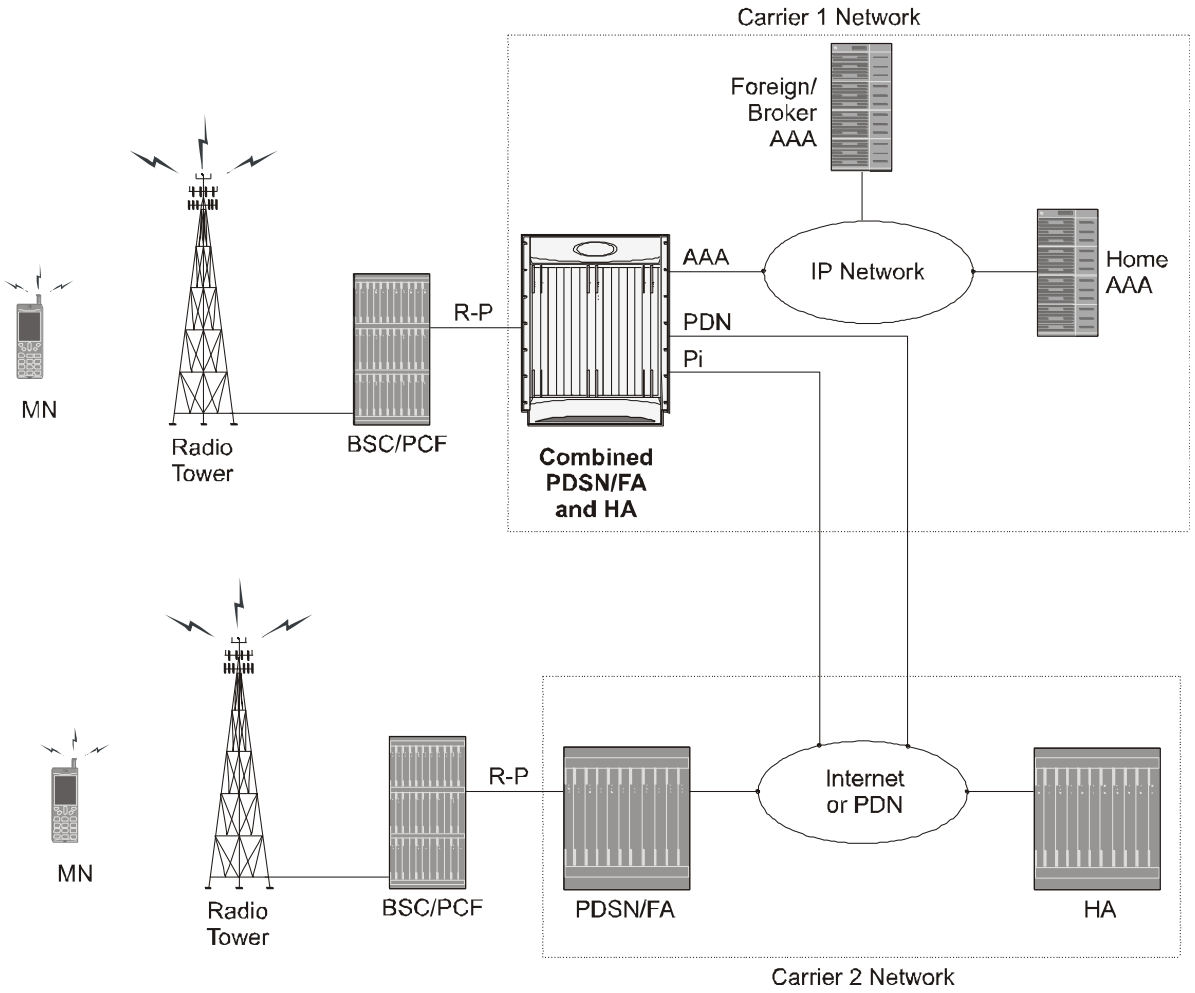
Important: Subscriber AAA interfaces should always be configured using Ethernet line card interfaces for the highest performance. The local context should not be used for service subscriber AAA functions.

Co-Located Deployments

An advantage of the system is its ability to support both high-density HA and PDSN/FA configurations within the same chassis. The economies of scale presented in this configuration example provide for both improved session handling and reduced cost in deploying a CDMA2000 data network.

The following figure depicts a sample co-located deployment.

Figure 2. Co-located PDSN/FA and HA Configuration Example.



It should be noted that all interfaces defined within the 3GPP2 standards for 1x deployments exist in this configuration as they are described in the two previous sections. This configuration can support communications to external, or standalone, HAs and/or PDSNs/FAs using all prescribed standards.

Mobile IP Tunneling Methods

Tunneling by itself is a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within a packet, carried by the second network. Tunneling is also called encapsulation. Service providers typically use tunneling for two purposes; first, to transport otherwise un-routable packets across the IP network and second, to provide data separation for Virtual Private Networking (VPN) services. In Mobile IP, tunnels are used to transport data packets between the FA and HA.

The system supports the following tunneling protocols, as defined in the IS-835-A specification and the relevant Request For Comments (RFCs) for Mobile IP:

IP in IP tunnels

IP in IP tunnels basically encapsulate one IP packet within another using a simple encapsulation technique. To encapsulate an IP datagram using IP in IP encapsulation, an outer IP header is inserted before the datagram's existing IP header. Between them are other headers for the path, such as security headers specific to the tunnel configuration. Each header chains to the next using IP Protocol values. The outer IP header Source and Destination identify the “endpoints” of the tunnel. The inner IP header Source and Destination identify the original sender and recipient of the datagram, while the inner IP header is not changed by the encapsulator, except to decrement the TTL, and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. If needed, other protocol headers such as the IP Authentication header may be inserted between the outer IP header and the inner IP header.

The Mobile IP working group has specified the use of encapsulation as a way to deliver datagrams from an MN's HA to an FA, and conversely from an FA to an HA, that can deliver the data locally to the MN at its current location.

GRE tunnels

The Generic Routing Encapsulation (GRE) protocol performs encapsulation of IP packets for transport across disparate networks. One advantage of GRE over earlier tunneling protocols is that any transport protocol can be encapsulated in GRE. GRE is a simple, low overhead approach—the GRE protocol itself can be expressed in as few as eight octets as there is no authentication or tunnel configuration parameter negotiation. GRE is also known as IP Protocol 47.

Important: The chassis simultaneously supports GRE protocols with key in accordance with RFC-1701/RFC-2784 and “Legacy” GRE protocols without key in accordance to RFC-2002.

Another advantage of GRE tunneling over IP-in-IP tunneling is that GRE tunneling can be used even when conflicting addresses are in use across multiple contexts (for the tunneled data).

Communications between the FA and HA can be done in either the forward or reverse direction using the above protocols. Additionally, another method of routing information between the FA and various content servers used by the HA exists. This method is called Triangular Routing. Each of these methods is explained below.

Forward Tunneling

In the wireless IP world, forward tunneling is a tunnel that transports packets from the packet data network towards the MN. It starts at the HA and ends at the MN's care-of address. Tunnels can be as simple as IP-in-IP tunnels, GRE tunnels, or even IP Security (IPSec) tunnels with encryption. These tunnels can be started automatically, and are selected based on the subscriber's user profile.

Reverse Tunneling

A reverse tunnel starts at the MN's care-of address, which is the FA, and terminates at the HA.

When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Using the Direct Delivery Style, which is the default mode for the system, the MN designates the FA as its default router and sends packets directly to the FA without encapsulation. The FA intercepts them, and tunnels them to the HA.

Using the Encapsulating Delivery Style, the MN encapsulates all its outgoing packets to the FA. The FA then de-encapsulates and re-tunnels them to the HA, using the FA's care-of address as the entry-point for this new tunnel.

Following are some of the advantages of reverse tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Triangular Routing

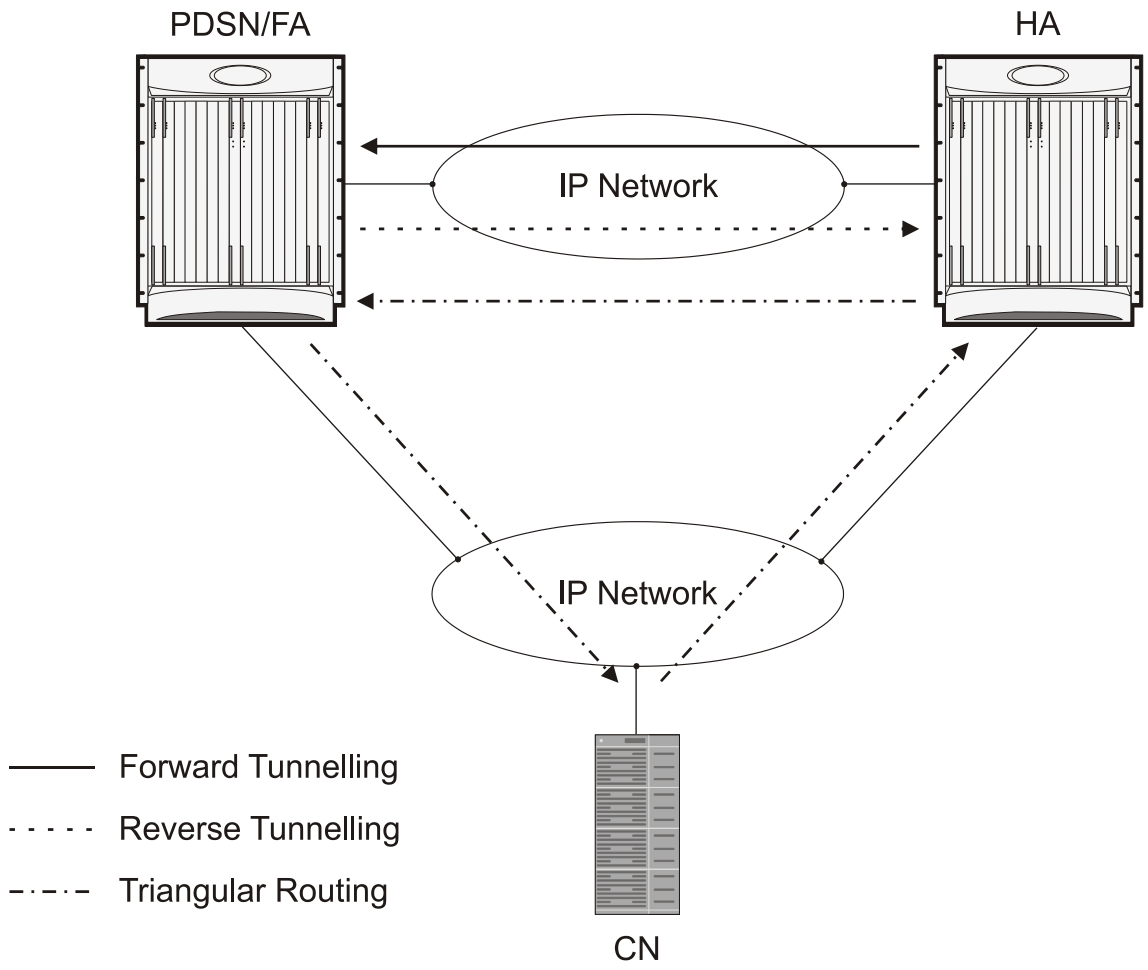
Triangular routing is the path followed by a packet from the MN to the Correspondent Node (CN) via the FA. In this routing scenario, the HA receives all the packets destined to the MN from the CN and redirects them to the MN's care-of-address by forward tunneling. In this case, the MN sends packets to the FA, which are transported using conventional IP routing methods.

A key advantage of triangular routing is that reverse tunneling is not required, eliminating the need to encapsulate and de-capsulate packets a second time during a Mobile IP session since only a forward tunnel exists between the HA and PDSN/FA.

A disadvantage of using triangular routing is that the HA is unaware of all user traffic for billing purposes. Also, both the HA and FA are required to be connected to a private network. This can be especially troublesome in large networks, serving numerous enterprise customers, as each FA would have to be connected to each private network.

The following figure shows an example of how triangular routing is performed.

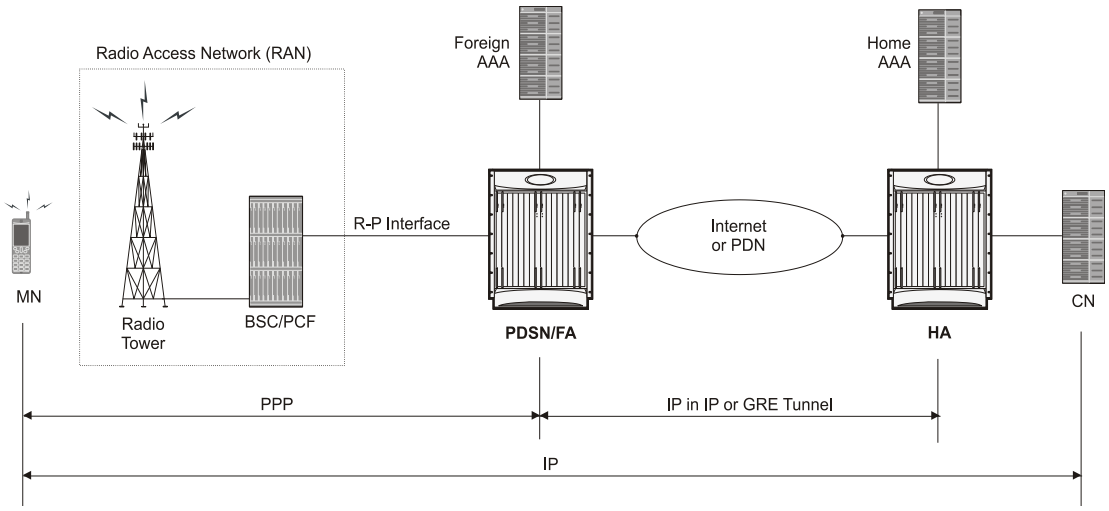
Figure 3. Mobile IP, FA and HA Tunneling/Transport Methods.



How Mobile IP Works

As described earlier, Mobile IP uses three basic communications protocols; PPP, IP, and Tunneled IP in the form of IP-in-IP or GRE tunnels. The following figure depicts where each of these protocols are used in a basic Mobile IP call.

Figure 4. Mobile IP Protocol Usage.



As depicted above, PPP is used to establish a communications session between the MN and the FA. Once a PPP session is established, the MN can communicate with the HA, using the FA as a mediator or broker. Data transport between the FA and HA use tunneled IP, either IP-in-IP or GRE tunneling. Communication between the HA and End Host can be achieved using the Internet or a private IP network and can use any IP protocol.

The following figure provides a high-level view of the steps required to make a Mobile IP call that is initiated by the MN to a HA. The following table explains each step in detail. Users should keep in mind that steps in the call flow related to the Radio Access Node (RAN) functions are intended to show a high-level overview of radio communications iterations, and as such are outside the scope of packet-based communications presented here.

Figure 5. Mobile IP Call Flow

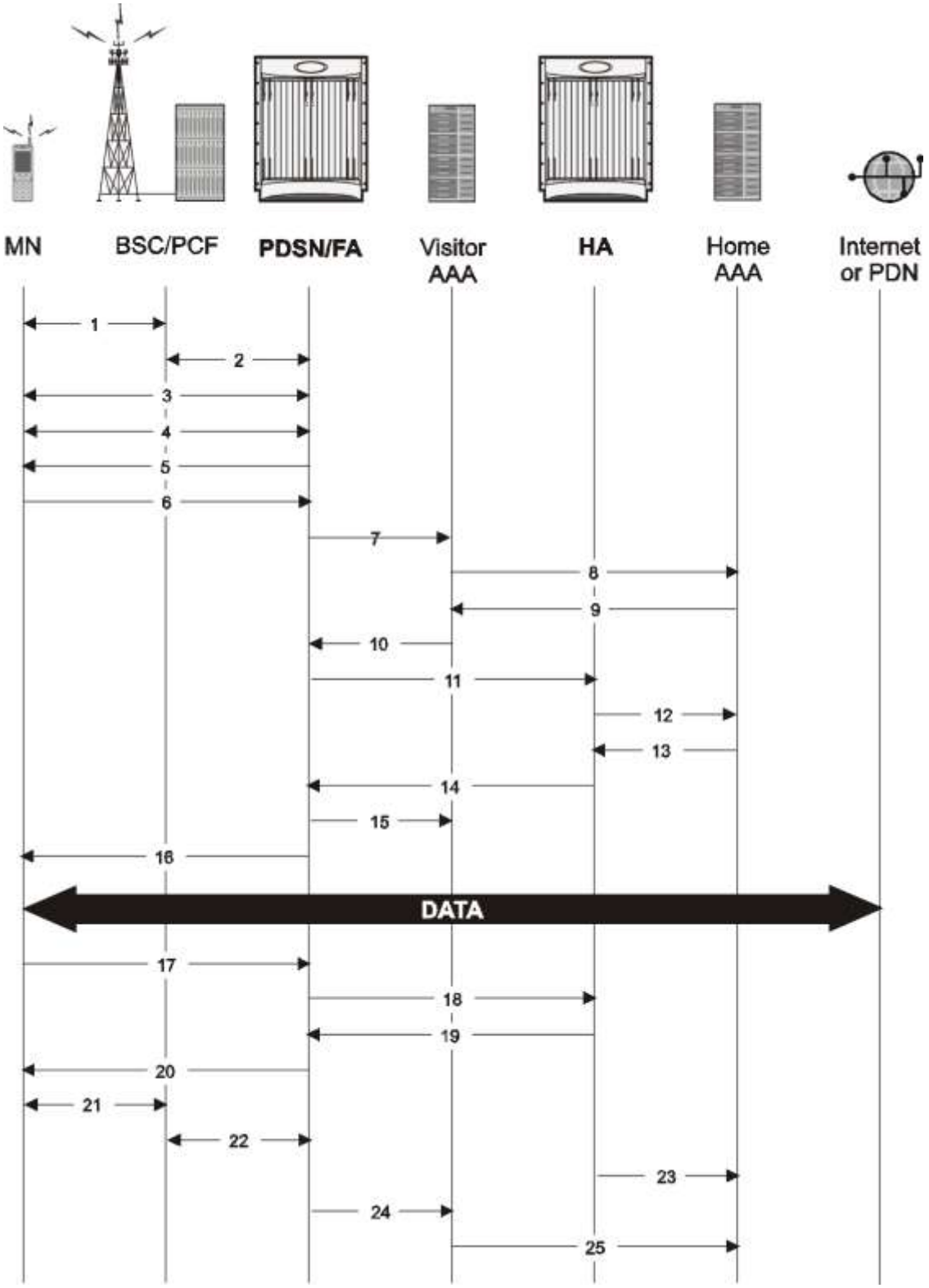


Table 1. Mobile IP Call Flow Description

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 establish the R-P interface for the session.
3	The PDSN and MN negotiate Link Control Protocol (LCP).
4	The PDSN and MN negotiate the Internet Protocol Control Protocol (IPCP).
5	The PDSN/FA sends an Agent Advertisement to the MN.
6	The MN sends a Mobile IP Registration Request to the PDSN/FA.
7	The PDSN/FA sends an Access Request message to the visitor AAA server.
8	The visitor AAA server proxies the request to the appropriate home AAA server.
9	The home AAA server sends an Access Accept message to the visitor AAA server.
10	The visitor AAA server forwards the response to the PDSN/FA.
11	Upon receipt of the response, the PDSN/FA forwards a Mobile IP Registration Request to the appropriate HA.
12	The HA sends an Access Request message to the home AAA server to authenticate the MN/subscriber.
13	The home AAA server returns an Access Accept message to the HA.
14	Upon receiving response from home AAA, the HA sends a reply to the PDSN/FA establishing a forward tunnel. Note that the reply includes a Home Address (an IP address) for the MN.
15	The PDSN/FA sends an Accounting Start message to the visitor AAA server. The visitor AAA server proxies messages to the home AAA server as needed.
16	The PDSN return a Mobile IP Registration Reply to the MN establishing the session allowing the MN to send/receive data to/from the PDN.
17	Upon session completion, the MN sends a Registration Request message to the PDSN/FA with a requested lifetime of 0.
18	The PDSN/FA forwards the request to the HA.
19	The HA sends a Registration Reply to the PDSN/FA accepting the request.
20	The PDSN/FA forwards the response to the MN.
21	The MN and PDSN/FA negotiate the termination of LCP effectively ending the PPP session.
22	The PCF and PDSN/FA close terminate the R-P session.
23	The HA sends an Accounting Stop message to the home AAA server.
24	The PDSN/FA sends an Accounting Stop message to the visitor AAA server.
25	The visitor AAA server proxies the accounting data to the home AAA server.

Understanding Mobile IP

Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

In Mobile IP, the Mobile Node (MN) receives an IP address, either static or dynamic, called the “home address” assigned by its Home Agent (HA). A distinct advantage with Mobile IP is that MNs can hand off between different radio networks that are served by different PDSNs.

In this scenario, the Network Access Function (such as a PDSN) in the visitor network performs as a Foreign Agent (FA), establishing a virtual session with the MN's HA. Each time the MN registers with a different PDSN/FA, the FA assigns the MN a care-of-address. Packets are then encapsulated into IP tunnels and transported between FA, HA, and the MN.

Session Continuity Support for 3GPP2 and WiMAX Handoffs

HA provides this feature for seamless session mobility for WiMAX subscriber and other access technology subscribers as well. By implementation of this feature HA can be configured for:

- 3GPP2 HA Service
- 3GPP HA Service
- WiMAX HA Service
- Combination of 3GPP2 and WiMAX HA Services for Dual mode device

The above configurations provide the session continuity capability that enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective. This capability brings the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity

Chapter 2
Mobile IP Configuration Examples

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.

Important: This chapter does not discuss the configuration of the local context. Information about the local context can be found in Chapter 1 of Command Line Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

This section includes the following examples:

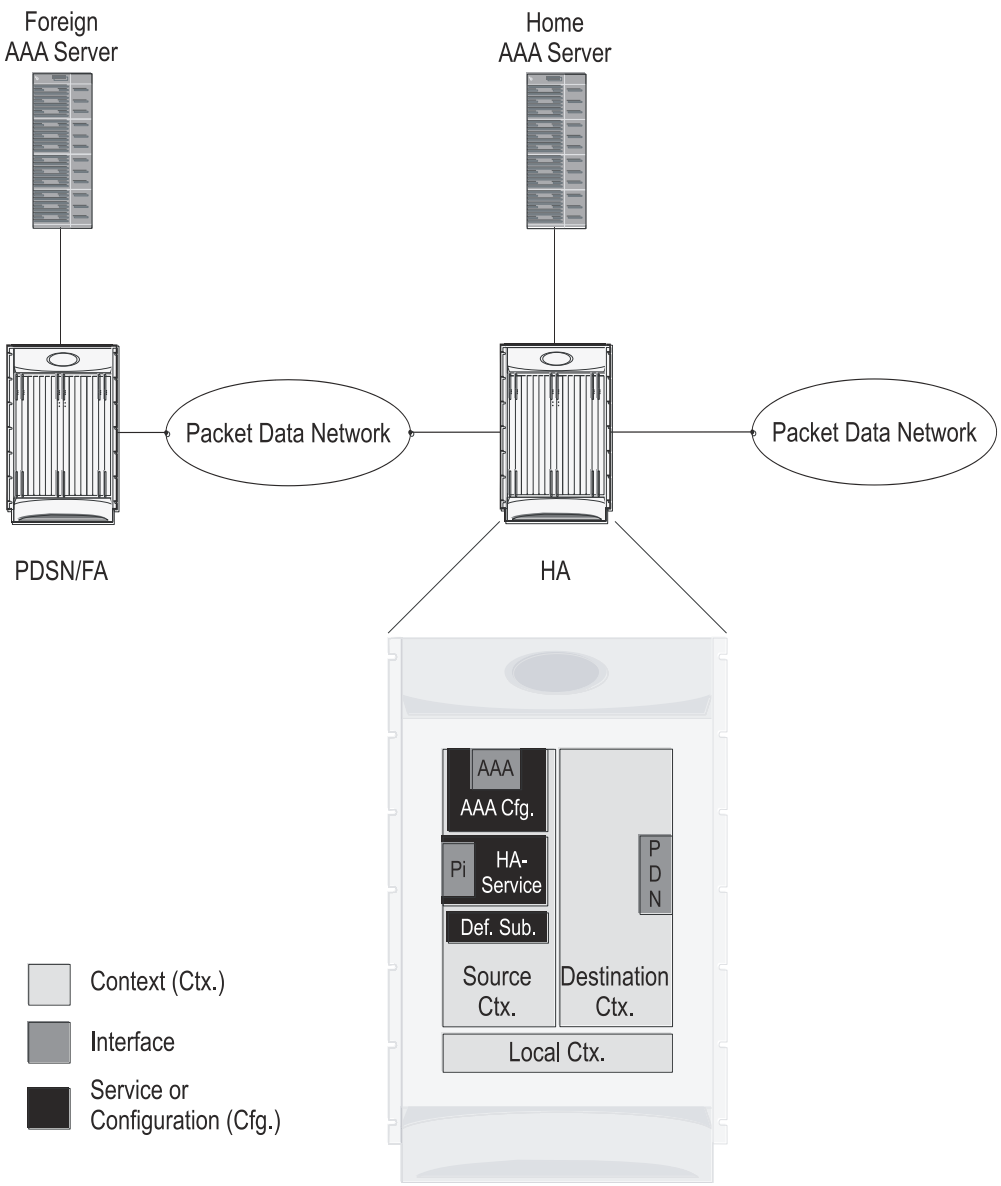
- Example 1: Mobile IP Support Using the System as an HA
- Example 2: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

Example 1: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a PDSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide PDSN/FA functionality.

The system's HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 6. Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Pi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 2. Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. **NOTE:** The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide PDSN/FA functionality.
Pi Interface Configuration	
Pi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Pi interfaces are configured in the destination context. If this interface is being used for Interchassis Session Recovery, you must specify a loopback interface type after the interface_name.
IP address and subnet	These will be assigned to the Pi interfaces.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Pi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Pi interfaces to a specific network.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations.The HA service can be configured as follows: • Always require authentication • Never require authentication (**NOTE:** the initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present

Required Information	Description
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295.Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65534. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured.Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server	IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.

Required Information	Description
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **NOTE:** For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

The following table lists the information required to configure the destination context.

Table 3. Required Information for Destination Context Configuration

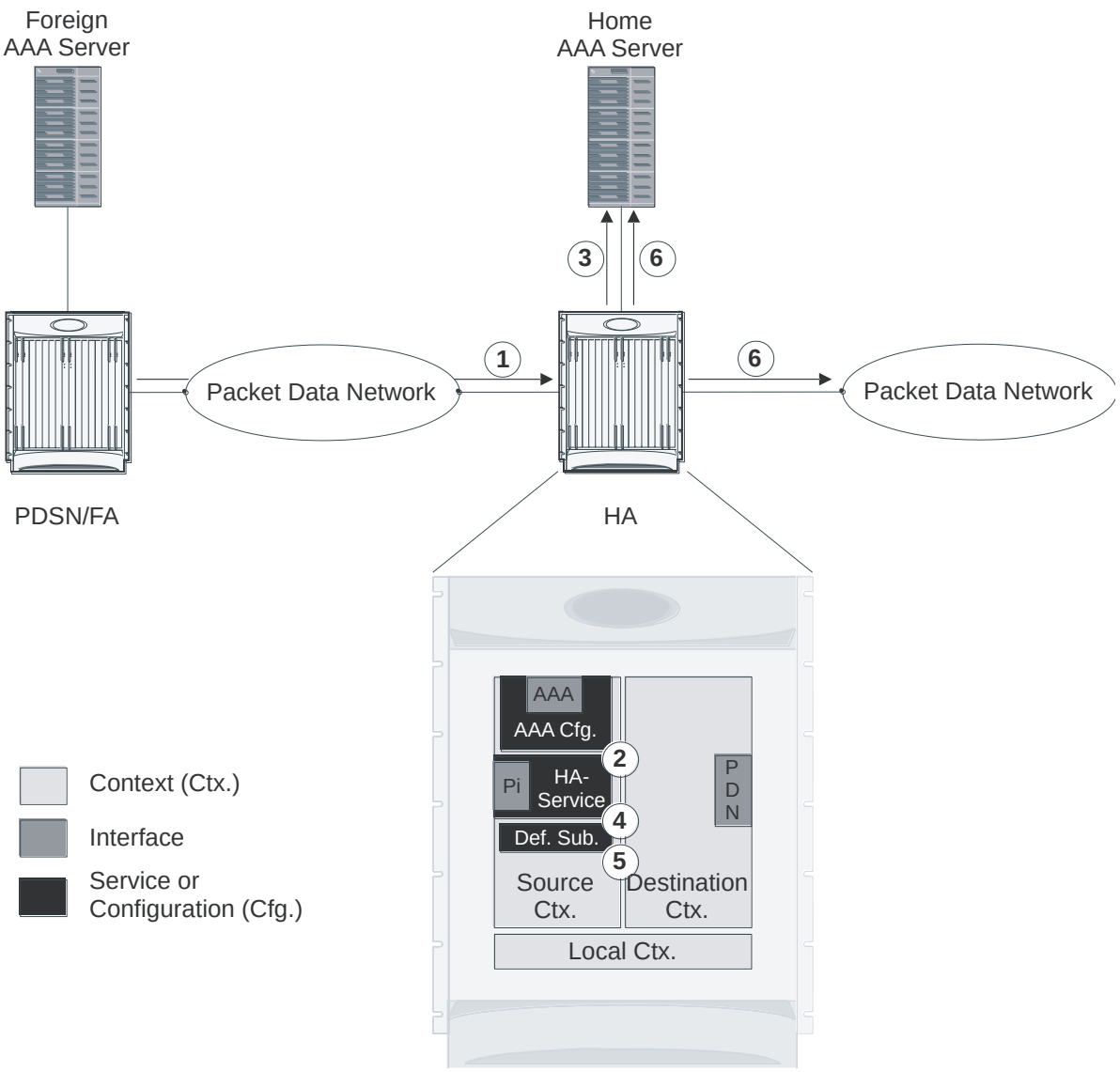
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.**NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	

Required Information	Description
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address.The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 7. Call Processing When Using the system as an HA



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the Source context.
3. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the Source context determines which egress context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

For this example, the system determines that the egress context is the Destination context based on the configuration of the Default subscriber.

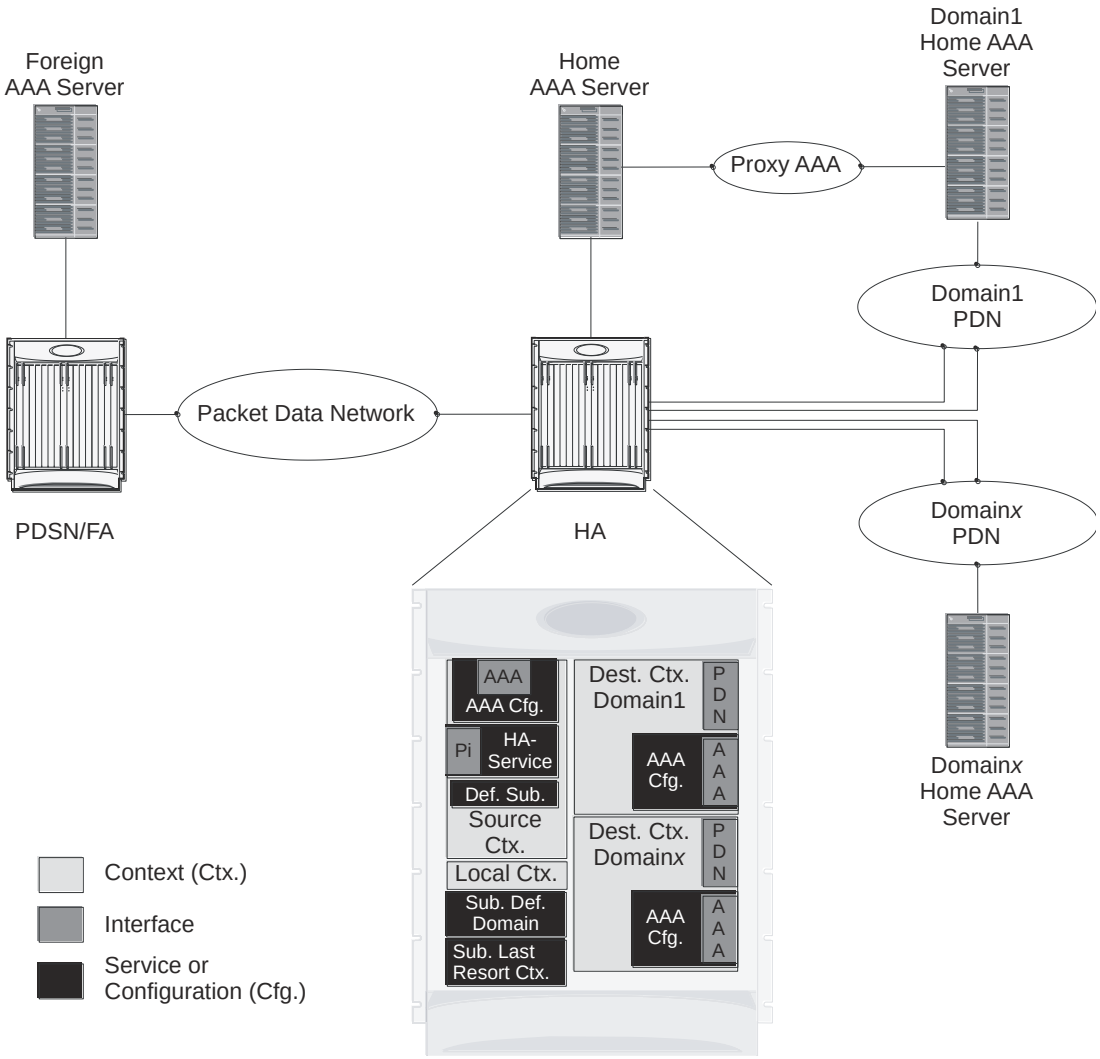
5. An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the Destination context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

Example 2: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could by owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

Figure 8. The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context will facilitate the HA service(s), and the Pi interface(s) to the FA(s).The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 4. Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Pi Interface Configuration	
Pi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Pi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Pi interfaces. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Pi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Pi interfaces to a specific network.
HA service Configuration	

Required Information	Description
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: Always require authentication Never require authentication (**NOTE:** the initial registration and de-registration will still be handled normally) Never look for mn-aaa extension Not require authentication but will authenticate if mn-aaa extension present
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5.A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.

Required Information	Description
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65534. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server	IP Address:Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.

Required Information	Description
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **NOTE:** For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

The following table lists the information required to configure the destination context.

Table 5. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	IP Address: Specifies the IP address of the RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.

Required Information	Description
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server	IP Address:Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary address can be optionally configured.

System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 6. Required Information for System-Level AAA Configuration

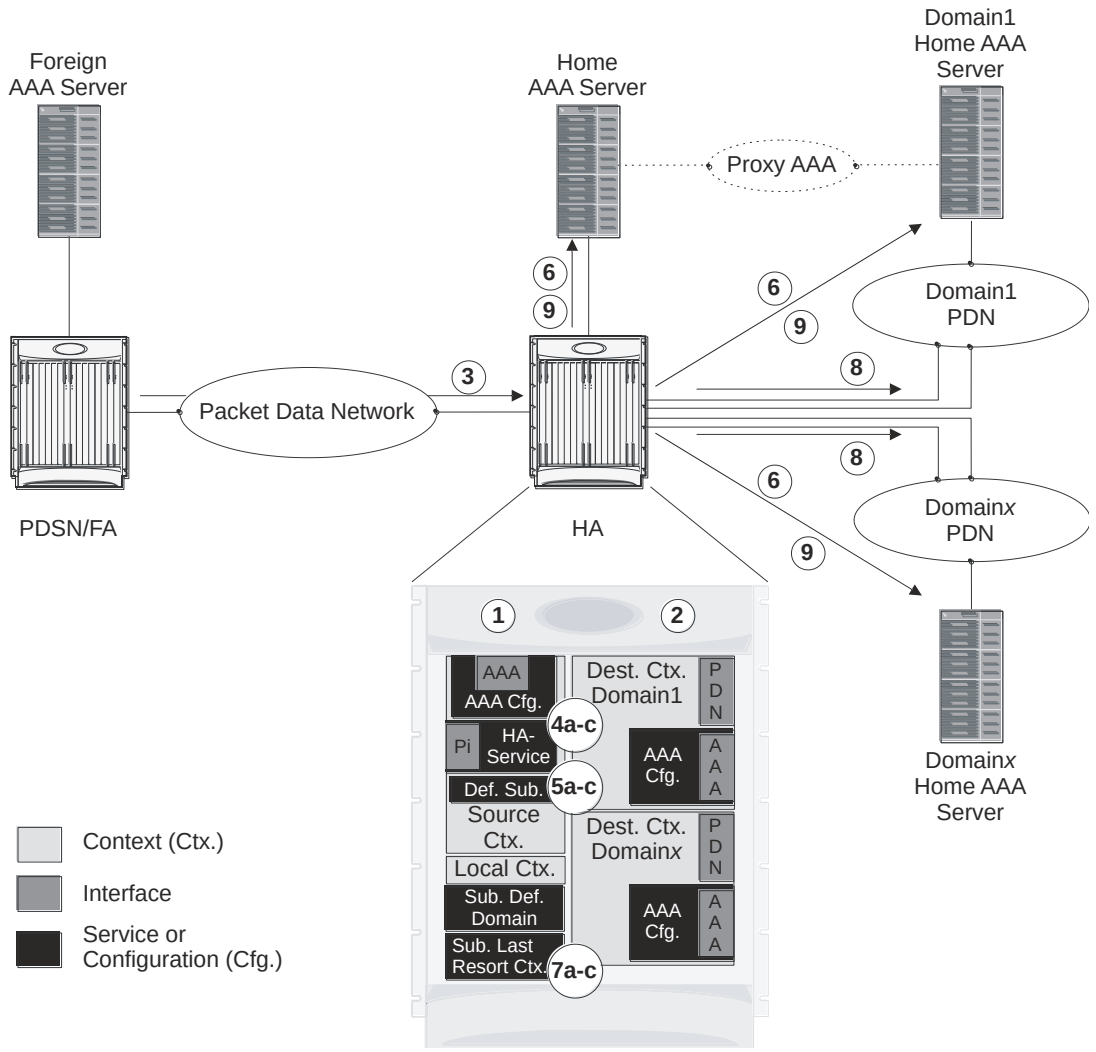
Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **NOTE:** The default domain name can be the same as the source context.
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context. This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. **NOTE:** The last-resort context name can be the same as the source context.

Required Information	Description
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is username @. **NOTE:** The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string , only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string user1@enterprise@isp1, the system resolves to the username user1@enterprise with domain isp1.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 9. Call Processing When Using the system as an HA with a Single Source Context and Multiple Outsourced Destination Contexts



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the Source context.
3. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the Source context determines which egress context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the System Administration Guide.

   For this example, the system determines that the egress context is the Destination context based on the configuration of the Default subscriber.

5. An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the Destination context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

Chapter 3
Simple IP and Mobile IP in a Single System Configuration Example

This chapter provides information for several configuration examples that can be implemented on the system to support Simple IP and Mobile IP data services in a single system.

Important: This chapter does not discuss the configuration of the localout-of-band management context. Information about the localout-of-band management context can be found in Chapter 1 of Command Line Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in the section MIP Timer Considerations

Using the System as Both a PDSN/FA and an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a Packet Data Service Node/Foreign Agent (PDSN/FA) and/or a Home Agent (HA). This example describes what is needed and how a single system simultaneously supports both of these functions.

In order to support PDSN, FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context will facilitate the PDSN service(s), and the R-P interfaces. The AAA context will be configured to provide foreign/home AAA functionality for subscriber sessions and facilitate the AAA interfaces.

The Mobile IP destination context will be configured to facilitate the FA service, the HA service and the PDN interfaces for Mobile IP data services. The Simple IP destination context will facilitate the PDN interfaces for Simple IP data Services.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Figure 10. sipmip_cfg_ex_1a.wmf

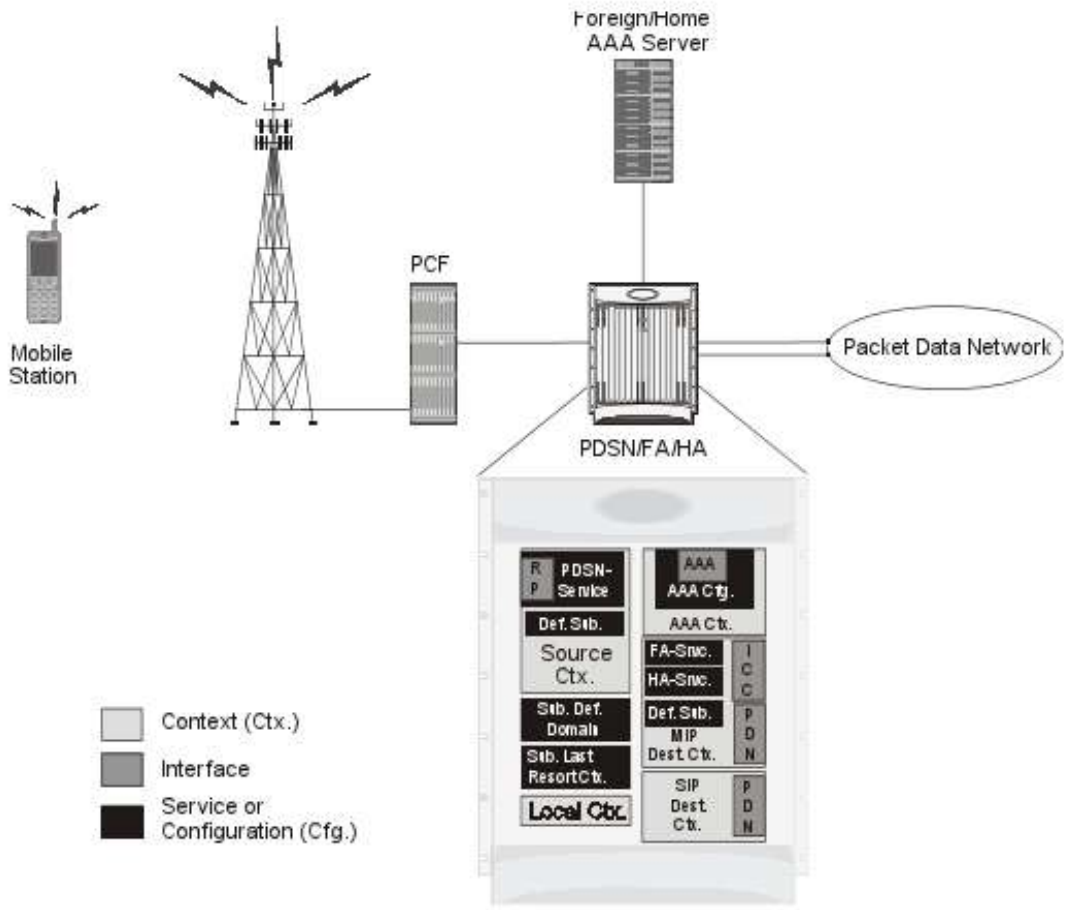


Figure 11. Simple and Mobile IP Support Within a Single System

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the required information to configure the source and destination contexts.

Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 7. Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
R-P Interface Configuration	
R-P interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. R-P interfaces are configured in the source context.
IP address and subnet	These will be assigned to the R-P interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical R-P interfaces.
Gateway IP address	Used when configuring static routes from the R-P interface(s) to a specific network.
PDSN service Configuration	
PDSN service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the PDSN service will be recognized by the system. Multiple names are needed if multiple PDSN services will be used. PDSN services are configured in the source context.
UDP port number for R-P traffic	Specifies the port used by the PDSN service and the PCF for communications. The UDP port number and can be any integer value between 1 and 65535. The default value is 699.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.
Security Parameter Index Information	**PCF IP address:** Specifies the IP address of the PCF that the PDSN service will be communicating with. The PDSN service allows the creation of a security profile that can be associated with a particular PCF. Multiple IP addresses are needed if the PDSN service will be communicating with multiple PCFs.
	Index: Specifies the shared SPI between the PDSN service and a particular PCF. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the PDSN service is to communicate with multiple PCFs.
	Secret: Specifies the shared SPI secret between the PDSN service and the PCF. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.

Required Information	Description
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is MD5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each SPI configured.
Subscriber session lifetime	Specifies the time in seconds that an A10 connection can exist before its registration is considered expired. The time is expressed in seconds and can be configured to any integer value between 1 and 65534, or the timer can be disabled to set an infinite lifetime. The default value is 1800 seconds.
Mobile IP FA context name	Specifies the name of the context in which the FA service is configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **NOTE:** For this configuration, the IP context name should be identical to the name of the destination context.

AAA Context Configuration

The following table lists the information that is required to configure the AAA context.

Table 8. Required Information for AAA Context Configuration

Required Information	Description
AAA context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system.
AAA Interface Configuration	
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign/Home RADIUS Server Configuration	
Foreign/Home RADIUS Authentication server	IP Address: Specifies the IP address of the foreign/home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Foreign/home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign/home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Foreign/Home RADIUS Accounting server	IP Address: Specifies the IP address of the foreign/home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Foreign/home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign/home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the foreign/home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary IP address interface can optionally be configured.

Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the destination context.

Table 9. Required Information for Destination Context Configuration

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
ICC Interface Configuration	
ICC interface name	The intra-context communication (ICC) interface is configured to allow FA and HA services configured within the same context to communicate with each other. The ICC interface name is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. ICC interface(s) are configured in the same destination context as the FA and HA services.
IP address and subnet	These will be assigned to the ICC interface(s). Multiple addresses (at least one per service) on the same subnet will be needed to assign to the same ICC interface.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical ICC interfaces.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	

Required Information	Description
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Security Parameter Index (indices) Information	**HA IP address:** Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.

Required Information	Description
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. **NOTE:** The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: • Always require authentication • Never require authentication (**NOTE:** the initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index:** Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.

Required Information	Description
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is hmac-md5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **NOTE:** For this configuration, the IP context name should be identical to the name of the destination context.

Simple IP Destination Context

The following table lists the information that is required to configure the optional destination context. As discussed previously, This context is only required if Reverse Tunneling is disabled in the FA service.

Table 10. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	

Required Information	Description
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

System-Level AAA Parameter Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 11. Required Information for System-Level AAA Configuration

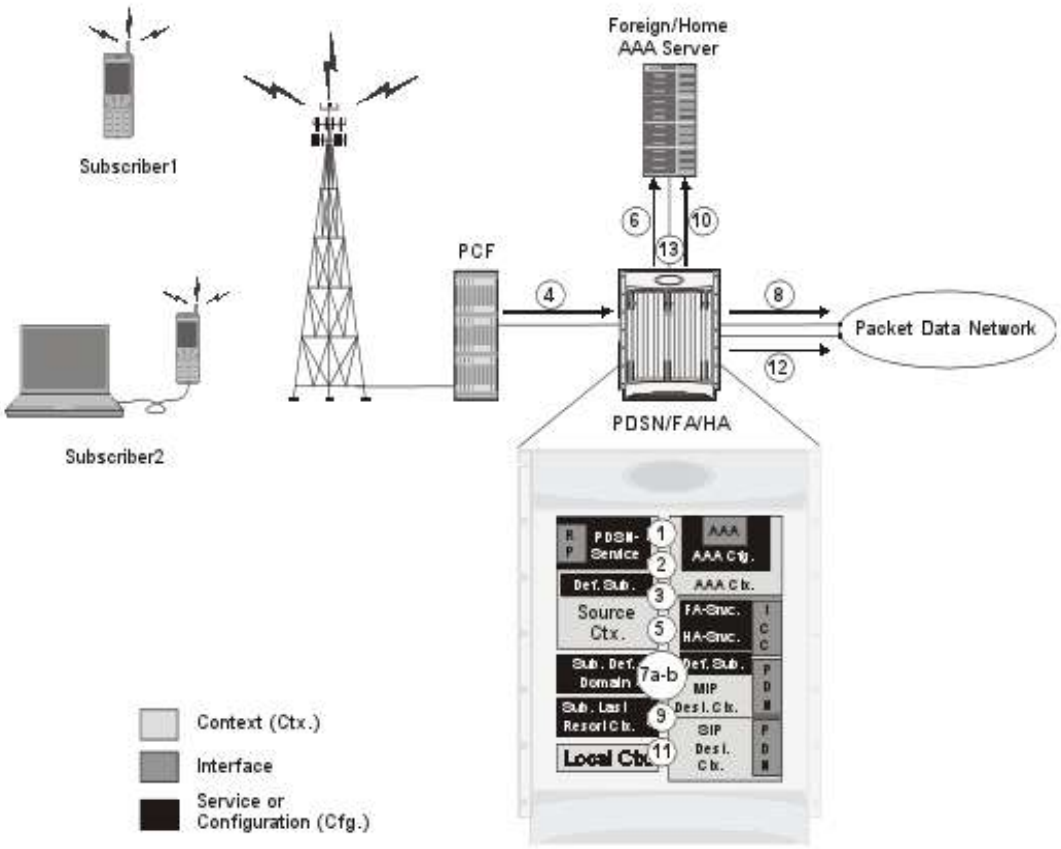
Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **NOTE:** The default domain name can be the same as the source context.

Required Information	Description
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context. This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. **NOTE:** The last-resort context name can be the same as the source context.
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is *username @*. **NOTE:** The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string , only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string *user1@enterprise@isp1*, the system resolves to the username *user1@enterprise* with domain *isp1*.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Simple IP data call.

Figure 12. Call Processing When Using the System as a PDSN, FA, and HA



In this example, *Subscriber1* is establishing a Simple IP data session, while *Subscriber2* is establishing a Mobile IP data session.

1. The system-level AAA settings were configured as follows:
   - Default domain name = *AAA*
   - Subscriber username format = *username @*
   - Last-resort context name = *AAA*
2. The Default Subscriber was configured with an IP context name of *SIP Destination.*
3. The Mobile IP FA context name parameter within the PDSN service was configured to the *MIP Destination* context.
4. Sessions for *Subscriber1* and *Subscriber2* are received by the PDSN service over the R-P interface from the PCF.
5. The PDSN service determines which context to use to provide foreign AAA functionality for each session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*.

For this configuration, the result of this process for both *Subscriber1* and *Subscriber2* would be that the system determines that AAA functionality should be provided by the *AAA* context.

6. The system would then communicate with the AAA server specified in the *AAA* context's AAA configuration to authenticate the subscribers.
7. Upon successful authentication, the PDSN service will take the following actions for *Subscriber1* and *Subscriber2*:
   - *Subscriber1*: The system will go through the process of determining which destination context to use for the subscriber session. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*. For this configuration, the system determines that the egress context is the *SIP Destination* context based on the configuration of the *Default* subscriber in the *Source* context.
   - *Subscriber2*: The system uses the Mobile IP FA context name configured within the PDSN service to determine what destination context facilitates the FA service. In this example, it determines that it must use the *MIP Destination* context and it passes the HA IP address to the FA service.
8. For *Subscriber1's session*, data traffic would then be routed through the PDN interface in the *SIP Destination* context.
9. For *Subscriber2*, the FA service then establishes a connection to the specified HA service through the ICC interface.
10. For *Subscriber2*, the system would then communicate with the AAA server specified in the *AAA* context's AAA configuration to authenticate the subscriber.
11. For *Subscriber2*, upon successful authentication, the *MIP Destination* context determines which destination context to use for the session and Mobile IP registration would be completed. This process is described in the How the System Selects Contexts section located in the Understanding the System Operation and Configuration chapter of the *System Administration Guide*.

    For this example, the *Source* context determines that the egress context is the *MIP Destination* context based on the configuration of the *Default* subscriber.
12. For *Subscriber2's session*, data traffic would then be routed through the PDN interface in the *MIP Destination* context.
13. Accounting messages for both sessions would be sent to the AAA server over the AAA interface in the *AAA* context.

Chapter 4
Service Configuration Procedures

This chapter is intended to be used in conjunction with the previous chapters that provide examples for configuring the system to support Simple IP services, Mobile IP services, or both. It provides procedures for configuring the various elements to support these services.

It is recommended that you first select the configuration example that best meets your service model, and then use the procedures in this chapter to configure the required elements for that model.

Procedures are provided for the following:

- Creating and Configuring HA Services
- Session Continuity Support
- Hybrid HA Service Configuration
- WiMAX-3GPP2 Interworking at HA

Creating and Configuring HA Services

HA services are configured within contexts and allow the system to function as an HA in the 3G wireless data network.

To create and configure an HA service:

Step 1 Create and configure an HA service as described the Creating and Configuring an HA Service section.

Step 2 Verify your configuration as described in the Verifying HA Service Configuration section.

Step 3 Save your configuration as described in the Saving Your Configuration chapter.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in the MIP Timer Considerations appendix.

Creating and Configuring an HA Service

Use the following example to configure HA services:

```
configure
   context <ha_context_name>
      ha-service <ha_service_name>
         ip local-port <port_number>
         authentication mn-aaa { allow-noauth | always | dereg-noauth | noauth |
renew-and-dereg-noauth | renew-reg-noauth }
         fa-ha-spi remote-address <fa_ip_address> spi-number <number> { encrypted
secret <enc_secret> | secret <secret> } [ description <string> ] [ hash-
algorithm { hmac-md5 | md5 | rfc2002-md5 } ]
         mn-ha-spi spi-number <number> [ description <string> ] { encrypted
secret <enc_secret> | secret <secret> } [ hash-algorithm { hmac-md5 | md5 |
rfc2002-md5 } ] [ permit-any-hash-algorithm ] [ replay-protection { nonce |
timestamp } [ timestamp-tolerance <tolerance> ]
         reg-lifetime <lifetime>
         simul-bindings <simul_bindings>
         bind address <address> max-subscribers <max_subs>
```

```
end
```

Notes:

- *<port_number>* must be the UDP port for the Pi interfaces' IP socket.
- A maximum of 2048 FA-HA Security Parameter Index (SPI) can be configured for each HA service.
- *<lifetime>* must the longest registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured using the **no reg-lifetime** command.
- Option: To configure the HA service for controlling the negotiation and sending of the I-bit in revocation messages, in the HA Service Configuration Mode, enter the following comand. By default, HA will not send I-bit in revocation message. **revocation negotiate-i-bit**
- Use the bind address command to bind the service to the Pi interface and specify the maximum number of subscribers that can access the service. The hardware configuration and features installed can affect the maximum subscriber sessions that can be supported.
- Option: To set the maximum period of time to set up a session, in the HA Service Configuration Mode, enter the following command: **setup-timeout** *<seconds>*
- Create and bind additional HA services to any other interfaces as required.

Verifying HA Service Configuration

Verify that your HA services were created and configured properly by entering the following command:

```
show ha-service { name service_name | all }
```

The output is a concise listing of HA service parameter settings similar to the following sample. In this sample, an HA service named ha1 was configured.

```
Service name: ha1
 Context: ha
 Bind: Done Max Subscribers: 500000
 Local IP Address: 192.168.4.10 Local IP Port: 434
 Lifetime: 00h01m40s Simul Bindings: 3
 Reverse Tunnel: Enabled
 GRE Encapsulation with-key: Enabled Keyless GRE Encapsulation: Disabled
 Optimize Tunnel Reassembly: Enabled Setup Timeout: 60 sec
 Allow Priv Addr w/o Rev Tunnel: Disabled
```

```
 WIMAX-3GPP2 Interworking: Disabled SPI(s): MNHA: Remote Addr: 0.0.0.0
Description: Hash Algorithm: HMAC_MD5 SPI Num: 258 Replay Protection:
Nonce Timestamp Tolerance: 100

 Permit Any Hash Algorithm: Enabled

 FAHA: Remote Addr: 195.20.20.6/32 Description: Hash Algorithm: HMAC_MD5
SPI Num: 258 Replay Protection: Timestamp Timestamp Tolerance: 60

 'S' Lifetime Skew: 00h00m10s

 IPSEC AAA Context: aaa_context

 GRE Sequence Numbers: Disabled GRE Sequence Mode: None

 GRE Reorder Timeout: 100 msec

 GRE Checksum: Disabled GRE Checksum Verification: Disabled

 Registration Revocation: Disabled Reg-Revocation I Bit: Enabled

 Reg-Revocation Max Retries: 3 Reg-Revocation Timeout: 3 (secs)

 Reg-Rev Handoff old-FA: Enabled Reg-Rev Idle-Timeout: Enabled

 Send NAI Extension in Reg-Revocation: Disabled

 MIP NAT Traversal: Disabled Force UDP Tunnel: Enabled

 Default Subscriber: None

 Max Sessions: 500000

 Service Status: Started

 MN-AAA Auth Policy: Always

 MN-HA Auth Policy: Always

 IMSI Auth: Disabled

 DMU Refresh Key: Disabled

 AAA Distributed MIP Keys:Disabled

 AAA accounting: Enabled

 Idle Timeout Mode: Aggressive

 Newcall Policy: None

 Overload Policy: Reject (Reject code: Admin Prohibited)

 NW-Reachability Policy: Reject (Reject code: Admin Prohibited)

 Null-username Policy: Reject
```

```
BC Rsp Code for Nw Fail: 0xffff

IP Pool/Group:

Name: n/a

Destination Context: n/a
```

Session Continuity Support

This section describes the procedure to enable the mobility for WiMAX subscriber and other access technology subscribers; i.e. 3GPP2. WiMAX HA implementation differs from 3GPP2 on the keys used to authenticate MN-HA and FA-HA AE in MIP RRQ. WiMAX HA involves using dynamic keys distributed by AAA for authenticating RRQ.

Following WiMAX support is provided for MIP keys management and WiMAX HA support:

- MIPv4 support
- Managing MIP Key distribution from AAA
- Registration Revocation
- MIPv4 RRQ with NAI extension
- Support of GRE key extension of CVSE in RRP
- MIPv4 Registration

For MIP registration HA uses the following extensions:

- MN-NAI Extension
- MN-HA AE
- Revocation Support Extension
- FA-HA AE

The MIP client includes the same NAI in all MIP RRQs it sends for the entire duration of the MIP session regardless of EAP re-authentication, including MIP renewal and de-registration messages. The MN-HA and FA-HA keys based on WiMAX VSA from AAA is used to authenticate the RRQ and compute authenticator in RRP.

Authentication algorithm used to authenticate MN-HA and FA-HA AE is HMAC-MD5. If renew/dereg RRQ is received, authentication with AAA will happen only if SPI value for authentication extension in RRQ changes. If SPI returned by AAA is different from the requested one, the RRQ will be rejected. Both MN-HA and FA-HA AE are expected in MIP RRQ for WiMAX calls.

The following describes the processing of different requests for HA support:

- Processing Access-Request: When initial MIP RRQ is received, HA authenticates with AAA to get the MIP Keys (MN-HA and HA-RK) required to authenticate MIP RRQ.
- Processing Access-Accept: In the Access Accept, MIP Keys MN-HA and HA-RK (if requested) is received. MN-HA key is maintained for each subscriber session and FA-HA key is computed based on HA-RK maintained per HA.

All the attributes (HA-RK-KEY, HA-RK-SPI, and HA-RK-Lifetime) must be returned if HA-RK key is requested for the HA-RK info in Access Accept to be valid.

Message Authenticator will be included in Access request and Accept packets for integrity protection of RADIUS packets and is mandatory.

- MIPv4 Revocation: MIP Revocation is supported as per RFC 3543 and it uses FA-HA keys fetched dynamically from AAA during MIP registration.

Apart from these processing, HA provides following function applicable to WiMAX HA.

- Functional Level Description: HA retrieves the MIP Keys dynamically from AAA to authenticate the RRQ.
- Authentication of MIP RRQ in WiMAX HA: When a MIP RRQ is received HA authenticates the user with AAA for both P-MIP and C-MIP call to get the MIP Keys.

The MN-HA and FA-HA keys will be used to authenticate the RRQ.

Hybrid HA Service Configuration

With this support an HA can work in a “hybrid” mode, meaning the same HA can handle a call from CDMA network, a call from WIMAX network, and a “hybrid call” with RRQ coming from one network and later from another network. This way, the operator can just deploy one HA service to support both types of network, instead of using two separate HA services. The HA is aware of the access technology, and choose the correct authentication method to handle RRQ.

This section describes the following configuration procedures:

- Configuring WiMAX HA for WiMAX Calls only
- Configuring WiMAX HA to Accept 3GPP2Static MIP Key
- Configuring Hybrid HA for WiMAX and 3GPP2 Calls

> ***Important:*** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

Configuring WiMAX HA for WiMAX Calls only

With this configuration the system will support only WiMAX HA behavior for the particular HA-service, where the system always expects WiMAX MIP keys from AAA and use it to do MN-HA and FA-HA authentication extension. With this configuration HA cannot support calls with static keys for MIP RRQ authentication in the particular HA service.

To configure WiMAX HA for WiMAX calls only:

Step 1 Configure WiMAX HA for WiMAX calls only as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to configure WiMAX HA services, and enable the usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with keys mandatory.

```
configure
   context <ha_context_name>
      ha-service <ha_service_name>
         authentication aaa-distributed-mip-keys required
         end
```

Configuring WiMAX HA to Accept 3GPP2/Static MIP Key

To configure WiMAX HA to accept 3GPP2/Static MIP key:

Step 1 Configure WiMAX HA to accept 3GPP2/Static MIP key as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to configure HA services to accept 3GPP2 calls and disable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ.

```
configure
   context <ha_context_name>
      ha-service <ha_service_name>
         authentication aaa-distributed-mip-keys disabled
         end
```

Configuring Hybrid HA for WiMAX and 3GPP2 Calls

With this configuration, both WiMAX and 3GPP2 based calls can be made where WiMAX based calls will use WiMAX MIP keys, and 3GPP2 calls can use static or 3GPP2 based dynamic keys. This particular HA service configuration supports calls of both access technologies.

To configure Hybrid HA for WiMAX and 3GPP2 calls:

Step 1 Configure Hybrid HA to accept WiMAX and 3GPP2 calls in the same service as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to configure HA services to accept WiMAX and 3GPP2 calls in the same service, and enable usage of AAA provided WiMAX MIP keys for authenticating MIP RRQ with fallback option to use 3GPP2/static keys:

```
configure
   context <ha_context_name>
      ha-service <ha_service_name>
         authentication aaa-distributed-mip-keys optional
```

```
wimax-3gpp2 interworking
end
```

WiMAX-3GPP2 Interworking at HA

The session continuity capability enables a dual mode device (a multi radio device) to continue its active data session as it changes its active network attachment from 3GPP2 to Wimax and vice versa with no perceived user impacts from a user experience perspective.

This capability provides the following benefits:

- common billing and customer care
- accessing home 3GPP2 service through Wimax network and vice versa
- better user experience with seamless session continuity

To provide this capability, the HA supports seamless handoff from 3GPP2 to WIMAX and vice versa.

This section describes the key configuration to enable this capability.

Mobile Node Requirement

Following are the mandatory functional requirements on mobile node to support 3GPP2-WIMAX Interworking at HA:

- The dual mode MS SHOULD use PMIP to access WIMIAX network and use CMIP to access 3GPP2 network.
- The static NAI (the NAI that is pre-provisioned for access to 3GPP2) has to be used in RRQ on both 3GPP2 and WiMAX networks.
- The dual mode MS SHOULD support “make-before-break” when changing between 3GPP2 and WiMAX networks, if coverage is available on both networks.
- The CMIP4 RRQ message used on 3GPP2 network MUST contain the MN-AAA and Foreign Agent Challenge Extension (FACE)

H-AAA Requirements

H-AAA MUST meets the following requirements to support 3GPP2-WIMAX Interworking at HA:

- The H-AAA servers used by 3GPP2 and WIMAX SHOULD be either the same or they have access to the same session state and subscriber profile.
- H-AAA server SHOULD assign and return the same HA address in response to 3GPP2 and WIMAX network access request

FA and HA Function for 3GPP-WiMAX Interworking at HA

The FA and PMIP4 client provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- For WiMAX access, the PMIP4 Client will NOT include MN-AAA AE in the RRQ.
- For 3GPP2 access, the FA will NOT remove the MN-AAA AE from the RRQ. This requirement stands even if the cdma2000 AAA sends the MN-AAA Removal Indication VSA with its value set.

The HA provides following functionality to support 3GPP2-WIMAX Interworking at HA:

- The HA recognizes the difference between 3GPP2 and WiMAX access technologies based on the presence or absence of MN-FA and MN-AAA AE. If the MN-FA and MN-AAA are present in the RRQ, the HA assumes that the RRQ is coming through a 3GPP2 network. Otherwise, the HA assumes that the RRQ is coming through a WiMAX network.
- The HA updates mobility bindings for different access technology types while maintaining binding integrity (binding continues to be active until updated).
- The same HA is able to handle packets from the MS with a given Care-of Address when the mobility binding is pointing to a different Care-of Address. This is to mitigate packet loss in the uplink during seamless mobility across access technologies.

Before configuring the 3GPP-WiMAX Interworking the following must be taken into consideration:

- Separate FA service is used for 3GPP2 and WIMAX network.
- The subscriber MUST be authorized to use PMIP for WIMAX access.
- The subscriber MUST use CMIP to access 3GPP2 network and MUST NOT set s-bit in RRQ.


Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

Configuring WiMAX FA Service

To configure WiMAX FA service:

Step 1 Configure WiMAX FA service as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to configure WiMAX FA service:

```
configure
```

```
context <context_name>
   fa-service <fa_service_name>
      authentication aaa-distributed-mip-keys override
      revocation negotiate-i-bit
      end
```

Configuring 3GPP2 FA Service

To configure 3GPP2 FA service:

Step 1 Configure 3GPP2 FA service as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to create and configure 3GPP2 FA service:

```
configure
   context <context_name>
      fa-service <fa_service_name>
         default mn-aaa-removal-indication
         revocation negotiate-i-bit
         end
```

Configuring Common HA Service

To configure common HA service:

Step 1 Configure common HA service as described in this section.

Step 2 Save your configuration as described in the Saving Your Configuration chapter.

Use the following example to configure common HA service:

```
configure
   context <ha_context_name>
      ha-service <ha_service_name>
```

```
authentication aaa-distributed-mip-keys required
wimax-3gpp2 interworking
authentication mn-aaa allow-noauth
revocation negotiate-i-bit
end
```

Chapter 5
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##################################################################################

Displaying Global
AAA-configuration errors
##################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

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

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices.This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

`save configuration` *`tftp://config_server/init_config.cfg`*

Chapter 6
Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference Guide* for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the *Counters and Statistics Reference.*


Important: Not all Show commands are available for all platforms and licenses.

Table 12. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View HA Manager statistics	**show session subsystem facility hamgr all**
View Mobile IP Home Agent Statistics	
Display Mobile IP HA Information for a Specific Subscriber	
View Mobile IP HA information and counters for a specific subscriber	**show mipha full username** *subscriber_name*
Display Mobile IP Statistics for HA Services	
View Mobile IP statistics for a specific HA service	**show mipha statistics ha-service** *service_name*
Display Mobile IP HA Counters	
View Mobile IP HA counters for individual subscriber sessions	**show mipha counters**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to *Command Line Reference* for detailed information on using this command.

Chapter 7
Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

Interface and Port Rules

The rules discussed in this section pertain to both the Ethernet 10/100, the Ethernet 1000 Line Card and the four-port Quad Gigabit Ethernet Line Card, known as the Quad Gig-E or QGLC and the type of interfaces they facilitate, regardless of the application.

Pi Interface Rules

HA to FA

The following engineering rules apply to the Pi interface between the HA and FA:

- When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA or both. This section describes the engineering rules for the Pi interface when using the system as an HA.
- A Pi interface is created once the IP address of a logical interface is bound to an HA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within an ingress context.
- HA services must be configured within an ingress context.
- If the system configured as an HA is communicating with a system configured as a FA, then it is recommended that the name of the context in which the HA service is configured is identical to the name of the context that the FA service is configured in on the other system.
- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the HA service to allow communications with multiple FAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Each HA service must be configured with a Security Parameter Index (SPI) that it will share with mobile nodes.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited in order to allow higher bandwidth per subscriber.

Subscriber Rules

The following engineering rule applies to subscribers configured within the system:

Default subscriber templates may be configured on a per HA service.

Service Rules

The following engineering rules apply to services configured within the system:

Important: Given capacities do not apply to the XT2 platform.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- A maximum of 256 services (regardless of type) can be configured per system.
- Up to 2,048 MN-HA and 2048 FA-HA SPIs can be supported for a single HA service.
- Up to 2,048 FA-HA SPIs can be supported for a single FA service.
- The system supports unlimited peer FA addresses per HA.
    - The system maintains statistics for a maximum of 8192 peer FAs per HA service.
    - If more than 8192 FAs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer HAs per FA service.
- There are a maximum of 8 HA assignment tables per context and per chassis.
- The total number of entries per table and per chassis is limited to 256.

Chapter 8
Supported Registration Reply Codes

The following section describes the registration reply codes supported by the system for the HA service.

HA Service Reply Codes

The following registration reply codes are supported by the system's HA service in accordance with the following Request For Comments (RFCs):

- RFC-2002, IPv4 Mobility, May 1995
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998

Table 13. Supported HA Service Registration Reply Codes

Reply Code (Hex / Base 10)	Description	Note
80H / 128	Registration Denied - reason unspecified	Sent when internal errors are encountered when processing the Request packet.
81H / 129	Registration Denied - administratively prohibited	Sent when a newcall policy is set to reject calls or the subscriber is not permitted to use Mobile IP HA services.
82H / 130	Registration Denied - insufficient resources	Sent when no memory or session managers are available to process the session.
83H / 131	Registration Denied - mobile node failed authentication	Sent when the mobile node failed authentication.
84H / 132	Registration Denied - foreign agent failed authentication	Sent when an FA attempted to communicate with the HA service using an incorrect security parameter index (SPI).
85H / 133	Registration Denied - registration Identification mismatch	Sent when the ID sent by the mobile node in the RRQ is different from the expected value.
86H / 134	Registration Denied - poorly formed request	Sent when the registration request is poorly formed (i.e. missing an Authentication extension).
87H / 135	Registration Denied - too many simultaneous mobility bindings	Sent when the mobile node has exceeded the maximum number of mobile bindings that the HA service supports for a single subscriber.
88H / 136	Registration Denied - unknown home agent address	Sent when HA redirect policy is invoked.
89H / 137	Registration Denied - reverse tunneling unavailable	Sent when reverse tunneling is requested by the mobile node but it is not enabled on the system.
8AH / 138	Registration Denied - reverse tunneling mandatory	Sent when reverse tunneling is enabled on the system but is not supported by the mobile node.
8BH / 139	Registration Denied - reverse tunneling encapsulation style unavailable	Sent if the Encapsulating Delivery Style Extension sent by the mobile is not supported by the HA service.

Reply Code (Hex / Base 10)	Description	Note
8DH / 141	Registration Denied - unsupported Vendor-ID or unable to interpret Vendor-CVSE-Type.	Sent if the Vendor Identification is unsupported or the HA is unable to interpret the Vendor-CVSE-Type in the CVSE sent by the Foreign Agent to the Home Agent.
8EH/142	Registration Denied - Requested UDP tunnel encapsulation unavailable	Sent by the HA if a UDP tunneling mode is not available.

Chapter 9
Mobile-IP and Proxy-MIP Timer Considerations

This appendix is intended to provide a brief explanation of the considerations for lifetime, idle, and absolute timer settings that must be understood when setting up a system in a Mobile-IP or Proxy-MIP environment. The focus of the document is to understand the call flow and understand the timer values that must be applied to make the system function in the most efficient manner.

Call Flow Summary

Important: Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

The following steps describe the call flow as regards the timers that affect a call initiated by the Mobile Node (MN).

1. The call arrives at the system and A11 (or L2TP, for Closed RP interfaces) (or L2TP, for Closed RP interfaces) is processed successfully. The call arrives at the system and R6 isThe call arrives at the system and R6 is processed successfully.The GGSN receives a Create PDP Context Request Message
2. PPP negotiation is started. At this point,PPP negotiation is started. At this point, since authentication is not performed the system does not have a username or password. So during the PPP phase, the system selects the default subscriber in the source context for a subscriber template (DNS, and timer settings can be configured in the default subscriber template). Once PPP is successfully established the system understands that the call is a Mobile IP call. since authentication is not performed the system does not have a username or password. So during the PPP phase, the system selects the default subscriber in the source context for a subscriber template (DNS, and timer settings can be configured in the default subscriber template). Once PPP is successfully established the system understands that the call is a Mobile IP call.The system determines the propertiesThe system determines the properties
3. The new RRQ is accepted by the FA and sent to the HA. The HA authenticates the user and compares the requested lifetime to the configured MIP lifetime in the HA-service and the subscriber idle and absolute timeouts. If the MIP lifetime is lower it is be sent back to the mobile; if the MIP lifetime is higher the system sends back an RRQ accept with the lifetime set to 5 seconds less than the lower of the idle or absolute timeout for the user.

   The following CLI command sequence is used to configure the Mobile IP reg-lifetime in the HA service:

```
configure
   context <host_name>
      ha-service <ha_service_name>
         reg-lifetime <value>
         end
```

Timer Values and Recommendations

The following table shows values that would be populated under a number of different configured scenarios.

Table 14. Sample Call Flow Timer Scenarios

Scenario	1	2	3	4	5	6	7
Mobile Sub. MIP Lifetime	600	600	600	600	600	600	600
Source Context Default Sub-Source Context Default Sub-Absolute	300	300	300	300	300	300	300
Source Context Default Sub-Source Context Default Sub-Idle	300	300	300	300	300	300	300
FA-Service Advertise Reg-Lifetime	400	400	400	400	400	400	400
Mobile Sub. Profile AAA Context Timeout idle	500	500	500	500	500	500	500
HA-Service MIP Lifetime	400	400	400	400	400	400	400
Agent Advertisement Reg-Lifetime	295	295	295	295	295	295	295
Mobile Sub. MIP RRQ requested lifetime	295	295	295	295	295	295	295
FA MIP RRP Lifetime	295	295	295	295	295	295	295
FA MIP RRP	success	success	success	success	success	success	Lifetime too long

Based on the table above, the recommended guidelines are as follows:

- If you are going to use timeout idle settings for subscribers, it is recommended that you configure the timeout idle parameter in the source context default subscriber to a value that is less than or equal to the lowest timeout idle for any subscriber.
- If you are going to use timeout absolute settings for subscribers, it is recommended that you configure the timeout absolute in the source context default subscriber to a value that is less than or equal to the lowest timeout idle for any subscriber.

Failure to follow these recommendations could result in lifetime too long failures when the FA processes the subscriber profileAPN template and finds an idle timeout that is less than the proposed MIP lifetime in the mobile RRQ.

Controlling the Mobile IP Lifetime on a Per-Domain Basis

The system does not support the configuration of the MIP lifetime timer on per- domain (context) basis. However, a domain-wide lifetime timer can be achieved by configuring the idle-timeout attribute for the default subscriber for each domain.

Important: Mobile IP lifetime settings can be controlled on a per-domain basis **only** in deployments for which the idle timeout attribute for individual subscriber profiles is **not** used during operation.

In this configuration, the value of the registration lifetime sent by the system in Agent Advertisements is selected by comparing the configured FA Agent Advertisement lifetime setting, and the idle and/or absolute timeout settings configured for the domain's default subscriber. If the value of the idle and/or absolute timeout parameter is less than the Agent Advertisement lifetime, then the system provides a registration lifetime equal to 5 seconds less than the lowest timer value.

If the idle timeout attribute is configured in individual subscriber profiles, per-domain lifetime control is not possible. In this case, the registration lifetime configured for the FA must be the lower of the two values.

Important: Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

The following is an example CLI command sequence used to configure the Mobile IP lifetime on a per-domain basis.

```
configure
   context <aaa_context_name>
      subscriber default
         ip context-name <abc>
         exit
      subscriber name <ptt.bigco.com>
         timeout idle <3605>
         ip context-name <abc>
         exit
      subscriber name <bigco.com>
         timeout idle <7205>
         ip context-name <abc>
         exit
```

```
      domain <ptt.bigco.com> default subscriber <ptt.bigco.com>
      domain <bigco.com> default subscriber <bigco.com>
         end
configure
   context <ha_context_name>
      subscriber default
      exit   ha-service <ha>
      idle-timeout-mode normal      reg-lifetime <7200>
      end
configure
   context <fa_context_name>
      fa-service <fa>
         advertise reg-lifetime <7200>
         end
```

In the example above, two domains (ptt.bigco.com and bigco.com) are configured. The default subscribers are defined for the two domains respectively. The desired operation requires a Mobile IP lifetime of 1 hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of 2 hours (7200 secs) for the bigco.com domain.

Whenever a subscriber session belonging to the ptt.bigco.com domain arrives, the system uses a Mobile IP lifetime timer value equal to 5 seconds less than the idle timeout configured for the default subscriber because the configured value is less than the registration lifetime value configured for the Agent Advertisement. 5 seconds less than the configured value of 3605 seconds equals 3600 seconds which meets the desired operation.

Whenever a subscriber session belonging to the bigco.com domain arrives, the system uses the configured registration lifetime value as the Mobile IP lifetime in Agent Advertisements because it is less than the configured idle timeout in the default subscriber's profile.

As a general rule, the registration lifetime value on the agent **must** be configured as the highest Mobile IP lifetime that is desired for a subscriber. (In the above example, it would be the subscriber bigco.com.)

Another important factor to consider is that the idle timeout value should be reset on receipt of a renewal request. To support this operation, the system provides the **idle-timeout-mode** configurable in the HA service. The following modes are supported:

- **normal**: Resets the idle timeout value on receipt of Mobile IP user data and control signaling
- **aggressive**: Resets the idle timeout value on receipt of Mobile IP user data only (this is the default behavior)
- **handoff**: Resets the idle timeout value on receipt of Mobile IP user dataand upon inter-AGW handoff

The following optional modifier is also supported:

- **upstream-only**: Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.