



Cisco ASR 5000 Series Access Service Network Gateway Administration Guide 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-22953-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Access Service Network Gateway Administration Guide

© 2010 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide	ix
Conventions Used.....	x
Contacting Customer Support	xii
ASN Gateway Overview.....	13
ASN Mobility Management	14
EAP User Authentication	15
ASN Gateway and AAA	15
Profile Management	15
Inter-ASN Handovers	16
Supported Features	17
Simple IPv4 Support.....	17
DHCP Proxy Server.....	17
ASN Gateway Micro-Mobility	18
Uncontrolled Handovers	18
Controlled Handovers	18
WiMAX R4 Inter-ASN Mobility Management.....	19
WiMAX R3 CSN Anchored Mobility Management	19
Proxy Mobile IPv4 (PMIPv4).....	19
Client Mobile IPv4 (CMIPv4)	20
Authenticator	20
EAP Authentication Methods	20
Supported RADIUS Methods	21
Supported Diameter Methods	21
WiMAX Prepaid Accounting	22
Volume and Duration-based Prepaid Accounting.....	22
Supported Enhanced Features.....	23
Lawful Intercept Enhancements.....	23
Intelligent Traffic Control.....	23
Hotlining/Dynamic RADIUS Attributes.....	23
Multi-flow QoS.....	24
ASN Gateway Intra-Chassis Session Recovery	25
Supported Inline Services	25
Enhanced Charging Service	25
Multi-host Support.....	26
How it Works.....	26
ASN Gateway in a WiMAX Network.....	28
Access Service Network (ASN)	29
Connectivity Service Network (CSN)	30
WiMAX Reference Points and Interfaces.....	31
Message Relay in ASN	31
ASN Gateway Architecture and Deployment Profiles	32
WiMAX Network Deployment Configurations	34
Standalone ASN Gateway/FA and HA Deployments.....	34
Co-Located Deployments	34
ASN Call Procedure Flows	36
Functional Components for Handover.....	36

Anchor ASN Gateway	36
Anchor Session	36
Non-Anchor ASN Gateway	37
Non-Anchor Session	37
Initial Network Entry and Data Path Establishment without Authentication	38
Initial Network Entry and Data Path Establishment with Authentication (Single EAP)	40
Unexpected Network Re-entry	42
MS Triggered Network Exit	43
Network Triggered Network Exit	44
Intra-ASN Gateway Handover	46
Intra-anchor ASN Gateway Uncontrolled Handover	46
Intra-anchor ASN Gateway Controlled Handover	48
Inter-ASN Gateway Handover	54
ASN Gateway Function for Handovers	55
Controlled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover	56
Uncontrolled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover	61
RADIUS-based Prepaid Accounting for WiMax	63
Obtaining More Quota after the Quota is Reached	63
Applying HTTP Redirection Rule when Quota is Reached	65
Applying HTTP Redirection Rule CoA is Received	67
Terminating the Call when Quota is Reached	69
CSN Procedure Flows	71
PMIP4 Connection Setup and Call Flow with DHCP Proxy	71
PMIP4 Session Release	73
WiMAX Deployment with Legacy Core Networks	75
ASN Gateway Interoperability with 3GPP Overlay	75
ASN Gateway Interoperability with 3GPP2 Overlay	75
Session Continuity Support for 3GPP2 and WiMAX Handovers	76
Supported Standards	77
WiMAX/IEEE References	77
IEEE Standards	77
IETF References	77
Object Management Group (OMG) Standards	78
ASN Gateway Service Operation and Configuration	79
Terminology	80
Contexts	80
AAA Realms	81
Authenticator	81
EAP Profile	81
Ports	82
Logical Interfaces	82
Bindings	83
Services	84
AAA Servers	85
Subscribers	85
Default Subscribers and Realm-based Subscriber Templates	86
How the System Selects Contexts	90
Context Selection for Context-level Administrative User Sessions	90
Context Selection for Subscriber Sessions	90
AAA Context Selection for Subscriber Sessions	90
Destination Context Selection for Subscriber Sessions	93
ASN Gateway Simple IP Configuration Examples	95
Simple IP Support with Single Source and Destination Context	96
Information Required	96
Source Context Configuration	97

Destination Context Configuration	99
System-Level AAA Configuration	102
How This Configuration Works	103
Single Source and Multiple Outsourced Destination Contexts	105
How This Configuration Works	106
ASN Keep Alive BS Monitoring	109
Keep Alive Request and Response Overview	110
Keep Alive Request Sender	110
Keep alive Request Receiver	111
Operation, Administration and Monitoring (OA & M)	111
Command Mode	112
Show Commands	112
SNMP Traps	115
WiMAX PMIPv6 Operation	117
Mobile Access Gateway Processing	118
Managing Binding Update List	118
Other MAG Functions	118
LMA Operation	120
Managing Binding Cache Entry Data Structure	120
Access Authentication	120
Proxy Binding Update Processing in LMA	120
Other LMA Functions	121
BCE (Binding Cache Entry) lookup on LMA	121
Fallback Mechanism between PMIPv6 and PMIPv4	122
PMIPv6 Call Flows: Connection Setup	123
PMIPv6 Call Flow-renew	124
PMIPv6 Call Flow: Connection Teardown	125
PMIPv6 Call Flow: Connection Release by LMA	126
Operation, Administration, and Maintenance	128
ASNGW Service Configuration Commands	128
MAG Service Configuration Commands	128
show subscribers	129
show subscribers summary	131
show asngw-service session full	133
show mag all	134
show mag statistics	134
LMA Service Configuration Commands	139
Show Commands	139
show subscriber summary	141
show lma all	143
show lma-service full	144
show lma-service statistics name lma-v6	144
Monitoring Global Protocols	148
Subscriber Configuration	149
ASN Gateway Mobile IP Configuration Examples	151
Mobile IP Support Using the System as ASN Gateway/FA	152
Information Required	153
Source Context Configuration	153
AAA Context Configuration	154
Mobile IP Destination Context Configuration	156
System-Level AAA Parameter Configuration	157
Optional Destination Context	158
How This Configuration Works	159

ASN Gateway Service Configuration Examples	163
Overview of Standalone ASN Gateway Configuration	164
Initial Configuration	164
ASN Gateway Configuration	167
Subscriber Configuration	168
Multi IP Host Configuration	169
BS Monitoring Configuration	169
ASN Gateway Logging Configuration	170
Configuring ASN Gateway/FA Service	171
Initial Configuration	171
Configuring the FA Service	174
Configuring Bulk Statistics Schema	176
Save the Configuration	177
Managing Your Configuration	178
Gathering ASN Gateway Statistics	180
ASN Gateway QoS and Service Flow Configuration	181
Introduction	182
Connection-oriented MAC Architecture	182
WiMAX Service Flow and QoS	182
WiMAX QoS Parameters and Functions	185
QoS Parameters	185
Service Class	185
Service Flow	187
Service Flow Authorization (SFA)	188
Subscriber Policy and QoS Profile	188
Subscriber QoS Profile	188
QoS Message Flow	189
Pre-provisioned Service Flow	189
QoS and Service Flow Configuration	192
AAA Provided Configuration	192
AAA Provided Service Profile Id	192
Configuring the Traffic Class-Map Parameters	192
Configuring QoS Descriptor Table Parameters	193
Configuring the ASN Gateway Service Profile Parameters	193
Configuring the Service Flow and Policy Interaction	194
Applying QoS to Subscriber Template	194
Configuring QoS for AAA-provided Service Profile Id	195
Service Configuration Procedures	197
Creating Contexts	198
Creating and Configuring Ethernet Interfaces and Ports	201
Creating and Configuring FA Services	208
Creating and Configuring HA Services	213
Session Continuity Support	219
Configuring Hybrid HA Service	220
Configuring WiMAX HA for WiMAX Calls	220
Configuring WiMAX HA to Accept 3GPP2/Static MIP Key	221
Hybrid HA for WiMAX and 3GPP2 Calls	222
WiMAX-3GPP2 Interworking at HA	224
Mobile Node Requirement	224
H-AAA Requirements	224
FA and HA Function for 3GPP-WiMAX Interworking at HA	225
Generic Configuration:	225
WiMAX FA Service Configuration	225
3GPP2 FA Service Configuration	227

Common HA Service Configuration.....	228
Configuring DHCP-based IP Address Assignment.....	230
Configuring the Destination Context Attribute.....	233
Configuring IP Address Pools on the System.....	235
Verifying and Saving Your Configuration	243
Verifying the Configuration	244
Feature Configuration.....	244
Service Configuration.....	245
Context Configuration.....	246
System Configuration.....	246
Finding Configuration Errors	246
Saving the Configuration.....	248
Saving the Configuration on the Chassis.....	249
Monitoring the Service	251
Monitoring Service Status and Performance	252
Clearing Statistics and Counters.....	257
Troubleshooting the ASN Gateway Service.....	259
Verifying Network Connectivity.....	260
Using the Ping Command.....	260
Using the Traceroute Command.....	261
Viewing IP Routes.....	263
Viewing the Address Resolution Protocol Table.....	263
Using the DHCP Test Command.....	264
Using the System's Diagnostic Utilities	266
Using the Monitor Utility	266
Using the Protocol Monitor	266
Using the Protocol Monitor for a Specific Subscriber	270
Using the RADIUS Testing Tools	274
Testing a RADIUS Authentication Server.....	274
Testing a RADIUS Accounting Server.....	275
ASN Paging Controller and Location Registry Overview.....	277
Introduction	278
Description of PC/LR Support.....	280
Licenses	280
Paging and Location Update Procedures	280
Paging Controller (PC)	280
Paging Agent (PA).....	281
Paging Group (PG)	281
Location Register (LR)	281
Location Update Procedure.....	281
Location Update with Paging Controller Relocation	283
Paging Operation	285
MS Initiated Idle Mode Entry	287
MS Initiated Idle Mode Exit	290
Supported Platforms and Software	293
ASN PC/LR Service Configuration	295
Configuring the ASN PC/LR Services	296
Overview	296
Initial Configuration	296
Creating the PC and LR Service.....	298
Configuring the PC and LR Service	299
Subscriber Configuration.....	299
ASN PC/LR Logging Configuration	300





Configuring Bulk Statistics Schema	301
Save the Configuration.....	302
Managing Your Configuration	303
Gathering ASN PC/LR Statistics	305
Engineering Rules.....	307
Interface and Port Rules	308
R6 Interface Rules	308
Connectivity Service Network (CSN) Interface Rules	308
FA to HA R3 Interface Rules	308
HA to FA R3 Interface Rules	309
Subscriber Rules	310
Service Rules.....	311
DHCP Service Engineering Rules.....	312
MIP Timer Considerations.....	313
Call Flow Summary	314
Timer Values and Recommendations	316
Controlling the Mobile IP Lifetime on a Per-Domain Basis	317
Supported Registration Reply Codes	321
FA Service Reply Codes	322
HA Service Reply Codes	324
Sample Configuration.....	327
ASN Gateway Configuration in Single Context (Simple IP)	328
FA and HA Configuration with Mobile IP	330
ASN Gateway Service QoS Configuration	335
ASN Gateway and ASN PC/LR Configuration.....	337

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 <i>screen display</i>	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 <i>variable</i> }	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 <i>variable</i>]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
	<p>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).</p> <p>Pipe filters can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ nonce timestamp }</pre> <p>OR</p> <pre>[count <i>number_of_packets</i> size <i>number_of_bytes</i>]</pre>

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

ASN Gateway Overview

Access Service Network Gateway (ASN Gateway) is the subscriber-aware mobility access gateway for IEEE 802.16 mobile WiMAX radio access networks. These carrier- and enterprise-class platforms provide exceptional reliability and performance characteristics for mobile WiMAX operators.

The ASN Gateway provides inter-technology mobility for 3GPP, 3GPP2, DSL, and WiFi access technologies. This assures common billing and seamless inter-technology handover.

ASN Gateway is available for all chassis running StarOS Release 7.1 or later.



Important: The ASN Gateway is a licensed product and requires an Access Service Network Gateway support license.

ASN Gateway provides the following functionality, all of which is integrated into the chassis:

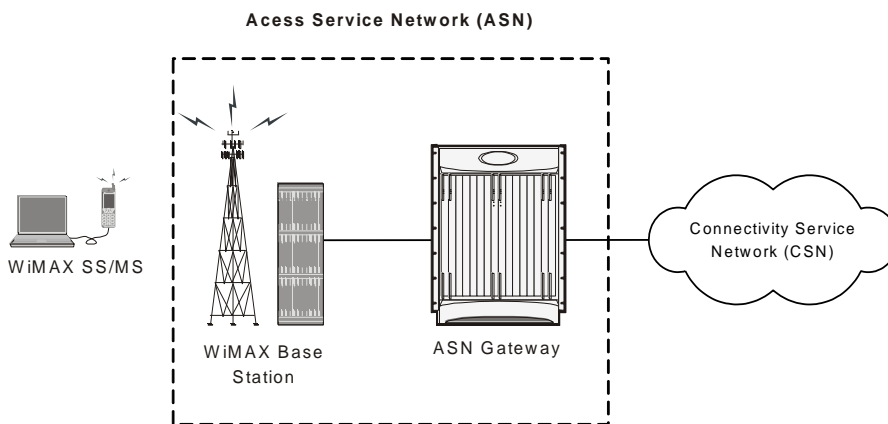
- ASN mobility
- Extensible Authentication Protocol (EAP) user authentication/Authentication, Authorization, Accounting (AAA) client
- DHCP proxy server
- Connectivity Service Network (CSN) mobility
- Intra-ASN and inter-ASN handover
- Paging controller/location register
- Radio resource controller relay function
- Service Flow Authenticator (SFA)
- Proxy-Mobile Internet Protocol (P-MIP) client
- Mobile IP Foreign Agent (MIP FA) protocol
- Data path function
- Context server function
- Handover relay function

ASN Mobility Management

The Access Service Network Gateway (ASN Gateway) processes subscriber control and bearer data traffic, and supports connection and mobility management across cell sites and inter-service provider network boundaries. An ASN Gateway is a logical entity in the Access Service Network (ASN) of a WiMAX radio access network and interfaces directly with base transceiver station or base station via an R6 GRE reference interface. An ASN Gateway performs control plane functions, bearer plane routing or bridging functions, resident functions in the connectivity service network, or a function in another ASN.

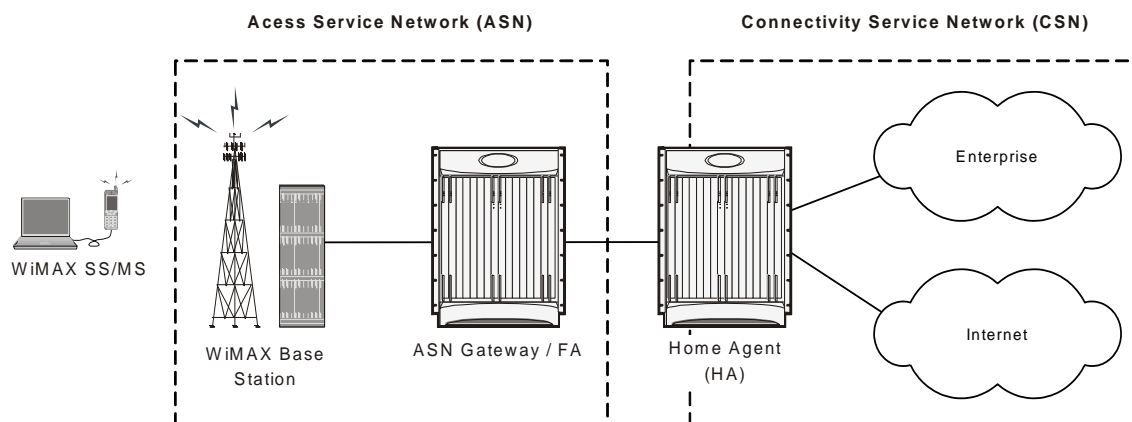
The ASN Gateway is placed at the edge of an ASN and is the link to the CSN. Each ASN Gateway can concentrate traffic from multiple radio base stations. This reduces the number of devices to manage and minimizes connection set-up latency by decreasing the number of call handovers in the network.

Figure 1. Basic ASN Gateway Network



To support Mobile IP and/or Proxy Mobile IP data applications, you can configure the system to perform the role of the ASN Gateway/foreign agent and/or the home agent within the connectivity service network (CSN) of your WiMAX data network. When functioning as a home agent, the system can be located within your WiMAX network or in the CSN of an external enterprise or ISP network. In either case, the ASN Gateway/foreign agent terminates the mobile subscriber's call session and then routes the subscriber's data to and from the appropriate home agent.

Figure 2. Basic ASN Gateway Mobile IP Network



EAP User Authentication

The ASN Gateway serves as the Extensible Authentication Protocol (EAP) authenticator and mobility key holder for subscriber connections and RADIUS clients to attached Authorization, Authentication, and Accounting (AAA) servers.

ASN Gateway and AAA

ASN control is handled by the ASN Gateway and the base station. The ASN Gateway control plane handles the feature set, including AAA functions, context management, profile management, service flow authorization, paging, radio resource management, and handover. The data plane feature set includes mapping radio bearer to the IP network, packet inspection, tunneling, admission control, policing, QoS, and data forwarding.

The ASN Gateway acts as an authenticator. It operates in pass-through mode for EAP authentication between the EAP client (the mobile station) and the EAP (AAA) server. After successful EAP authentication, the AAA server sends the master session key (MSK) to the ASN Gateway. The ASN Gateway, as authenticator, performs authorization key (AK) context management. It derives the AK from the MSK and sends it to the base station. As part of the AK context, other information, such as the AkID and CMAC are sent to the base station to secure the R1 interface.

An AAA module in the ASN Gateway provides flow information for accounting. Every detail about a flow, such as the transferred or received number of bits, the duration of the connection, and the applied policy, is retrievable from the data plane.

Profile Management

The ASN Gateway provides profile management and a policy function that resides in the connectivity network. Profile management identifies a subscriber's feature set, such as the allowed QoS rate, number of flows, and type of flows.

In addition, the ASN Gateway maintains a context for the mobile subscriber and the base station. Each subscriber's context contains the subscriber's profile and security context, and the characteristics of the subscriber's mobile device.

The subscriber's context is retrieved and exchanged between the serving base station and a target base station during handover.

The ASN Gateway authorizes service flows according to the subscriber's profile. Allowed service flows and active service flows can change over time, so the ASN Gateway provides admission control for downlink traffic. The ASN Gateway creates a GRE tunnel per service flow.

Inter-ASN Handovers

During a handover, the ASN Gateway provides the subscriber's context to a target base station and when requested, changes the data path. To minimize latency and packet loss, the ASN Gateway implements data integrity through bi-casting or multi-casting. For paging, buffering is also supported. A foreign agent maintains the IP connectivity if the mobile subscriber initiates an inter-ASN handover. The ASN Gateway supports either Proxy-Mobile IP (PMIP) or Client-Mobile IP (CMIP) in order to communicate with home agents.

The ASN Gateway maintains location information to provide the paging service that tracks subscribers when they are operating in idle mode. If there is any download traffic, ASN Gateway requests the PC to trigger paging. During active operation, location information is also updated as the mobile subscriber moves to a new base station.


Supported Features

The Access Service Network Gateway (ASN Gateway) provides ASN Gateway control and bearer plane routing functions:

- BS Interface: R6 IP/GRE bearer plane
- Inter-ASN handovers to other ASN Gateways: R4 IP/GRE bearer plane
- Interactions with AAA management or policy servers: R3 RADIUS interface
- Mobile IP Interface to HA in Connectivity Service Network: R3 IP-in-IP tunneling

A Profile C ASN Gateway is one of three alternative designs for radio resource management proposed by the WiMAX Forum. In a Profile C architecture, the handover control component resides in the base stations. The ASN Gateway represents a transparent message relay point between neighboring base stations. The Radio Resource Controller (RRC) component in every BTS periodically polls its neighbors to build a resource availability database that it checks prior to triggering call handovers.

provides a high performance ASN Gateway platform with the following supported features in the current software version.

 **Important:** Not all features are supported on all platforms.

Simple IPv4 Support

A Simple IP model supports non-mobile IP terminals and provides ASN-anchored mobility for fixed, nomadic, or portable mobility applications. A Simple IP architecture removes dependencies for separate foreign agent and home agent functions. ASN Gateway handles simultaneous combinations of Simple IP, Mobile IP, or Proxy Mobile IP calls. A Simple IP model permits the ASN to be combined or split from the CSN, depending upon the need for roaming. The Simple IP implementation includes a DHCP Proxy Server function for local or AAA-provided IP address assignment.

Simple IP provides a solution for stationary wireless DSL-like applications. It enables mobility on intra-ASN handovers between neighboring base stations and permits inter-ASN mobility via an R4 interface between ASN Gateways.

DHCP Proxy Server

Compared to 3G wireless technologies such as EV-DO (Evolution-Data Optimized) or PDP (Packet Data Protocol) Type PPP (Point-to-Point Protocol) contexts in General Packet Radio Service/Wideband Code division Multiple Access (GPRS/W-CDMA) networks, WiMAX networks do not use a PPP data link layer between access devices and the ASN Gateway. An alternative approach to IP address allocation is needed in Simple IP and Proxy Mobile IP usage models.

The ASN-GW includes a DHCP proxy/server/relay that interacts with the DHCP client function on the access device. In a Simple IP usage model, the DHCP server allocates dynamic addresses from a local address pool or fetches static addresses from subscriber profiles during authentication from a AAA server. Alternatively, the ASN-GW uses a DHCP relay process to forward the DHCP request to an external DHCP server.

In a Proxy Mobile IP use case, the ASN-GW uses a DHCP proxy to trigger a local foreign agent function to initiate a Mobile IP Request via the R3 interface to a home agent. The home agent returns the address via the Mobile IP Response. The DHCP Proxy component on the ASN Gateway conveys the address in a DHCP Response message to the DHCP client running on the user's access device.

This solution enables mobility on intra-ASN handovers between neighboring base stations. It also permits inter-ASN mobility via an R4 interface between ASN Gateways.

ASN Gateway Micro-Mobility

ASN Gateway micro-mobility provides ASN Gateway-anchored L2 handovers. This low-latency procedure assures the seamless mobility of mobile access devices within a WiMAX network. The ASN Gateway supports both uncontrolled and controlled handovers for micro-mobility.

Uncontrolled Handovers

In an uncontrolled handover scenario, a mobile subscriber attempts to re-enter the WiMAX network at a target base station without the handover preparation procedures with the serving base station. In order to authenticate the roaming user, the target base station obtains the subscriber and security context information from the serving ASN. The anchor authenticator ASN Gateway conveys the context response message and assists in the establishment of a new R6 GRE bearer connection to the target base station. It is referred to as an L2 operation because the previously assigned IP address for the binding remains the same on the anchor authenticator/data path ASN Gateway while the L2 BSID (Ethernet MAC address) is updated for the target base station. Uncontrolled handovers are supported for both Simple IP or Mobile IP use cases.

With uncontrolled L2 handover procedures, interactive and non-real-time applications incur minimal performance degradation and packet loss during subscriber movement between cell sites.

Controlled Handovers

A controlled handover occurs when a subscriber access device explicitly requests handover assistance from the serving base station to a new target base station. This process minimizes packet loss to the WiMAX access device. During the handover request, the serving base station provides the subscriber's context information to the anchor authenticator ASN Gateway and a list of target base stations that are preferred by the mobile device. Upon a successful response from potential target base stations, the anchor authenticator ASN Gateway initiates a data path for the mobile subscriber to the target base station. It also transfers all contextual information for the session to the target base station. The downlink traffic for the mobile subscriber is simultaneously broadcast and subsequently buffered by each of the target base stations.

Controlled handovers may be triggered by the mobile access device or the serving base station as a congestion overload control mechanism.


Controlled handovers and associated data path pre-registrations minimize the impact on performance to a greater extent than uncontrolled handovers and significantly reduce datapath outages.

WiMAX R4 Inter-ASN Mobility Management

R4 inter-ASN mobility management procedures enable low latency call handovers between neighboring ASN Gateways located in different geographical regions or different operator networks. During mobility operations, the call is anchored on the anchor authenticator ASN Gateway. When a mobile subscriber roams to a destination cell site, the target base station connects to the anchor gateway over the serving ASN Gateway's R4 interface. The R4 interface provides control functions such as security context transfers and IP/GRE bearer level connections. The data conveyed to the subscriber by the remote hosts is subsequently tunneled over R4 by the anchor authenticator gateway to the serving gateway. The current ASN Gateway implementation supports the co-existence of anchor authenticator and anchor datapath functions in the same ASN Gateway.

Supported R4 functionality includes:


- R4 over Simple IP connections
- R4 over Mobile IP connections
- Anchor Gateway bi-casting over simultaneous R6 and R4 sessions
- Co-location of DHCPv4 Proxy and PMIPv4 FA on anchor authenticator gateway
- Support for multiple QoS service flows per-session via R4 tunnels

 **Important:** Both the anchor gateway session and non-anchor gateway sessions are counted towards the session license separately. Licensed session limits are enforced based on the total number of anchor and non-anchor sessions.

WiMAX R3 CSN Anchored Mobility Management

The R3 reference point defines a set of control plane protocols between the Access Service Network (ASN) and Connectivity Service Network (CSN) to support AAA, policy enforcement, and mobility management functions. The R3 reference interface is used in a mobile IP application with the home agent acting as the call anchor point. In contrast to L2-based ASN anchored mobility procedures, CSN anchored mobility is L3-based and supports both proxy mobile IP and mobile IP calls. The R3 interface uses mobile IP signaling and IP-in-IP tunneling or GRE tunneling and includes standard features such as dynamic Home of Address (HoA) address allocation. Mobility signaling messages are authenticated by the home agent based on a dynamic user identity called a pseudo-NAI which changes after each authentication.

Mobile IP applications are well suited for inter-provider roaming applications and inter-technology handovers such as WiMAX-HRPD Rev A, WiMAX-WiFi, and WiMAX-W-CDMA. Mobile IP also provides an attractive solution for operators with a heterogeneous radio access network who want to support seamless mobility across base transfer stations from multiple RAN suppliers.

 **Important:** Support for this function requires the HA feature license key.

Proxy Mobile IPv4 (PMIPv4)

The P-MIP procedure is designed for Simple IP-capable access devices for which mobility procedures are performed entirely in the network. Certain events on the access device require relocation of the L3 anchor point (for example,

CoA). One case is for the initial connection establishment in which the home agent or H-AAA server assigns an IP address and generates the mobility binding. Another is when the mobile subscriber roams across cell sites or ASNs and attaches to a target ASN Gateway.

Client Mobile IPv4 (CMIPv4)

CMIPv4 provides mobility procedures for mobile IP-capable access devices. In contrast to PMIPv4, where stateful DHCP proxy signaling triggers R3 signaling between the ASN Gateway and the home agent, CMIPv4 uses agent advertisement between the foreign agent component in the ASN Gateway and mobile IP client on subscriber access device. Mobile IP signaling occurs directly between the access device and the anchor foreign agent component in the ASN Gateway.

Authenticator

The authenticator function in the ASN Gateway acts as an anchored authenticator for a subscriber for the duration of the session. For example, as a subscriber moves between base stations served by the ASN Gateway, the authenticator anchor remains stationary. If a subscriber moves to a base station served by a different ASN Gateway, the anchor authenticator is hosted at that ASN Gateway. If the R4 interface is not supported between both gateways, only the subscriber needs to be re-authenticated.

The RADIUS client for authentication and accounting is collocated with the authenticator function. The ASN Gateway acts as an EAP relay and is agnostic to the EAP method. EAP transport between the ASN Gateway and the base station is performed as a control exchange. The base station functions as an EAP relay, converting Pair-wise Master Key version 2 (PKMv2) to the EAP messages for the ASN Gateway. The ASN Gateway works in pass-through mode and any EAP method that generates keys, such as MSK or EMSK, is supported in the system.

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

EAP Authentication Methods

WiMAX networks use Ethernet as the L2 protocol for network access authentication. The Extensible Authentication Protocol (EAP) provides the network authorization function. The ASN Gateway represents the EAP authenticator and supports a transparent relay point between the EAP client on the subscriber access device and EAP server on the AAA. The ASN Gateway triggers an EAP-identity request to the subscriber device. The subscriber device responds with an EAP-identity response. It subsequently unpacks EAP messages over the R6 interface and transfers them via RADIUS or Diameter signaling to the AAA server.

EAP authentication provide multiple authentication methods that can be tailored to the operator's preference toward user-level, device-level, or user- and device-level network authorization. At the H-AAA server in Home Network

Service Provider (H-NSP), device-level authentication in a roaming application guards against unauthorized network access by users with stolen access devices.

Supported RADIUS Methods

ASN Gateway supports following EAP authentication and authorization methods using RADIUS:

- EAP-Pre-shared Key (EAP-PSK)
- EAP-Transport Layer Security (EAP-TLS)
- EAP-Tunneled Transport Layer Security (EAP-TTLS)
- EAP-Authentication and Key Agreement (EAP-AKA)

EAP-Pre-shared Key (EAP-PSK)

EAP-PSK is a symmetric mutual authentication method that uses manually provisioned pre-shared keys between an EAP client on an access device and an EAP server component on AAA. The size of the pre-shared key can be up to 256 bytes.

EAP-Transport Layer Security (EAP-TLS)

EAP-TLS is an asymmetric authentication method that uses X.509 digital certificates, for example public/private key pairs, and enables device-based authentication.

EAP-Tunneled Transport Layer Security (EAP-TTLS)

EAP-TTLS is a multi-level authentication scheme to enable device and user-based authentication. The first level handshake provides device-level authentication and uses the same encryption and ciphering algorithms as EAP-TLS. The secure connection established through the first level handshake is then extended with MS-CHAP-V2 authentication to verify user credentials. As with other EAP methods, successful EAP transactions at AAA result in a Master Session Key (MSK) that is returned over an encrypted connection. The ASN Gateway uses the key to generate a derivative key for securing the air interface between ASN and user access device.

EAP-Authentication and Key Agreement (EAP-AKA)

EAP-AKA uses symmetric cryptography based on pre-shared private client/server keys and challenge-response mechanisms similar to other EAP methods. It verifies credentials for users of Removable User Identity Modules (R-UIMs).

Supported Diameter Methods

ASN Gateway supports the following Diameter methods for EAP authentication and authorization:

EAP-Authentication and Key Agreement (EAP-AKA)

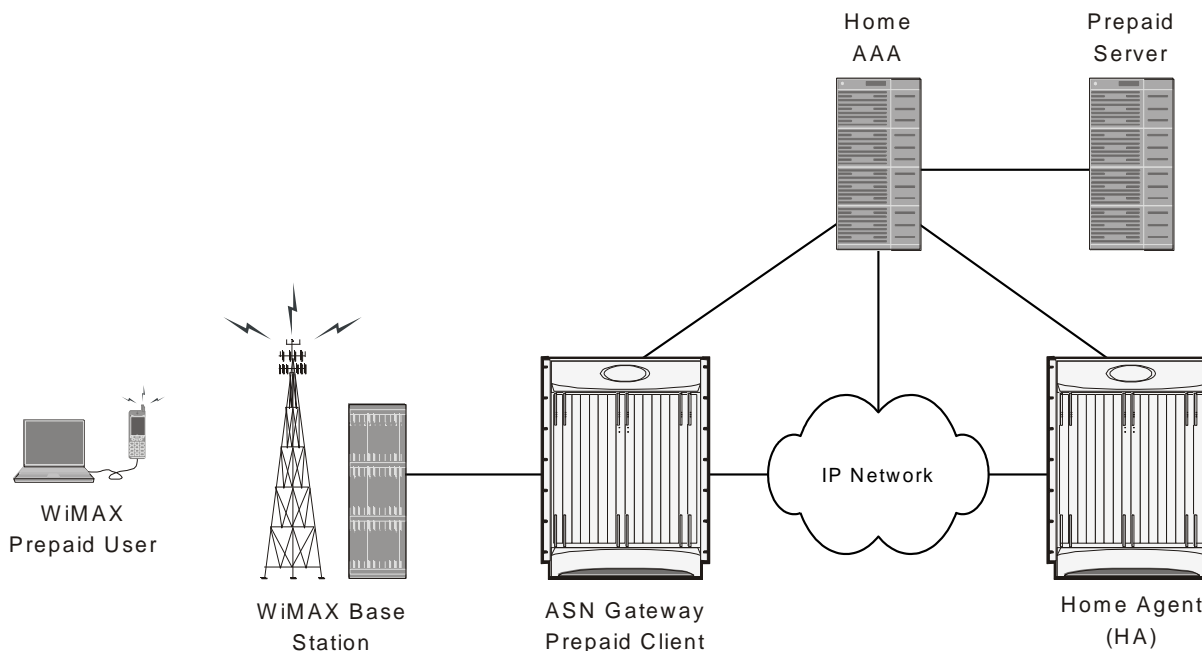
EAP-AKA uses symmetric cryptography based on pre-shared private client/server keys and challenge-response mechanisms similar to other EAP methods. It verifies credentials for users of Removable User Identity Modules (R-UIMs).

WiMAX Prepaid Accounting

The system supports prepaid accounting for clients on the ASN Gateway.

Clients can communicate directly to a home AAA server or be proxied through a visited network's AAA server. The following figure shows a typical prepaid network topology.

Figure 3. Prepaid Network Topology



Volume and Duration-based Prepaid Accounting

Prepaid accounting is a licensed-enabled feature. The ASN Gateway supports both volume threshold and duration threshold based prepaid accounting. Even though session-level accounting is performed for both volume and duration, the number of bytes in a multi-flow session are applied to a duration-based configuration.

RADIUS attributes identify thresholds and quotas for both volume (number of bytes) and duration (length of session).

Supported Enhanced Features

All enhanced features described in this section require the appropriate feature license keys.

Lawful Intercept Enhancements

Lawful Intercept (LI) provides a mechanism for telecommunication service providers (TSPs) to assist Law Enforcement Agencies (LEAs) in monitoring suspicious individuals (referred to as targets) for potential criminal activity. LEAs provide one or more TSPs with court orders or warrants requesting the monitoring of a particular target. The target is identified by information such as their Mobile Station Identification (MSID) number, their name, or their assigned IP address.

It is not possible to provision an LI trigger on the ASN Gateway (Simple IP) or home agent (Mobile IP) with pseudo-NAI identifiers, since the outer identity is concealed from the gateway. For this reason, if it is necessary to provision triggers with the pseudo-NAI, the basic LI license (with AAA event detection) must be used.

Once the target has been identified the system, functioning as either an ASN Gateway (Simple IP) or home agent (Mobile IP), serves as an access function (AF) and monitors new data sessions or sessions already in progress. While monitoring, the system intercepts and duplicates session content and forwards it to a delivery function (DF) over an extensible, proprietary interface. The DF delivers the intercepted content to one or more collection functions.

The WiMAX implementation of LI monitoring includes the following features:

- Active triggers (using AAA assist for control plane event detection)
- Event delivery (AF to DF) with ability to configure UDP/IP message acknowledgements

Intelligent Traffic Control

Intelligent Traffic Control (ITC) supports customizable policy definitions. The policies enforce and manage service level agreements for a subscriber profile, thus enabling differentiated levels of services for native and roaming subscribers.

ITC includes features such as traffic prioritization, for example, marking DiffServ codepoints to enable unique treatments for the five WiMAX classes of service, queue redirection, and per-subscriber/per-flow traffic bandwidth control. Traffic policing enables maximum rate-based services and tiered bandwidth charging models. ITC includes a local policy engine that runs on an ASN Gateway in a Simple IP usage model, or as a home agent in a Mobile IP application. You can configure ITC policies statically with Class-Maps to identify applications flows that use L3/L4 5-tuple identifiers. You can then apply the resulting policy actions through policy maps and policy groups. The detection and programming of the local policy engine can alternatively be triggered on network access at the ASN Gateway as it retrieves QoS profiles for each authenticated user.

This feature provides a policy mechanism so you can enable user entitlements and provision treatments for native users and applications relative to roaming subscribers, Mobile Virtual Network Operators (MVNOs), and offnet P2P traffic.

Hotlining/Dynamic RADIUS Attributes

WiMAX is an all IP-based networking technology in which mobile operators seek a more profitable business model. One way to do this is to avoid traditional device subsidization that accompanies the sale of locked devices that restrict

access to provisioned subscribers of an operator's network. The WiMAX Forum has proposed remote Over-the-Air (OTA) activation protocols such as Open Mobile Alliance Device Management (OMA DM) to enable self-provisioned, self-configured, retail subscription models.

The ASN GW supports hotlining on a session basis. This capability is enabled by default. The rule-based hotlines use an IP redirection rule with the standard attribute Filter-ID. The server sends the ACL names in the Filter-ID attribute, which in turn, locates the rules.

Upon receiving a RADIUS Access-Accept message containing the Filter-ID attribute, the ASN GW locates the rule list, using the name contained in Filter-ID, and applies them to the session.

Configure the rules locally on the ASN GW under ACL groups.

In this scenario:

- A user with an unprovisioned access device registers with a special decorated NAI that represents him/her as a non-subscriber to the AAA.
- The AAA grants limited network access by returning a hotlining filter rule to the ASN Gateway. ASN GW hotlining support uses the standard attribute Filter-ID, along with the session identification parameters User-Name, Calling-Station-ID, and AAA-Session-ID.
- An IP address is assigned during initial network entry. The ASN Gateway uses the redirect address associated with the filter rule to hotline the call to a web activation portal.
- The user profile and subscription activation process is completed. The call is forwarded to the OMA DM server.
- The OMA DM server triggers a network-initiated bootstrapping session with the OMA DM client on the user access device.
- The OMA DM uses XML messaging over a secure OTA connection to remotely configure the access device.
- If a session and an ACL list are located, the rules are applied to the session and a COA-ACK is returned. The AAA server transmits a RADIUS message to the ASN Gateway instructing it to "unhotline" the session.
- At this point, the user is a known subscriber to the back-end subscription database and is granted unrestricted access to the network.

This feature facilitates a non-subsidized retail activation model through over-the-air user-driven subscription and remote device configuration. It also prevents unprovisioned users unrestricted access to the wireless operator's network. This is a complementary technique you can use with operator fraud prevention systems by quarantining fraudulent user sessions or redirecting them to a billing/web portal.

Multi-flow QoS

Within a WiMAX ASN, QoS enforcement is administered by the Service Flow Authorization (SFA) component in the ASN Gateway (also referred to as Anchor Policy Charging Enforcement Function, or A-PCEF). SFA provides traffic management and QoS policy management for subscriber service flows.

Multi-flow QoS enables the establishment of static traffic policies for various subscriber application level service flows. It can be used in Simple IP or Mobile IP usage scenarios. The policies are stored in a Subscriber Policy Repository (SPR) database and retrieved as authenticated QoS profiles by the ASN Gateway. The A-PCEF negotiates via R6 with the Service Flow Manager (SFM) function on the base station. If the authorized QoS profile matches the available base station resources, the request is granted. The A-PCEF provides the following:

- Traffic classification
- Admission control
- Prioritization (DSCP marking)

- Per-session/per-flow bandwidth control
- Flow mapping across application-specific R6/R4 GRE tunnels

In conjunction with multiflow QoS, the ASN Gateway offers configurable accounting on a per-session, per-R6, or per-service flow basis. Multi-flow QoS enables the OFDM radio access connection to be separated into multiple logical Connection ID's (CIDs) with each pair of forward and reverse sub-channels transporting one or more application flows.

Currently, the ASN Gateway supports static pre-provisioned service flows. A total of up to three bi-directional or 6 unidirectional service flows per subscriber R6 or R4 session are possible.


Multi-flow QoS provides enhanced user experience via end-to-end differentiated QoS connection-oriented services and stringent treatment for isochronous voice and delay-sensitive multimedia applications over broadband WiMAX networks. This feature also enables service convergence and is the foundation for delivery of IMS service control.

ASN Gateway Intra-Chassis Session Recovery

This feature enables the system to recover from single software or hardware faults without interrupting subscriber sessions or losing accounting information. Intra-chassis session recovery uses regular task check-pointing of active call states to insure that the fail-over task has the identical configuration and state as the failed process.

Session recovery is supported for the following major features:

- Simple IP, Proxy Mobile IP or Client Mobile IP calls
- R6 or R4 control signaling and bearer level subscriber traffic
- Paging Controller/Location Register (PC/LR) idle mode sessions. PC/LR is a licensed-based feature.
- L2TP LAC & LNS tunnels and sessions

 **Important:** Minimum hardware requirements consist of four processing cards (3 Active, 1 Standby). When session recovery is enabled, overall system capacity may be reduced, depending upon configuration.

Intra-chassis session recovery provides hitless in-service recovery that increases system availability. This eliminates the need for the Radio Access Network to re-register large blocks of simultaneous users. It also minimizes the likelihood of revenue leakage due to the failure of network elements.

This feature requires a feature license key for ASN Gateway session recovery.

Supported Inline Services

All inline services described in this section require the appropriate feature license keys.

Enhanced Charging Service

The Enhanced Charging Service (ECS) is an in-line service feature integrated with the system. ECS provides flexible, differentiated, and detailed billing to subscribers by using Layer 3 through Layer 7 packet inspection. ECS can integrate with a back-end billing system. ECS functionality is supported at the point where sessions are anchored—for example, on the ASN Gateway for Simple IP sessions and on the home agent for Mobile IP sessions.

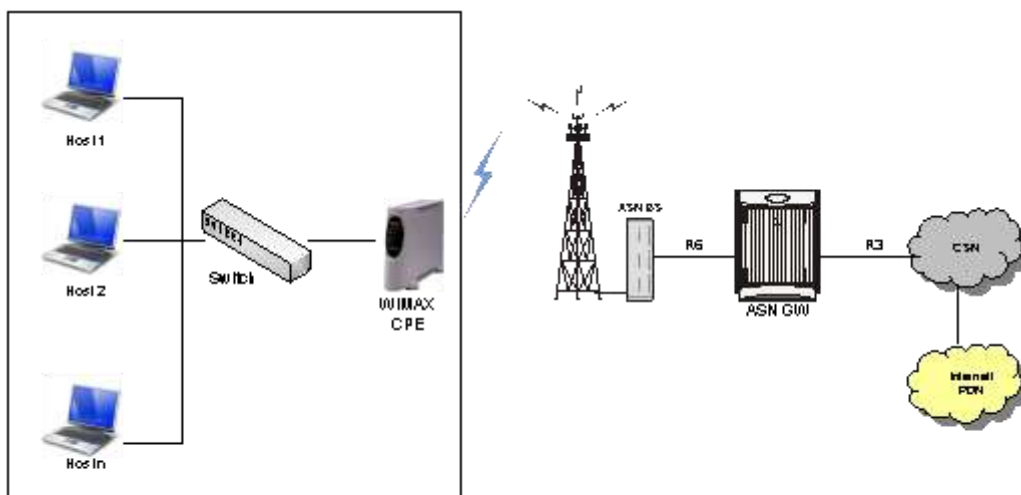
For more information about ECS, refer to the Enhanced Charging Services Administration Guide.

Multi-host Support

ASN Gateway's multi-host feature provides multiple host connectivity.

A WiMAX CPE modem supports multiple IP hosts in fixed/nomadic applications. The modem shares a single WiMAX airlink to connect to the WiMAX IP network. This feature is an effective solution for small or home office users to provide multiple station connectivity through one airlink.

Figure 4. Multi Host Support in WiMAX Network



The WiMAX ASN Gateway allows each WiMAX MS (identified by its 6-byte MSID) to be assigned a single IP address. IP accounting is maintained for the IP address.

How it Works

The DHCP proxy server and the IP pool hosted locally on the ASN Gateway provide the primary IP address from a primary IP pool to the WiMAX customer premise equipment (CPE). The CPE is identified by its WiMAX R6 MSID (6-byte MAC address).

Important: Multiple IP hosts feature is not supported for Proxy-MIP session.

Once a primary IP address is assigned dynamically to the WiMAX CPE, additional IP addresses are assigned dynamically to other IP hosts. Each of the IP hosts is identified by its unique 6-byte MAC address. The DHCP proxy on the ASN Gateway manages the IP addresses by mapping them to the unique MAC addresses supplied by the client in the **chaddr** option field in DHCP DISCOVER or REQUEST messages.

The primary IP address is assigned to the CPE first via DHCP. It is followed by requests for additional IP addresses by individual IP hosts behind the CPE. The ASN Gateway allocates secondary hosts on-demand, up to the configured limit of 4.

Primary IP addresses assigned to WiMAX CPE and secondary IP addresses assigned to the IP hosts, are configured in separate IP pools or the same IP pool. Accounting is based on the primary IP address assigned to CPE and UDR accounting is enabled only for the primary session (flow/session based). No accounting is performed for secondary sub-sessions.

Using the device credentials of the WiMAX CPE, authentication is performed with the EAP-TLS method. There is no authentication for each assigned IP address, and no validation of MAC addresses contained in DHCP requests, except to make sure that they are unique across all subscribers connected to the DHCP proxy server.

IP Address Allocation through DHCP

The dynamic IP address allocation procedure for primary node and secondary hosts is described below:

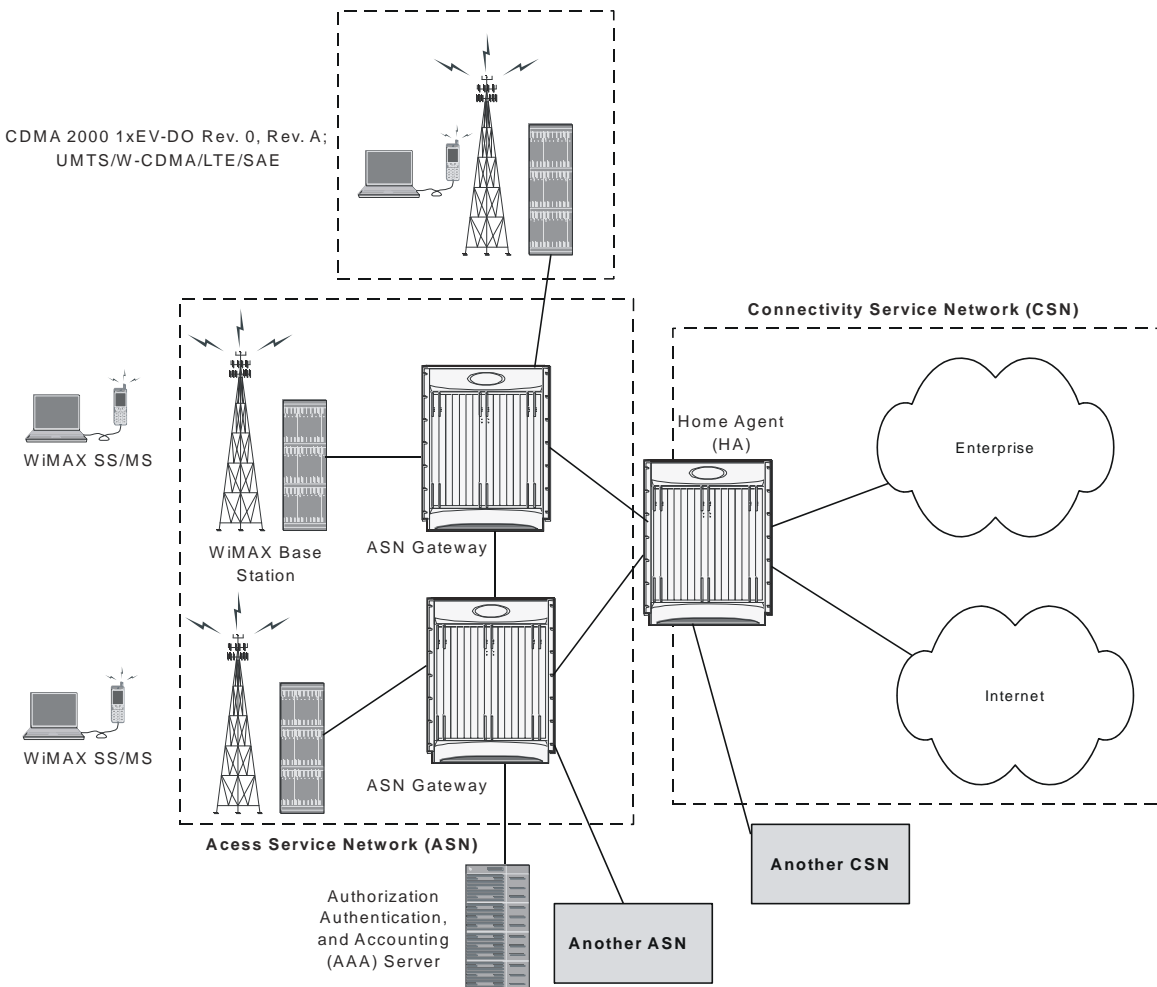
- After the initial network entry for WiMAX CPE is completed, the WiMAX CPE acts as a primary node and starts the DHCP process with the WiMAX ASN Gateway.
- The DHCP proxy server hosted on the ASN Gateway allocates the Primary IP address to the WiMAX CPE as a primary node from the configured primary IP Pool.
- The primary IP address is the first IP address assigned to the WiMAX CPE. The DHCP DISCOVER and REQUEST messages for this must contain the WiMAX R6 MSID as the **chaddr** field. After this IP address is assigned, the session goes into Connected state and is ready to accept DHCP requests for additional IP addresses for other IP hosts.
- Once the primary IP address is assigned to the primary node (WiMAX CPE), hosts behind the CPE start the DHCP process with the WiMAX ASN Gateway for each host mapping to its 6-byte MAC address.
- The DHCP proxy server hosted in the ASN Gateway allocates the secondary IP addresses to the hosts behind the CPE as an auxiliary node from the configured secondary IP Pool.
- When session termination is requested, the primary IP address is the last IP address to be released by the clients and ASN Gateway. This means the primary IP address must be in use and in lease for the session to continue in Connected state. When the Primary IP address is released, the ASN Gateway session is terminated and all IP addresses are freed.
- The auxiliary IP addresses can be assigned and freed any time during the call via DHCP messages.

ASN Gateway in a WiMAX Network

In a WiMAX network architecture, each of the entities, Subscriber Station (SS)/Mobile Station (MS), Access Service Network (ASN) and Connectivity Service Network (CSN) represent a grouping of functional entities.

Each of these functions may be in a single physical device or distributed over multiple physical devices to meet functional and interoperability requirements. The following figure shows a high-level example of WiMAX network architecture

Figure 5. WiMAX Network Architecture



Access Service Network (ASN)

The ASN is an aggregation of functional entities and corresponding message flows associated with the access services. The ASN represents a boundary for functional interoperability with WiMAX clients, WiMAX connectivity service functions, and other vendor-specific functions.

An ASN is defined as a complete set of network functions that provide radio access to a WiMAX subscriber. The ASN provides the following functions:

- WiMAX Layer-2 (L2) connectivity with WiMAX SS/MS
- The transfer of AAA messages to WiMAX subscribers' Home Network Service Provider (H-NSP) for authentication, authorization, and session accounting for subscriber sessions
- Network discovery and the selection of an appropriate NSP from which WiMAX subscribers access WiMAX service(s)
- Relay functionality for establishing Layer-3 (L3) connectivity with a WiMAX SS/MS (IP address allocation)
- Radio resource management
- ASN-CSN tunneling

In addition to the above mandatory functions, for a portable and mobile environment the ASN supports the following functions:

- ASN anchor mobility
- CSN anchor mobility
- Paging and location management

The ASN has the following network elements:

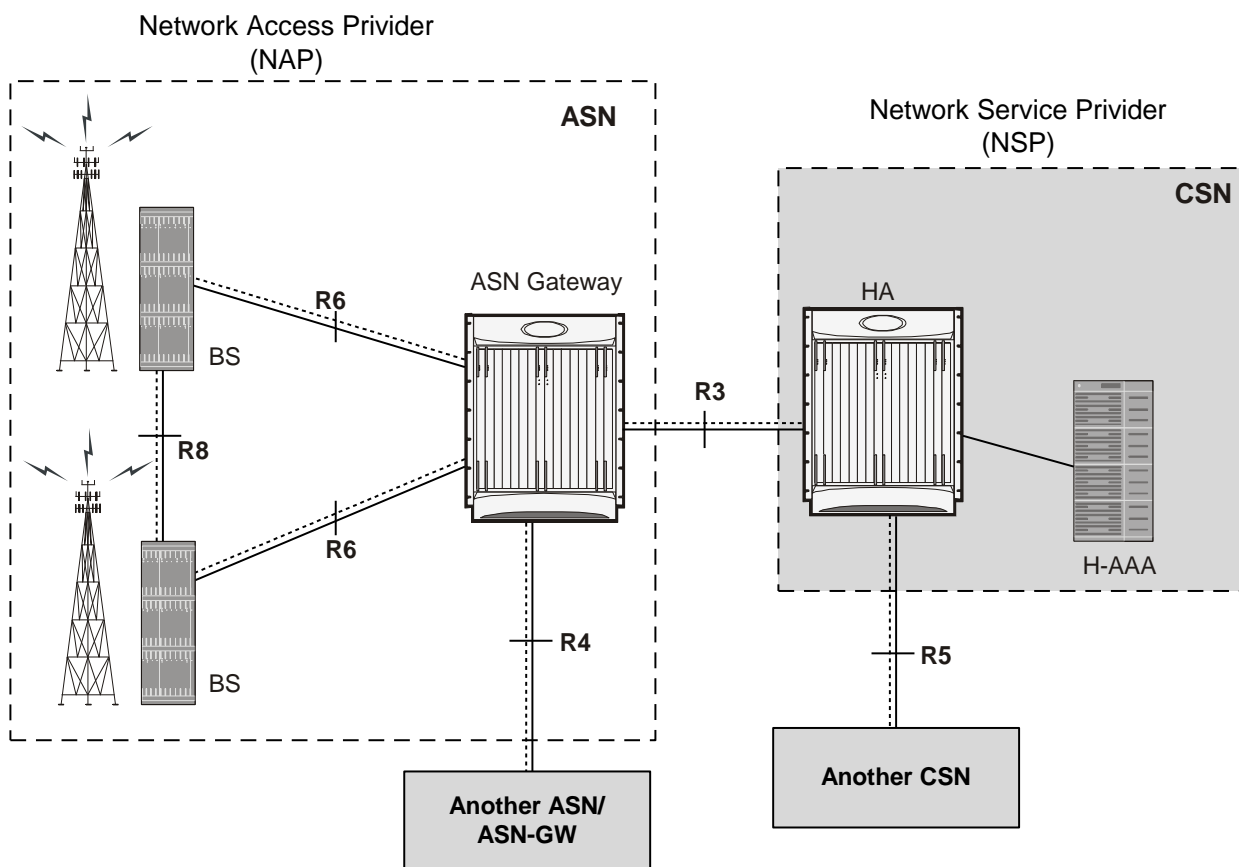
- The WiMAX base station, which is a logical entity that embodies a full instance of the WiMAX Medium Access Control (MAC) layer and physical layer in compliance with the IEEE 802.16 suite of applicable standards. The base station may host one or more access functions and is logically connected to one or more ASN Gateways.
- The ASN Gateway (ASN Gateway), which is a logical entity that represents an aggregation of control plane functional entities. These entities are paired with a corresponding function in the ASN, for example a base station instance, a resident function in the CSN, or a function in another ASN.

The ASN Gateway may also perform bearer plane routing or bridging functions.

The ASN consists of at least one instance of a base station and at least one instance of an ASN Gateway (ASN Gateway). An ASN may be shared by more than one Connectivity Service Networks (CSN).

The ASN decomposition with Network Reference Model (NRM) is shown in the following figure.

Figure 6. ASN Network Reference Model with ASN Gateway




Connectivity Service Network (CSN)

The Connectivity Service Network (CSN) is a set of network functions that provide IP connectivity services to the WiMAX subscriber. A CSN provides the following functions:

- SS/MS IP address and endpoint parameter allocation for user sessions
- Internet access
- AAA proxy or server
- Policy and admission control based on user subscription profiles
- ASN-CSN tunneling support,
- WiMAX subscriber billing and inter-operator settlement
- Inter-CSN tunneling for roaming
- Inter-ASN mobility
- Home agent

The CSN also provides location-based services, connectivity for peer-to-peer services, provisioning, authorization and/or connectivity to IP multimedia services, and support for lawful intercept services in the WiMAX radio access network.


 **Important:** CSN is out of the scope of this document.

WiMAX Reference Points and Interfaces

A reference point (RP) in a WiMAX network is a conceptual link. An RP connects two groups of functions that reside in different functional entities of an ASN, CSN, or mobile station (MS). It is not necessarily a physical interface; an RP becomes a physical interface only when the functional entities on either side of it are contained in different physical devices.

Following are the reference points implemented with the ASN Gateway for WiMAX mobility functions:

- **R3 Reference Point**—Consists of the set of control plane protocols between the ASN and the CSN to support AAA, policy enforcement, and mobility management capabilities. It also encompasses the bearer plane methods (for example, tunneling) to transfer user data between the ASN and the CSN. R3 supports three types of clients: PMIPv4, CMIPv4, CMIPv6 (this is IPv4 and IPv6 support for Proxy Mobile IP (PMIP)) and Client Mobile IP (CMIP).
- **R4 Reference Point**—Consists of the set of control and bearer plane protocols originating and terminating in various functional entities of an ASN that coordinate MS mobility between ASNs and ASN Gateways. R4 is the only interoperable RP between similar or heterogeneous ASNs.
- **R5 Reference Point**—Consists of the set of control plane and bearer plane protocols for internetworking between the CSN operated by the home NSP and that operated by a visited NSP.
- **R6 Reference Point**—Consists of the set of control and bearer plane protocols for communication between the base station and the ASN Gateway. The bearer plane is an intra-ASN datapath between the base station and ASN gateway. The control plane includes protocols for datapath establishment, modification, and release control, in accordance with the MS mobility events. R6, in combination with R4, may serve as a conduit for exchange of MAC state information between base stations that cannot interoperate over R8.
- **R7 Reference Point**—Consists of an optional set of control plane protocols, for example, AAA and policy coordination in the ASN gateway as well as other protocols for coordination between the two groups of functions identified in R6. The decomposition of the ASN functions using the R7 protocols is optional.

 **Important:** To provide high throughput and high density call processing, the ASN Gateway integrates both the Decision Point and Enforcement Point functions. Therefore, the R7 reference point is not exposed.

Message Relay in ASN

The ASN Gateway provides relay procedures to send or distribute received messages with responses from a base station or another ASN Gateway. Supported types of relay functions are:

- **Passive Relay:** In this type of message relay, when the ASN Gateway receives a message on an R4 or R6 interface, it retrieves the destination ID and forwards the same request message to the given destination.
- **Active Relay:** In this type of message relay, upon receiving the message on R4/R6 interface, the ASN Gateway creates a similar R4/R6 message on the basis of original message and relays it to the destination. For example, if during the inter-ASN Gateway handover a non-anchor ASN Gateway receives the data path registration request from the target base station, it creates a new data path registration request and sends it to the anchor ASN Gateway. After receiving the duplicate message, the anchor ASN Gateway sends the data path registration response to the non-anchor ASN Gateway. When it receives that message, the non-anchor ASN Gateway creates a new response message and sends the new data path registration response to the target base station.

ASN Gateway Architecture and Deployment Profiles

The ASN Gateway is part of the Access Service Network (ASN) within the WiMAX network. The ASN Gateway comprises logical and functional elements that provide different functionality in an ASN.

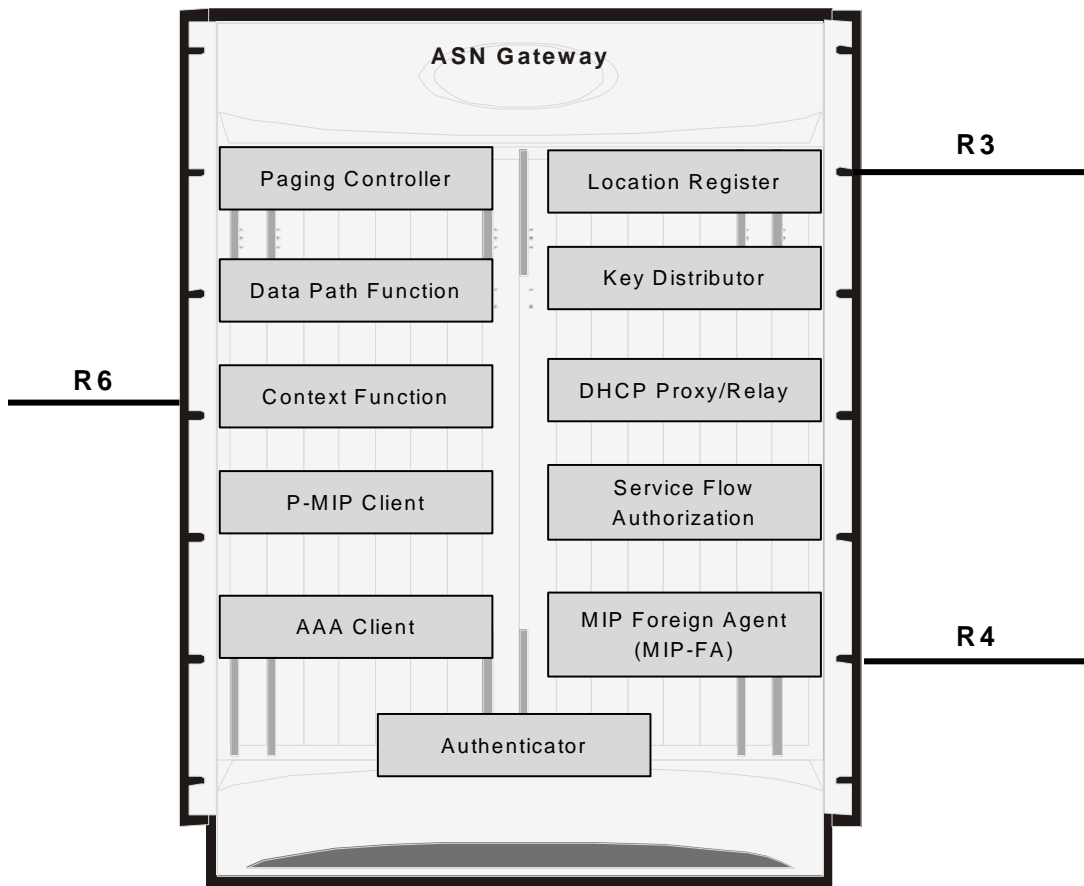
ASN profiles provide a framework for interoperability among entities within an ASN. At a high level, the WiMAX forum has defined groups of functionality for an ASN. These are called Profile Mappings A, B, and C. The key attributes of the profile mappings are:

- **ASN Profile-A**
 - Handover control and Radio Resource control (RRC) in the ASN Gateway
 - ASN anchored mobility among base stations using R6 and R4 reference points
 - CSN anchored mobility among ASNs using PMIP/CMIP (R3)
 - Paging Controller and Location Register in the ASN Gateway
- **Profile-B:** ASN Profile-B removes the ASN Gateway altogether and pushes all its functionality into the base station. This functionality includes the following:
 - Radio Resource control (RRC) handling within the base station
 - R3 reference point
 - R4 reference point
- **Profile-C:** ASN Profile-C functionality is a subset of Profile-A with following functionality in Base Station:
 - HO control
 - Radio Resource Controller (RRC)

The ASN Gateway supports ASN Profile-C functionality. For more information on supported features and functionality, refer to the Supported Feature section.

The following figure shows the mapping of functional entities in an ASN Gateway for Profile-C.

Figure 7. Functional view of ASN Gateway Profile-C



WiMAX Network Deployment Configurations

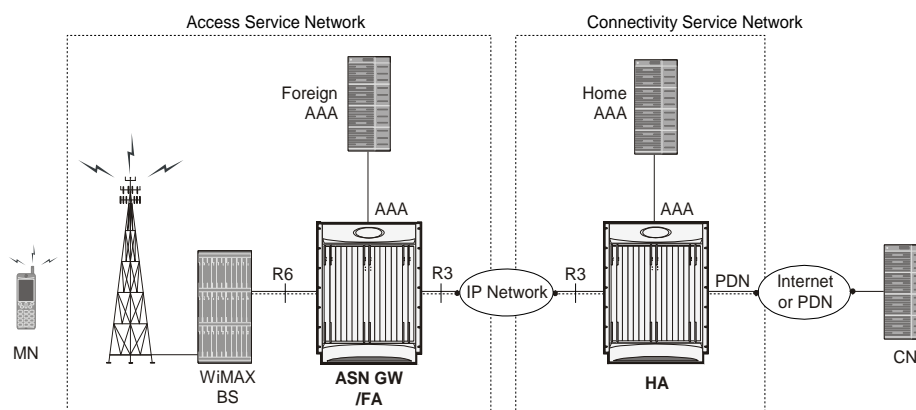
This section provides examples of how the system can be deployed within a WiMAX carrier's network. As noted previously, the system can be deployed in standalone configurations, serving as an Access Service Network Gateway/Foreign Agent (ASN Gateway/FA), a Home Agent (HA), or in a combined ASN Gateway/FA/HA configuration which provides all services from a single chassis.

Standalone ASN Gateway/FA and HA Deployments

The ASN Gateway/foreign agent (FA) serves as an integral part of a WiMAX network by providing packet processing and re-direction to a mobile user's home network through communications with the home agent (HA). No redirection is required when mobile users connect to an ASN Gateway that serves their home network.

The following figure shows an example of a network configuration in which the ASN Gateway/FA and HA are separate systems.

Figure 8. ASN Gateway/FA and HA Network Deployment Configuration Example

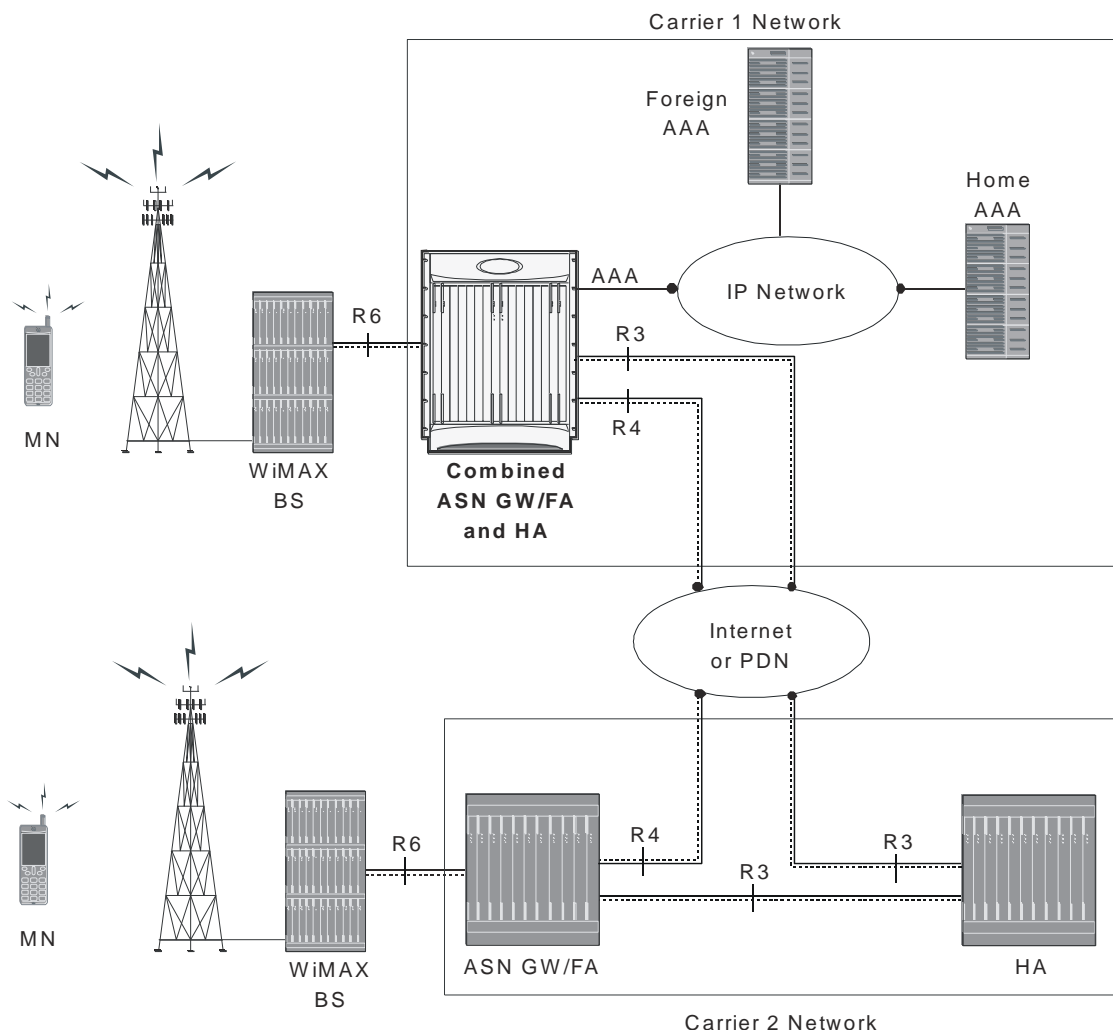


Co-Located Deployments

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

The following figure shows an example of a co-located deployment.

Figure 9. Co-located ASN Gateway/FA and HA Network Deployment Configuration Example



ASN Call Procedure Flows

This section provides information on the function of the ASN Gateway in a WiMAX network and presents call procedure flows for different stages of session setup.

Functional Components for Handover

This section describes the functional components used during handover between ASN Gateways on R4 and R6 interfaces.

Anchor ASN Gateway

The anchor ASN Gateway is the ASN Gateway that holds the anchor data path functions for a given MS. As shown in the following figure, the anchor ASN Gateway hosts the following functions:

- Authenticator (includes Accounting Client)
- Anchor DP function
- DHCP proxy
- PMIP client
- MIP FA
- Anchor SFA
- DHCP proxy function

The ASN Gateway service IP address is the R6 and R4 tunnel endpoint and handles both R6 and R4 traffic.

Anchor Session

The following identifiers identify the anchor ASN Gateway session:

- MSID
- MS NAI
- MS IP address
- DHCP MAC address

The ASN Gateway session consists of an access R6 session and a MIP FA network session. The R6 session has a GRE data path to a base station for an active session. In this session the ASN Gateway service IP address is the R6 and R4 tunnel endpoint and handles both R6 and R4 traffic.

Upon initial network entry, when the DPF is in the anchor ASN Gateway, there is no R4 session. After a MS does a handover to a target BS, it connects to the anchor GW over R4 via a different serving ASN Gateway. At this point, the anchor GW session has an access R4 session and a MIP FA network session. The anchor GW can maintain the R6 session and a R4 session simultaneously.

Note that R6 and R4 tunnels are handled uniformly by the anchor GW as both are access-side tunnels. The anchor GW can check the IP address of the non-anchor GW peer against the configured list of peer ASN Gateway's, so that it can control which R4 connections are accepted.

The anchor GW handles all the Layer 3 processing for the subscriber without including any other rule and policy.

When an anchor GW receives a request message, it reads the source ID in this request and sends the response to this source ID as destination ID. The anchor ASN Gateway remembers the source IP address of the peer from where the message was received, if it is different from the source ID of the message. The response message is sent to this peer IP address, which is the immediate peer.

Non-Anchor ASN Gateway

The non-anchor ASN Gateway hosts the following functions:

- **Serving DP Function:** The subscriber data is not processed in the non-anchor GW. It relays the subscriber data to anchor ASN Gateway over R4. When the inner IP packet emerges from R6 tunnel at the non-anchor ASN Gateway, the packet is sent over R4 data path tunnel to the Anchor ASN Gateway.
- **Serving SFA Function:** No packet classification is performed in this function. It provides only tunnel switching between R4 to R6 or vice versa.
- **DHCP Proxy relay Function:** DHCP messages are not processed in the non-anchor GW and relayed to the DHCP proxy in the anchor ASN Gateway over R4. When the inner IP packet emerges from the R6 tunnel at the non-anchor ASN Gateway, a check is made to see if DHCP proxy is co-located in the ASN Gateway. and whether to process DHCP packet locally or not. If the session is not anchored locally, that is, the DHCP proxy is not co-located, the non-anchor ASN Gateway sends the DHCP packet over an R4 data path tunnel to the anchor ASN Gateway.
- **Relay Function:** The non-anchor ASN Gateway provides relay functions to distribute received messages and subscriber information. The message relay is supported for following functions:
 - Context transfer
 - Paging
 - Accounting
 - Authentication
 - Handover (HO)
 - Radio Resource Controller (RRC)

Non-Anchor Session

A non-anchor session is created upon receiving an R6 Data Path Registration Request from the target base station. Note that the non-anchor ASN Gateway session is identified by MSID only. This non-anchor ASN Gateway does NOT know

the MS NAI and MS IP address of the subscriber, since the authenticator, DHCP and PMIP functions are not exposed here and the MSID is used as the username in session manager. The non-anchor session has the following attributes:

- The Registration Type in the request is set to HO.
- The Destination ID in the message does not match the destination IP address of the message. It needs to match the anchor ASN Gateway ID in the message if an R6 and R4 Data Path setup is intended.
- The anchor ASN Gateway is one of the peer ASN Gateway configured in the ASN Gateway service.

Initial Network Entry and Data Path Establishment without Authentication

This section describes the procedure of initial entry and data session establishment for a WiMAX subscriber station (SS) or MS without authentication by ASN Gateway.

Figure 10. Initial Network Entry and Data Session Establishment without Authentication Call Flow

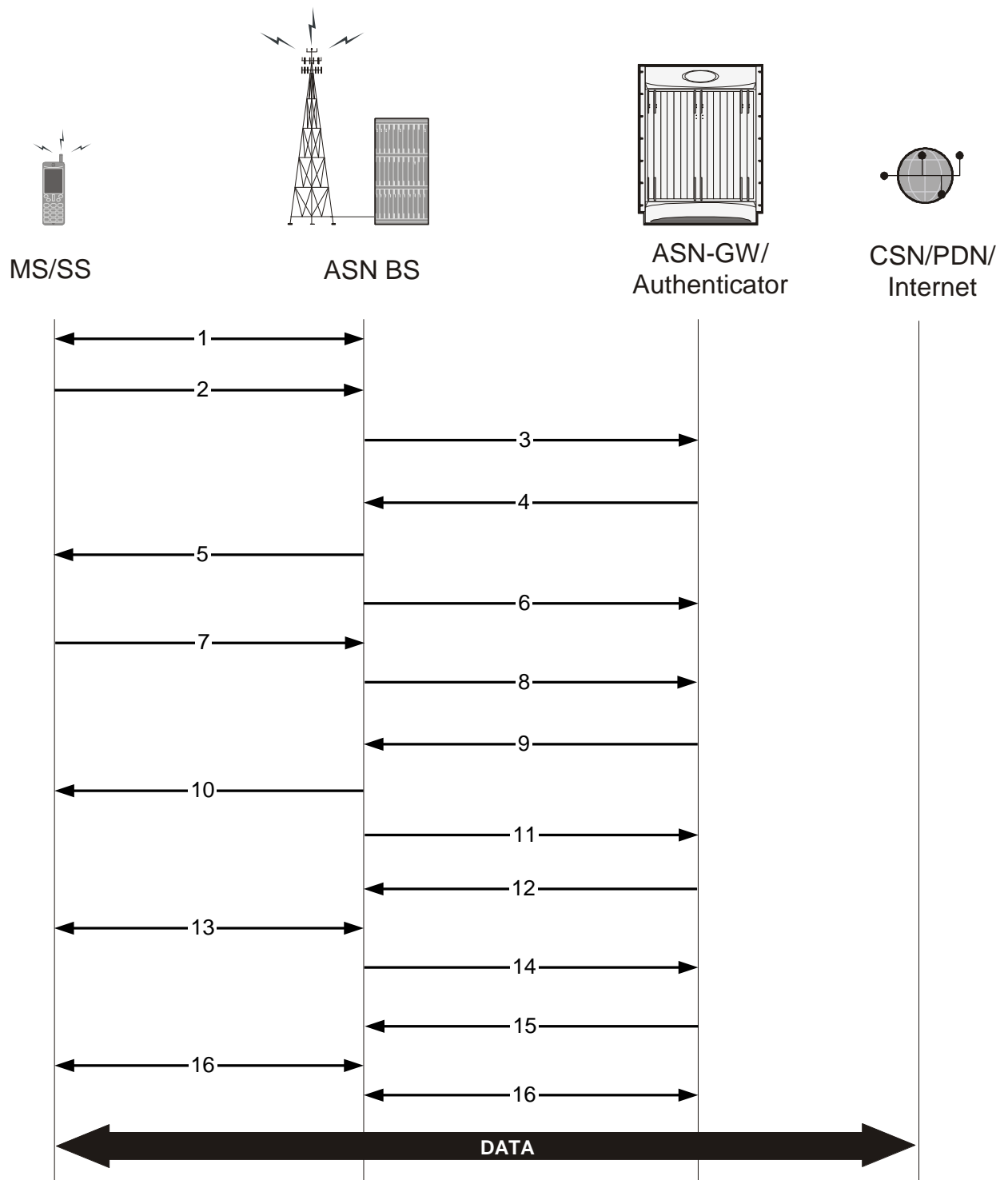


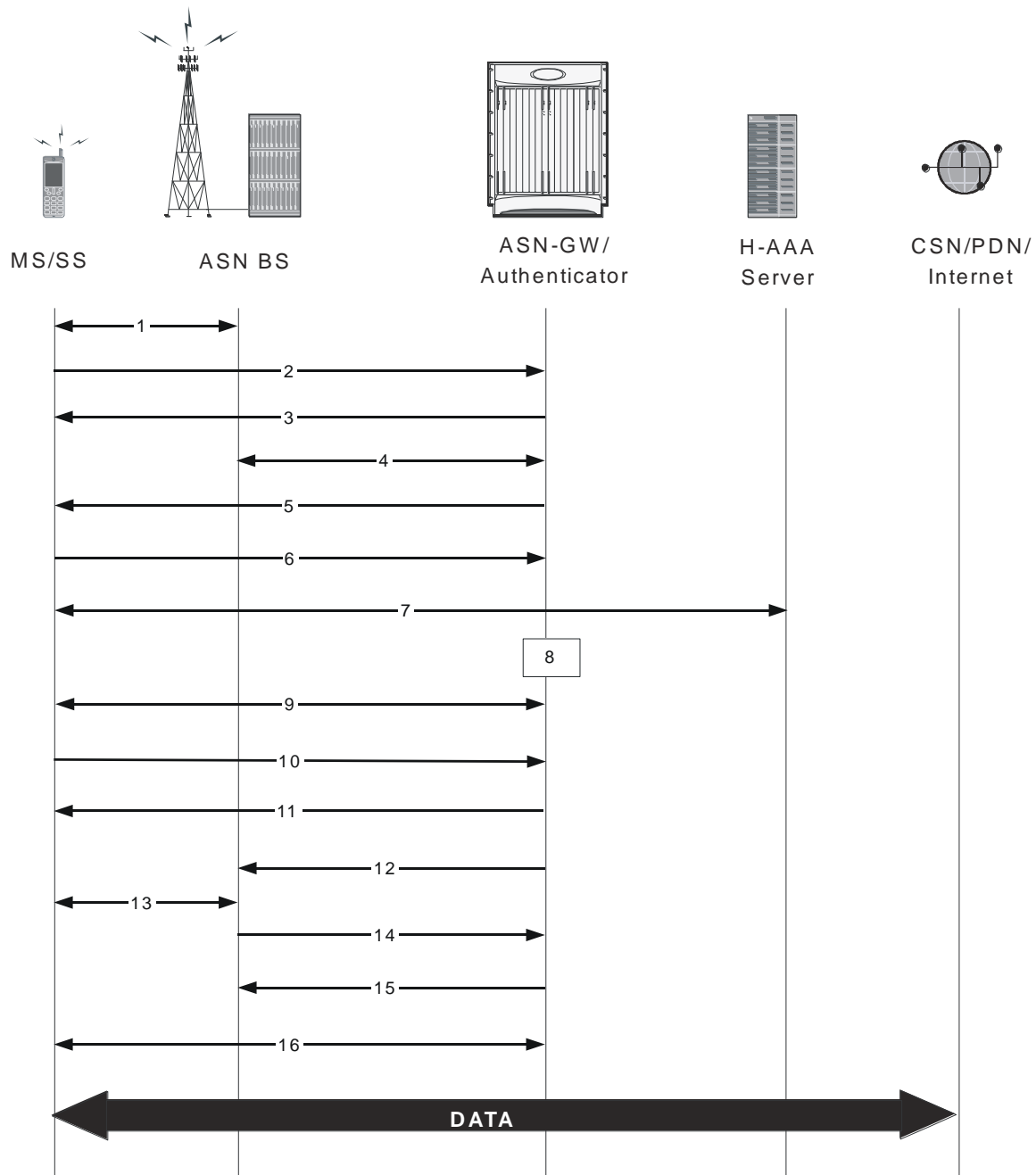
Table 1. Initial Network Entry and Data Session Establishment without Authentication Call Flow Description

Step	Description
1	MS performs initial ranging with the ASN BS. Ranging is a process by which an MS becomes time-aligned with the ASN BS. The MS is synchronized with the BS at the successful completion of ranging and is ready to set up a connection.
2	MS sends basic capability exchange request (SBC-REQ) to ASN BS.
3	ASN BS sends MS-Pre-Attachment Request (authorization policy request) to ASN Gateway.
4	ASN Gateway sends MS-Pre-Attachment Response on the basis of authorization policy to ASN BS for MS.
5	ASN BS sends basic capability exchange response (SBC-RSP) to MS.
6	If authorization policy allows, ASN BS sends MS Pre-Attachment Acknowledgement to ASN Gateway.
7	MS sends Registration-Request (REG-REQ) to ASN BS.
8	ASN BS sends MS-Attachment-Request to ASN Gateway.
9	ASN Gateway sends MS-Attachment-Response to ASN BS and reserves the resource.
10	ASN BS sends Registration-Response to MS.
11	ASN BS sends MS-Attachment-Acknowledgement to ASN Gateway.
12	ASN Gateway sends Path Registration Request to ASN BS.
13	ASN BS creates 802.16 connection and establishes path with MS.
14	ASN BS sends Path Registration Response to ASN Gateway and ASN Gateway creates service flow with CSN over which PDUs can be sent and received.
15	ASN Gateway sends Path Registration Acknowledgment to ASN BS.
16	GRE tunnel mapped to 802.16 connection between MS and ASN BS.
17	R6 GRE data path established between ASN BS and ASN Gateway and data flow starts.

Initial Network Entry and Data Path Establishment with Authentication (Single EAP)

This section describes the procedure of initial entry and data session establishment for a WiMAX Subscriber Station (SS) or MS with single EAP authentication.

The following figure provides a high-level view of the steps involved for initial network entry of an SS/MS with EAP authentication and data link establishment. The following table explains each step in detail.

Figure 11. Initial Network Entry and Data Session Establishment with Authentication Call Flow**Table 2. Initial Network Entry and Data Session Establishment with Authentication Call Flow Description**

Step	Description
1	MS performs initial ranging with the BS. Ranging is a process by which an MS becomes time aligned with the BS. The MS is synchronized with the BS at the successful completion of ranging and is ready to set up a connection.

Step	Description
2	SS Basic capability exchange (SBC-REQ) between MS and BS starts and MS-Info-Request for authorization policy sent to AAA client/authenticator in ASN Gateway.
3	AAA client/authenticator (ASN Gateway) sends MS-Info-Report to BS and BS sends SS Basic Capability Response (SBC-RSP) to MS.
4	BS acknowledges the MS-Info-Report to AAA client/authenticator.
5	AAA client/authenticator (ASN Gateway) starts EAP transfer request to BS and MS.
6	MS and BS sends EAP transfer response to AAA client/authenticator.
7	The MS progresses to an authentication phase with home AAA Server. Authentication is based on PKMv2 as defined in the IEEE standard 802.16 specification. EAP authentication process starts
8	EAP authentication successful and AAA client/authenticator starts security context transfer.
9	PKMv.2-RSP/EAP-Transfer/SA-TEK-Challenge-Request-Response/Key-Request-Response exchange between MS and BS.
10	MS sends 802.16 Registration Request (REG-REQ) to ASN BS and ASN BS sends MS-Info-Request to AAA client/authenticator.
11	AAA client/authenticator sends MS-Info-Report to BS and BS sends Registration Response (REG-RESP) to MS and MS-Info-Report Acknowledge to AAA client/authenticator.
12	ASN Gateway sends Path Registration Request to ASN BS.
13	ASN BS creates 802.16e connection and establishes path with MS.
14	ASN BS sends Path Registration Response to ASN Gateway and ASN Gateway creates service flow with CSN over which PDUs can be sent and received.
15	ASN Gateway sends Path Registration Acknowledgment to ASN BS.
16	GRE tunnel mapped to 802.16 connection between MS and ASN BS.
17	R6 GRE data path established between ASN BS and ASN Gateway and data flow starts.

Unexpected Network Re-entry

An unexpected network re-entry is when a mobile station starts the process of initial network entry to the ASN Gateway via the same or new base station while an existing call for the MS is still in progress or being set up. When this occurs, the ASN Gateway's default behavior is to:

- Accept the new call regardless of the existing call state if the pre-attachment request of the new call comes from a different BS.
- Accept the new call if the original call is in any state past the pre-attachment phase and the pre-attachment request of the new call comes from the same BS.
- Drop the original call in favor of new call.

To disable this default behavior use the **policy ms-unexpected-network-reentry** command in the ASN Gateway Service Configuration Mode. For more information regarding this command, refer to the Cisco Systems Command Line Interface Reference.

MS Triggered Network Exit

This section describes the procedure of MS Triggered network exit for a WiMAX Subscriber Station (SS) or MS in normal mode.

The following figure provides a high-level view of the steps involved for network exit of an SS/MS in normal mode. The following table explains each step in detail.

Figure 12. MS Triggered Network Exit Call Flow

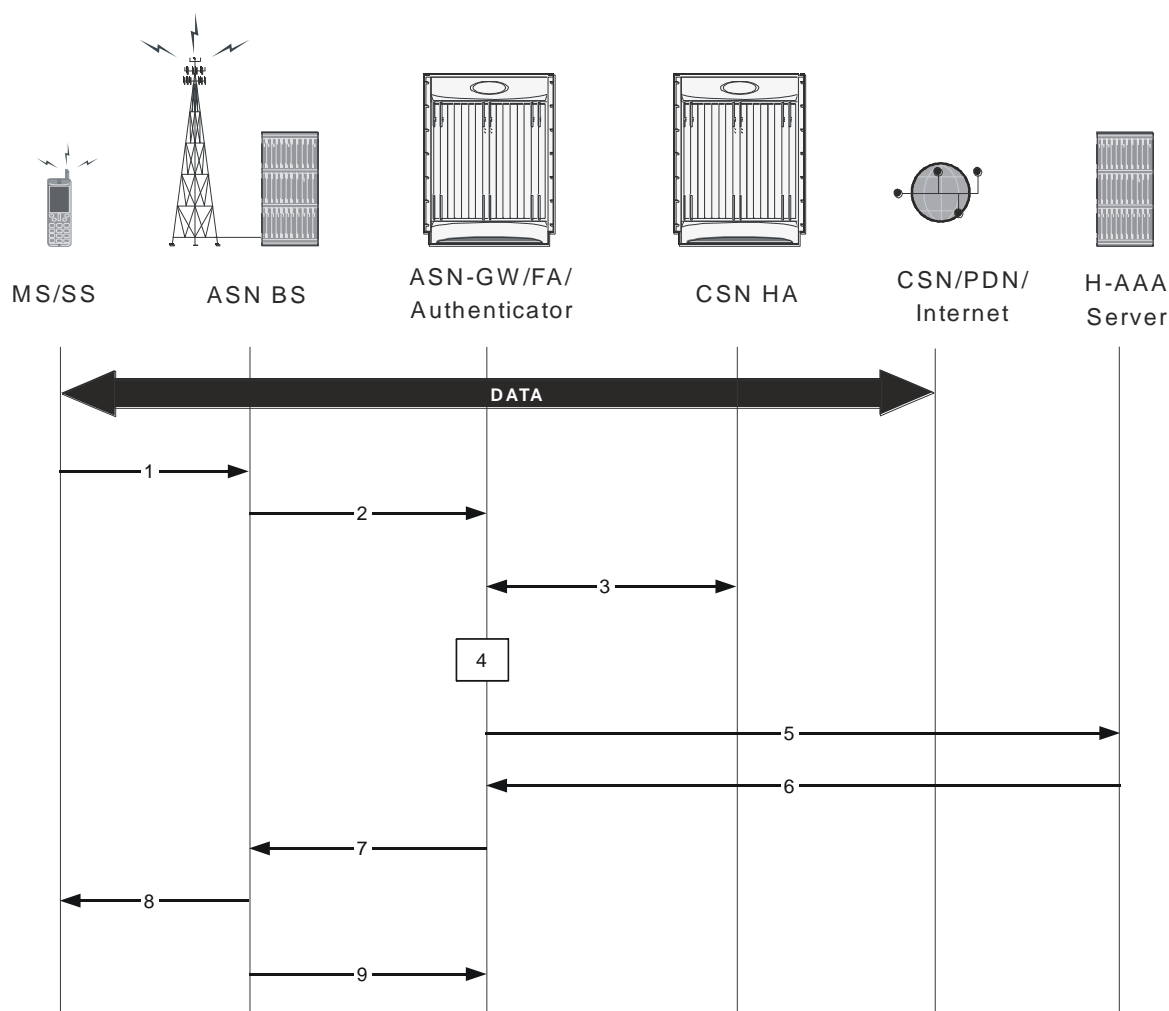


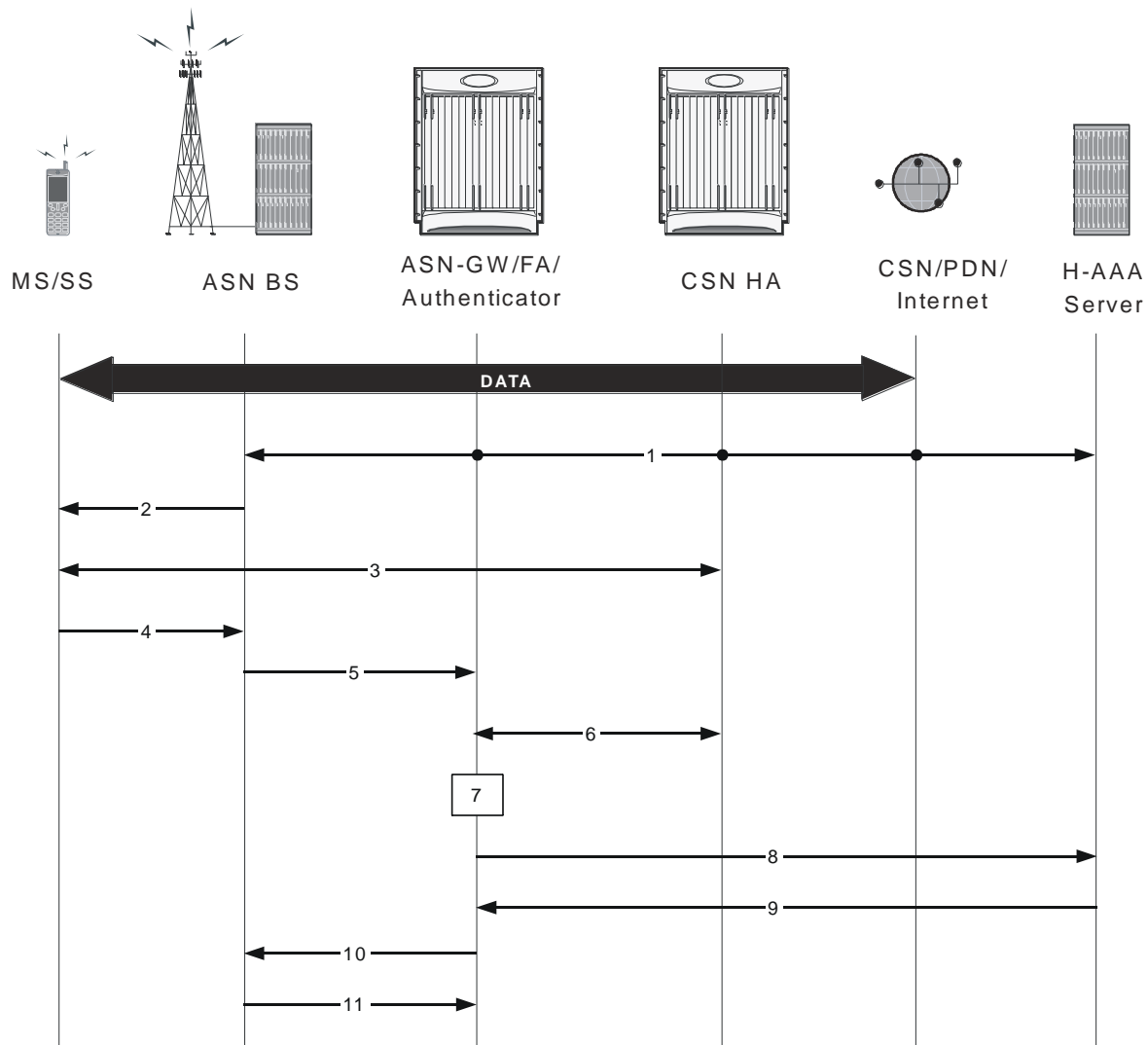
Table 3. MS Triggered Network Exit Call Flow Description

Step	Description
1	MS sends DREG_REQ message to ASN BS in serving ASN, including De-Registration_Request Code=0x00.
2	ASN BS sends R6 Path_Dereg_Req message to ASN Gateway.
3	ASN Gateway/FA and HA starts MIP release procedure.
4	ASN Gateway/FA starts MS context delete procedure.
5	ASN Gateway sends Accounting-Stop-Request (Release Indication) message to AAA.
6	AAA replies with Accounting-Stop-Response message to ASN Gateway.
7	ASN Gateway/FA replies with Path_Dereg_Response message to ASN BS.
8	ASN BS sends DREG_CMD message to MS, including Action Code=0x04.
9	ASN BS sends R6 Path_Dereg_Ack to the ASN Gateway and related entities releases the retained MS context and the assigned data path resource for the MS.

Network Triggered Network Exit

This section describes the procedure of a network triggered network exit for a WiMAX Subscriber Station (SS) or MS in normal mode.

The following figure provides a high-level view of the steps involved for a network-triggered network exit of an SS/MS in normal mode. The following table explains each step in detail.

Figure 13. Network Triggered Network Exit Call Flow**Table 4. Network Triggered Network Exit Call Flow Description**

Step	Description
1	Network entities, such as AAA Server, ASN Gateway FA/HA, trigger Session Release Trigger to ASN BS. This can be from H-AAA ServerAnchor ASN Gateway/FA/HAServing ASN BS, etc.
2	ASN BS sends DREG_CMD message to MS, including Action Code=0x00 to indicate MS existing network.
3	IP session for DHCP/MIP release starts between MS and network entities.
4	MS sends DREG_REQ to ASN BS with De-Registration_Request_Code=0x02.
5	ASN BS sends Path_Dereg_Req message to ASN Gateway.
6	ASN Gateway/FA and HA starts MIP release procedure.

Step	Description
7	ASN Gateway/FA exchanges NetExit_MS_State_Change_Req and NetExit_MS_State_Change_Rsp messages with the anchor accounting client, anchor authenticator, and MIP client to delete MS contexts.
8	ASN Gateway sends Accounting-Stop-Request (Release Indication) message to H-AAA.
9	AAA replies with Accounting-Stop-Response message to ASN Gateway.
10	ASN Gateway/FA replies with Path_Dereg_Response message to ASN BS.
11	ASN BS sends R6 Path_Dereg_Ack to the ASN Gateway and related entities releases the retained MS context and the assigned data path resource for the MS.

Intra-ASN Gateway Handover

This section describes the handover procedure between two ASN BSs connected to one ASN Gateway. The ASN Gateway supports following types of handover:

- Intra-anchor ASN Gateway Uncontrolled Handover
- Intra Non-anchor ASN Gateway Uncontrolled Handover
- Intra-anchor ASN Gateway Controlled Handover
- Intra Non-anchor ASN Gateway Controlled Handover

Details regarding controlled and uncontrolled handovers for the anchor ASN gateways are provided below.

Intra-anchor ASN Gateway Uncontrolled Handover

This section describes the procedure for an uncontrolled intra-anchor ASN Gateway handover for a WiMAX Subscriber MS.

The following figure provides a high-level view of the steps involved in an intra-anchor ASN Gateway uncontrolled handover of an SS/MS. The following table explains each step in detail.

Figure 14. Intra-ASN Gateway Uncontrolled Handover Call Flow

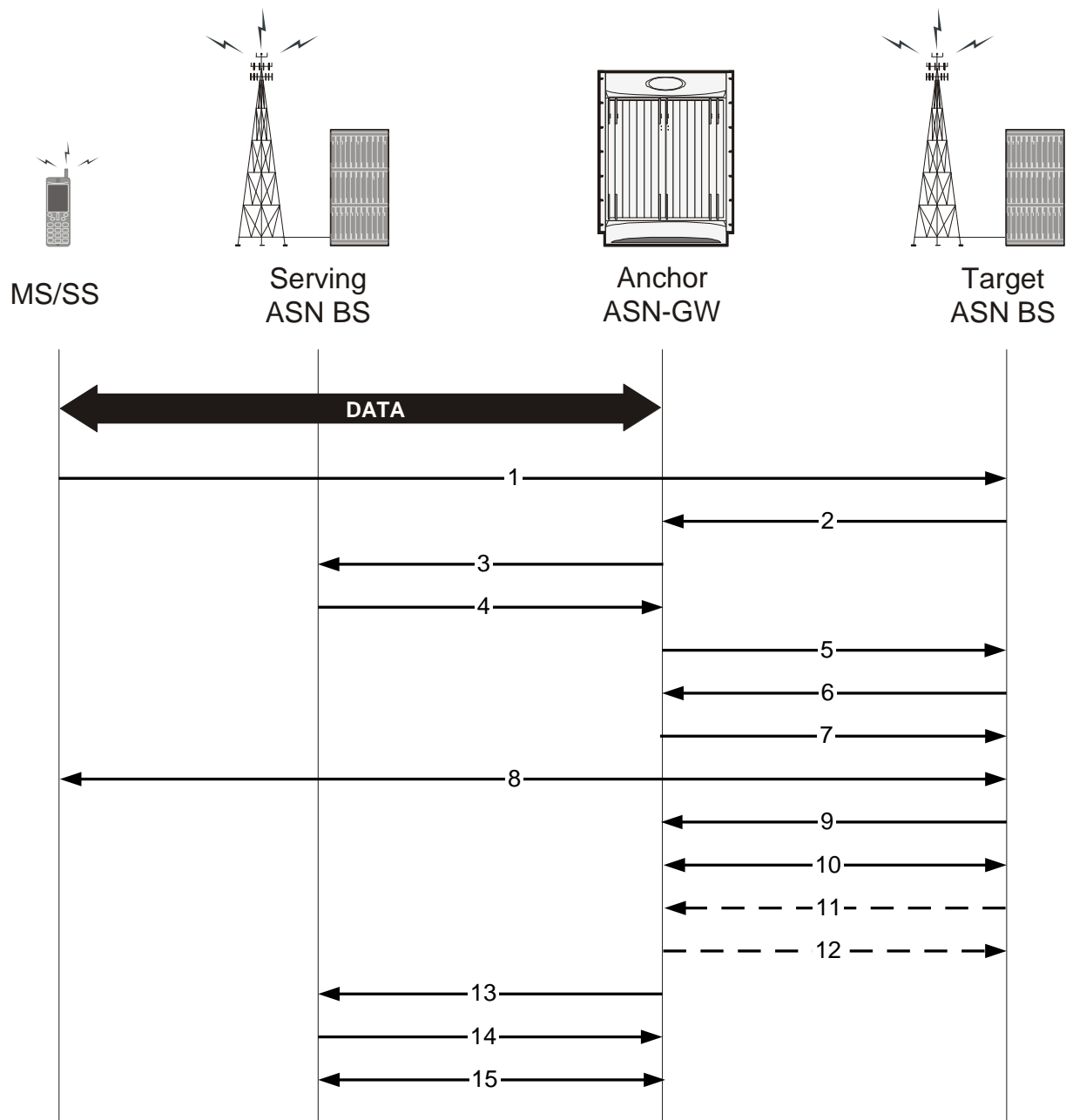


Table 5. Intra-ASN Gateway Uncontrolled Handover Call Flow Description

Step	Description
1	MS sends RNG-REQ message to target ASN BS.
2	Target ASN BS sends Context-Request message to anchor ASN Gateway for this MS.
3	Anchor ASN Gateway forwards Context-Request message to serving ASN BS.

Step	Description
4	Serving ASN BS sends Context-Report message with MS context information to anchor ASN Gateway.
5	Anchor ASN Gateway forwards Context-Report message with MS context information to target ASN BS.
6	Target ASN BS sends Path Registration Request to anchor ASN Gateway.
7	Anchor ASN Gateway replies with Path Registration Response to target ANS BS.
8	Target ANS BS sends ranging response with RNG_RSP message to MS.
9	Target ASN BS sends Path Registration Acknowledge to anchor ASN Gateway.
10	R6 GRE data path established between target ASN BS and anchor ASN Gateway and data flow starts.
11	Target ASN BS sends CMAC Key Count Update message to anchor ASN Gateway.
12	Anchor ASN Gateway replies with CMAC Key Count Update ACK message to target ASN BS.
13	Anchor ASN Gateway sends Path_De-Reg_Req message to release data path to serving BS.
14	Serving ASN BS sends Path_De-Reg_Rsp message to anchor ASN Gateway.
15	R6 GRE data path terminated between serving ASN BS and anchor ASN Gateway.

Intra-anchor ASN Gateway Controlled Handover

An intra-anchor ASN Gateway controlled handover consists of the following types and phases.

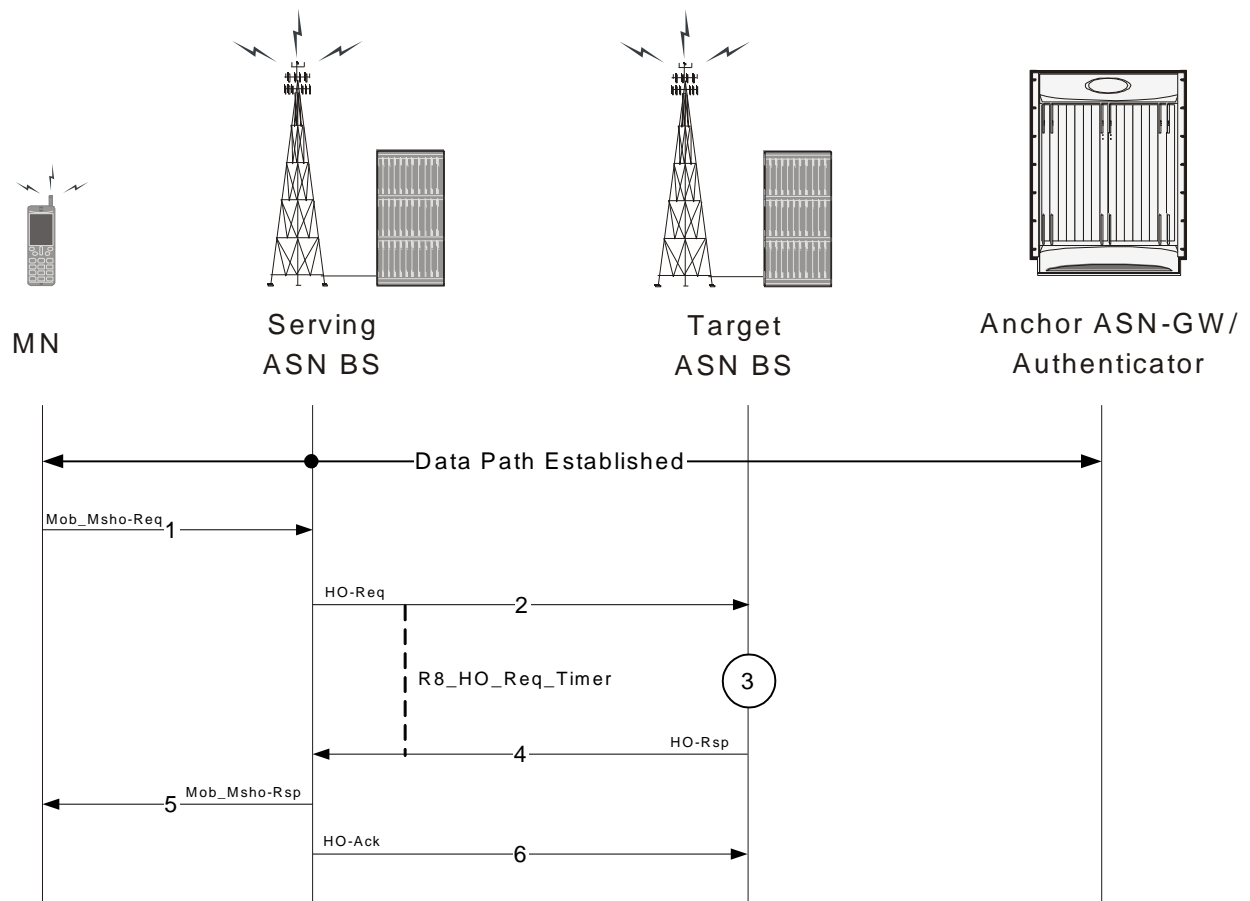
MS Initiated Intra-anchor ASN Gateway Controlled Handover

This section describes the intra-anchor ASN Gateway controlled handover between two base stations initiated by a mobile station.

HO Preparation Phase

This is the initial phase for a controlled handover between two BSs.

The following figure and table describe the call flow for the steps involved in an uncontrolled intra-ASN Gateway handover preparation phase between two BSs.

Figure 15. MS initiated Uncontrolled Intra-ASN Gateway Handover Preparation Phase**Table 6. MS initiated Uncontrolled Intra-ASN Gateway Handover Preparation Phase Description**

Step	Description
1	MS sends MOB_MSHO_REQ messages to serving BS
2	Upon receiving MS initiated handover request (MOB_MSHO_REQ), the serving BS sends HO_Req messages to target BS selected by MS and starts R8_HO_Req timer
3	Targeted BS tests the acceptability of the requested HO by comparing the amount of available resources and required bandwidth/QoS parameters in the HO request received from serving BS
4	Once a target BS accepts the request it sends the HO_Rsp message to the serving BS
5	Serving BS sends MOB_MSHO_RSP response to MS
6	Serving BS sends HO_Ack message to the target BS and HO preparation phase is completed

HO Action Phase

The following figure and table describe the call flow for the steps involved in uncontrolled intra-ASN Gateway handover action phase between two BSs.

Figure 16. MS initiated Uncontrolled Intra-ASN Gateway Handover Action Phase

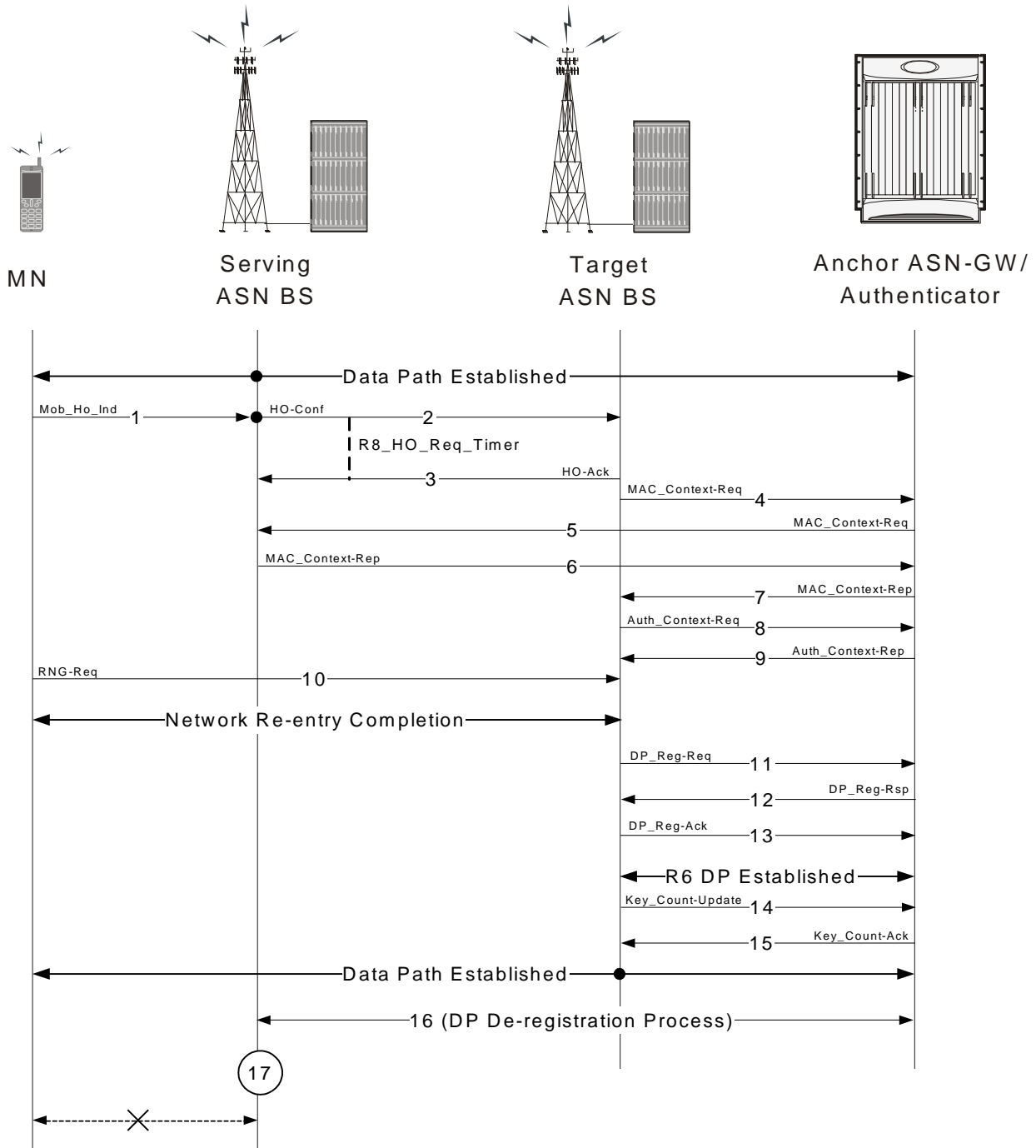


Table 7. MS initiated Uncontrolled Intra-ASN GW Handover Phase

Step	Description
1	Once HO preparation phase is completed and target BS receives HO-Ack message, the MS sends MOB_HO-IND messages to the serving BS.
2	The serving BS sends HO_Conf messages to the selected target BS with other context information and starts R8_HO_Confirm Timer.
3	The target BS accepts the request and sends the HO_Ack message to serving BS and serving BS stops R8_HO_Confirm Timer.
4	Target BS sends MAC Context Request message to the anchor ASN Gateway.
5	The anchor ASN Gateway forwards the MAC Context Request to the serving BS.
6	Serving BS sends MAC Context Report information to anchor ASN Gateway.
7	Anchor ASN Gateway forwards MAC Context Report information to the target BS.
8	Target BS sends Authentication Context Request to anchor ASN Gateway.
9	Anchor ASN Gateway transfers Authentication Context information to target BS.
10	MS starts ranging with target BS and sends RNG-REQ to the target BS and network reentry completed.
11	Target BS sends Data Path Registration Request to anchor ASN Gateway.
12	Anchor ASN Gateway sends Data Path Registration Response to target BS.
13	Target BS sends Data Path Registration Ack message to Anchor ASN Gateway and R6 data path is established.
14	Target BS sends CMAC Key count Update message to anchor ASN Gateway.
15	Anchor ASN Gateway sends CMAC Key Count Update Ack message to target BS and handover completed.
16	Anchor AS NGW starts Data Path De-registration process with serving BS.
17	Serving BS releases all resources and terminates data path with MS.

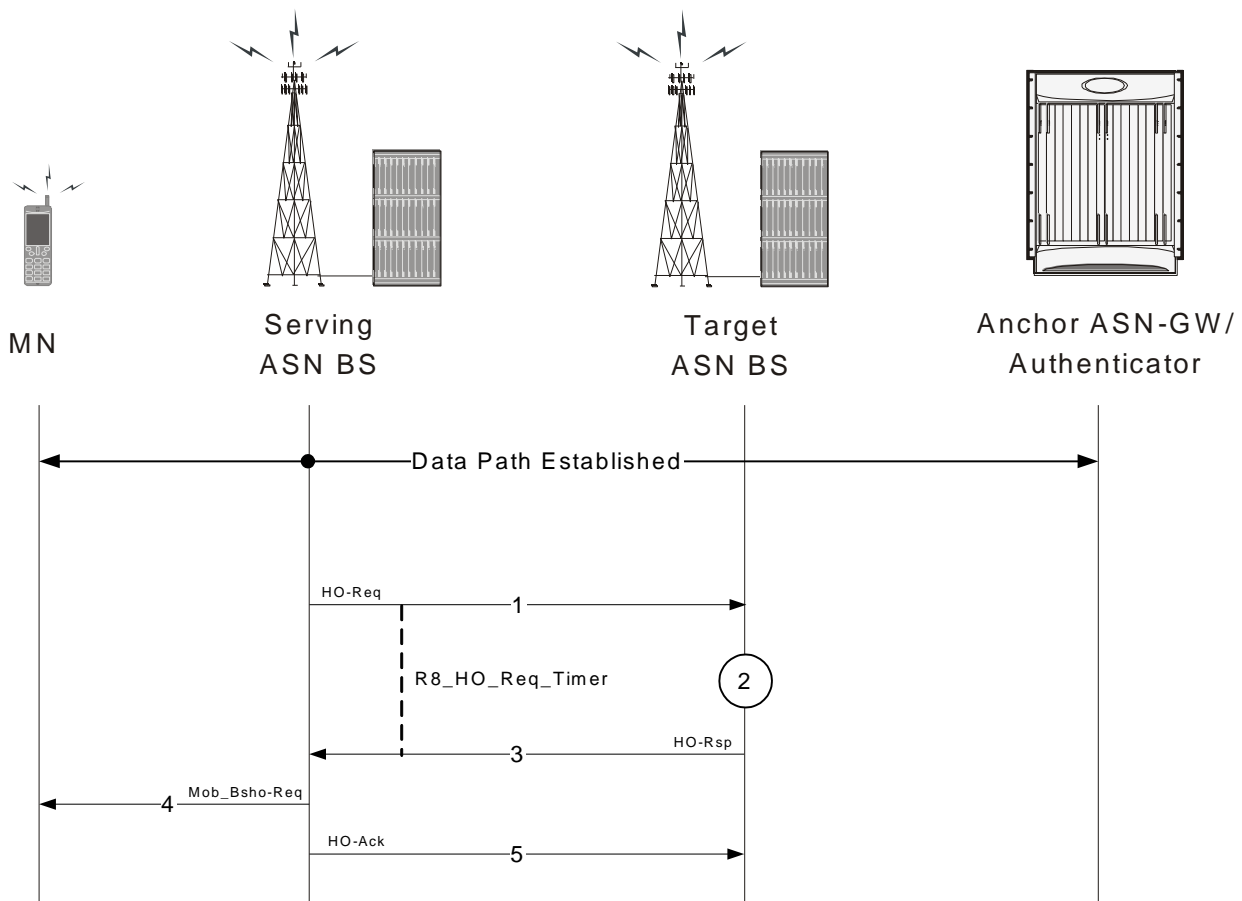
BS Initiated Intra Anchor ASN Gateway Controlled Handover

This section describes the intra-anchor ASN Gateway controlled handover between two base stations initiated by serving base station.

HO Preparation Phase

This is the initial phase for a controlled handover between two BSs.

The following figure and table describe the call flow for the steps involved in uncontrolled intra-ASN Gateway handover preparation phase between two BSs.

Figure 17. BS initiated Uncontrolled Intra-ASN Gateway Handover Preparation Phase**Table 8. BS initiated Uncontrolled Intra-ASN Gateway Handover Preparation Phase Description**

Step	Description
1	In BS initiated HO scenario, the serving BS sends HO_Req messages to target BS from its peer list and starts R8_HO_Req timer.
2	Targeted BS tests the acceptability of the requested HO by comparing the amount of available resources and required bandwidth/QoS parameters in the HO request received from serving BS.
3	Once a target BS accepts the request it sends the HO_Rsp message to the serving BS.
4	Serving BS sends MOB_MSHO_RSP response to MS.
5	Serving BS sends HO_Ack message to the target BS and HO preparation phase is completed.

HO Action Phase

The following figure and table describe the call flow for the steps involved in an uncontrolled intra-ASN Gateway handover action phase between two BSs.

Figure 18. BS initiated Uncontrolled Intra-ASN Gateway Handover Action Phase

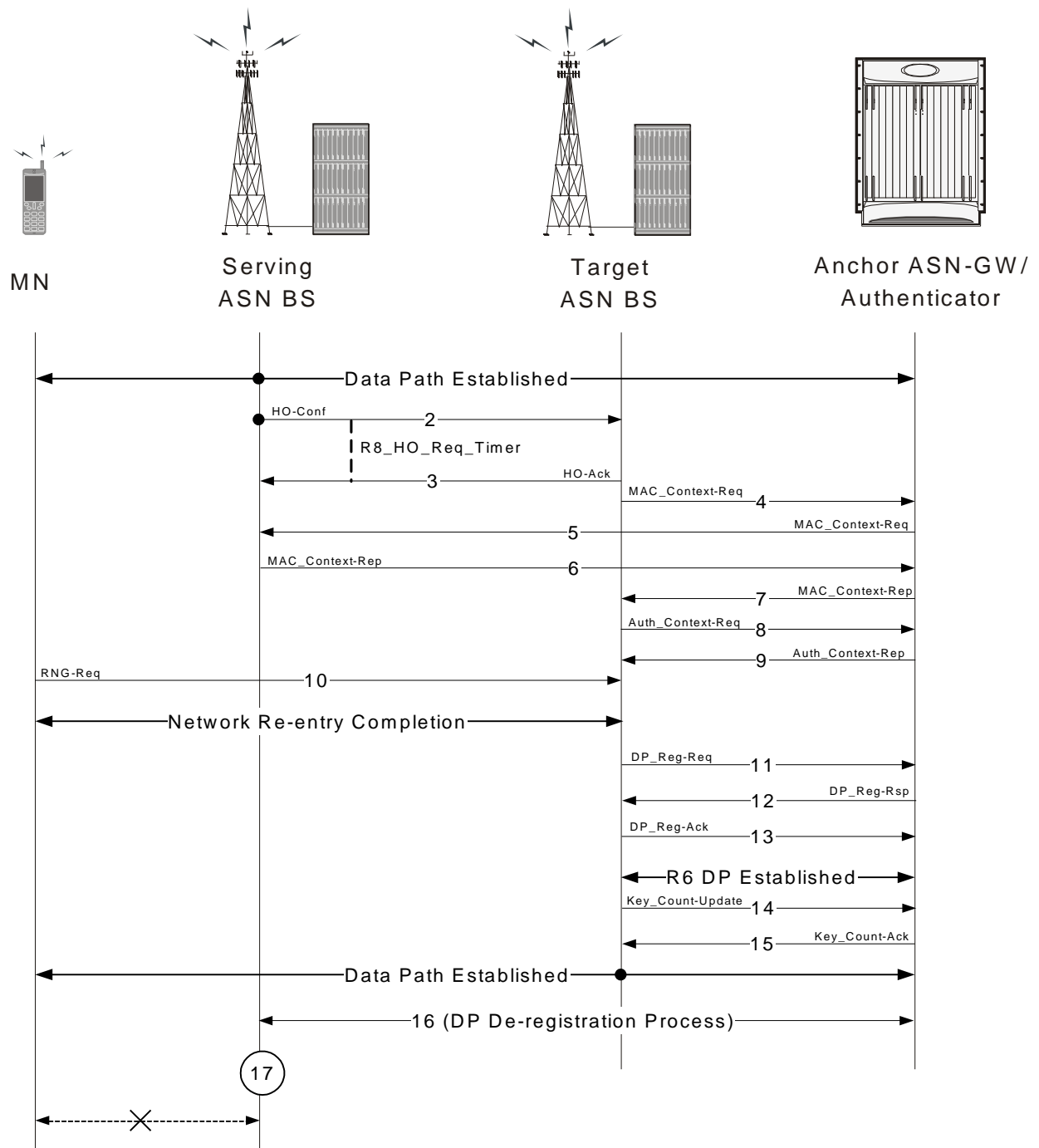


Table 9. BS initiated Uncontrolled Intra-ASN Gateway Handover Action Phase Description

Step	Description
1	Handover preparation phase is completed and data path is established.

Step	Description
2	The serving BS sends HO_Conf messages to the selected target BS with other context information and starts R8_HO_Confirm Timer.
3	The target BS accepts the request and sends the HO_Ack message to serving BS and serving BS stops R8_HO_Confirm Timer.
4	Target BS sends MAC Context Request message to the anchor ASN Gateway.
5	The Anchor ASN Gateway forwards the MAC Context Request to the serving BS.
6	Serving BS sends MAC Context Report information to anchor ASN Gateway.
7	Anchor ASN Gateway forwards MAC Context Report information to the target BS.
8	Target BS sends Authentication Context Request to anchor ASN Gateway.
9	Anchor ASN Gateway transfers Authentication Context information to target BS.
10	MS starts ranging with target BS and sends RNG-REQ to the target BS and network reentry completed.
11	Target BS sends Data Path Registration Request to anchor ASN Gateway.
12	Anchor ASN Gateway sends Data Path Registration Response to target BS.
13	Target BS sends Data Path Registration Ack message to anchor ASN Gateway and R6 data path established.
14	Target BS sends CMAC Key count Update message to anchor ASN Gateway.
15	Anchor ASN Gateway sends CMAC Key Count Update Ack message to target BS and handover completed.
16	Anchor AS NGW starts Data Path De-registration process with serving BS.
17	Serving BS releases all resources and terminates data path with MS.

Inter-ASN Gateway Handover

This section describes the procedure of inter-ASN Gateway handovers through an R4 interface for a WiMAX Subscriber Station (SS). The R4 reference is the interface over which ASN control and data messages are exchanged between two ASN Gateways, either within the same ASN or across separate ASNs.

For a given subscriber, a WiMAX session may be handled by ASN Gateway functions located in different physical nodes in the network. For example, the authenticator and FA may be located in ASN Gatewayx and the R6 Data Path Function in ASN Gatewayy. The various ASN Gateway functions communicate over the R4 interface.

The following inter-ASN Gateway handover scenarios are supported on the ASN Gateway over the R4 interface:



Important: Not all features are supported on all platforms.

- Controlled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover
- Controlled Non-Anchor ASN Gateway to Anchor ASN Gateway Handover
- Controlled Non-Anchor ASN Gateway to Non-Anchor ASN Gateway Handover

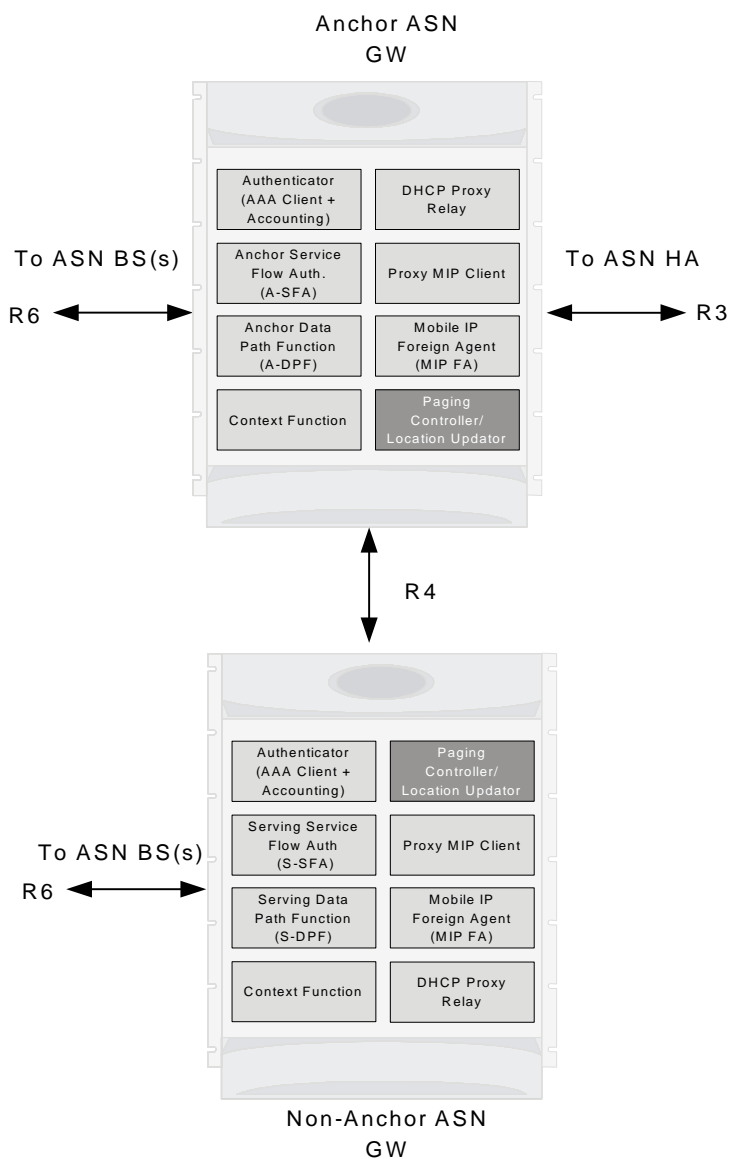
- Uncontrolled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover
- Uncontrolled Non-Anchor ASN Gateway to Anchor ASN Gateway Handover
- Uncontrolled Non-Anchor ASN Gateway to Non-Anchor ASN Gateway Handover

ASN Gateway Function for Handovers

An ASN Gateway configured for inter-ASN Gateway handovers requires the following functionality to support the handover via an R4 interface.

The following figure provides a high-level view of the components and functions distribution in ASN Gateway.

Figure 19. Distribution of Components and Function in ASN Gateway for Handover



Controlled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover

For Controlled handovers, the ASN Gateway provides and/or supports the following functions:

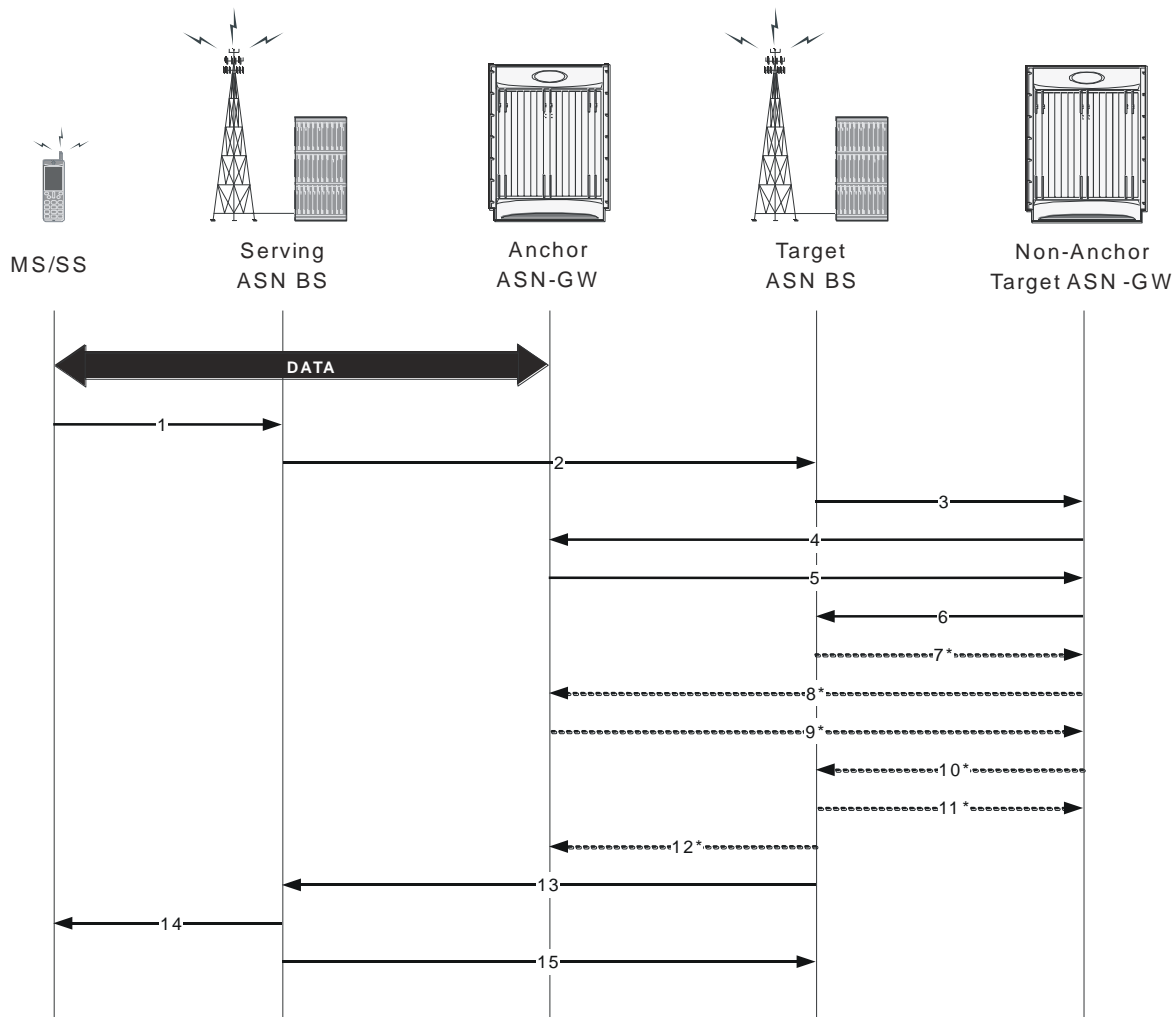
- **Message Relay:** The ASN Gateway provides the passive relay function for HO Request, HO Response, HO Ack, HO Confirm, and HO Complete messages in a stateless fashion. The gateway keeps the statistics of the different types of messages it has relayed. Retransmission of these messages is handled by the BS.

The serving BS generates these messages. The serving BS generates a different HO Request transaction for each target BS. In other words, the gateway does not generate multiple HO Request messages after receiving a single HO Request message with multiple target BSs. Generally, the HO transaction is initiated by the serving BS which also chooses the selected target BS to which the handover will take place.

- **Security Context Retrieval:** The ASN Gateway supports the retrieval of the security context using Context Request and Context Report messages. This retrieval is also stateless. The context retrieval operation can be performed at any time during the lifetime of a call.
- **Data Path Registration:** After Pre-Registration, the target BS performs Data Path Registration. Data Path Registration is performed using a 3-way handshake. If Pre-Registration has occurred, the Data Path Registration messages do not contain any service flow information.
 - If Pre-Registration has not occurred, the Data Path Registration messages carry the service flow information.
 - Data Path Pre-Registration and Data Path Registration is initiated by the BS.

Preparation Phase

The following figure and table provides a high-level view of the steps involved during the preparation phase of a controlled inter-ASN Gateway handover of an SS/MS from an anchored gateway to a non-anchored gateway.

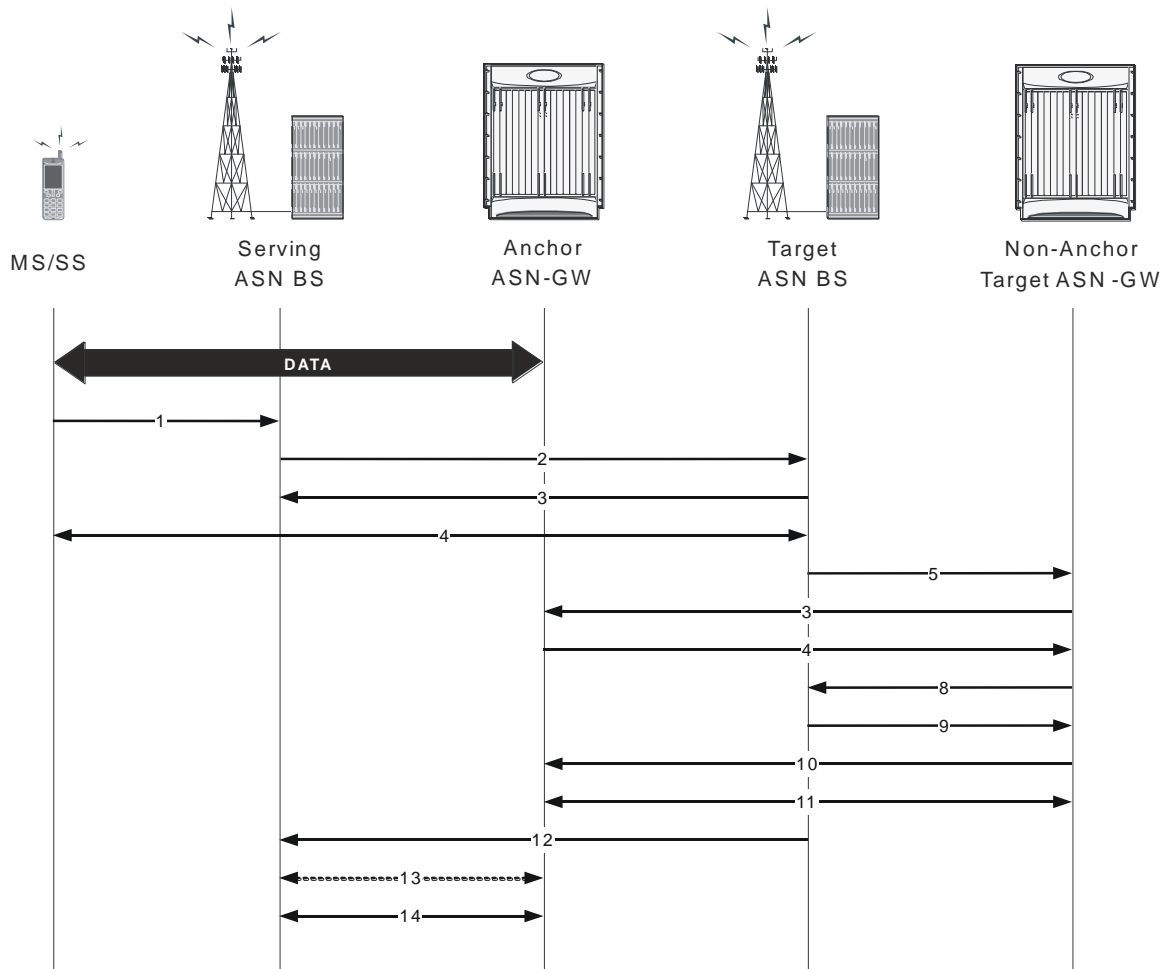
Figure 20. Controlled Inter-ASN Gateway Handover Procedure - Preparation Phase**Table 10. Controlled Inter-ASN Gateway Handover Procedure - Preparation Phase Description**

Step	Description
1	MS sends a MOB_MSHO-REQ message to the serving ASN BS.
2	Serving ASN BS sends a Handover Request message to the target ASN BS.
3	Target ASN BS sends a Context-Request message to the target non-anchor ASN Gateway for this MS.
4	Target non-anchor ASN Gateway forwards the Context-Request message to the anchor ASN Gateway.
5	Anchor ASN Gateway sends a Context-Report message to the target non-anchor ASN Gateway.
6	Target non-anchor ASN Gateway forwards the Context-Report message to the target ASN BS.
7	Target ASN BS sends a Path Pre-Registration Request message to the target non-anchor ASN Gateway. Pre-registration is optional.

Step	Description
8	Target non-anchor ASN Gateway forwards the Path Pre-Registration Request message to the anchor ASN Gateway. Pre-registration is optional.
9	Anchor ASN Gateway sends a Path Pre-Registration Response message to the target non-anchor ANS GW. Pre-registration is optional.
10	Target non-anchor ASN Gateway forwards the Path Pre-Registration Response message to the target ASN BS. Pre-registration is optional.
11	Target ASN BS sends a Path Pre-Registration Acknowledge message to the target non-anchor ASN Gateway. Pre-registration is optional.
12	Target non-anchor ASN Gateway forwards the Path Pre-Registration Acknowledge message to the anchor ASN Gateway. Pre-registration is optional.
13	Target BS sends a Handover Response message to the serving BS.
14	Serving BS sends a MOB_BSHO-RSP message to the MS.
15	Serving BS sends a Handover Acknowledge message to the target BS.

Action Phase

The following figure and table provides a high-level view of the steps involved during the action phase of a controlled inter-ASN Gateway handover of an SS/MS from an anchored gateway to a non-anchored gateway.

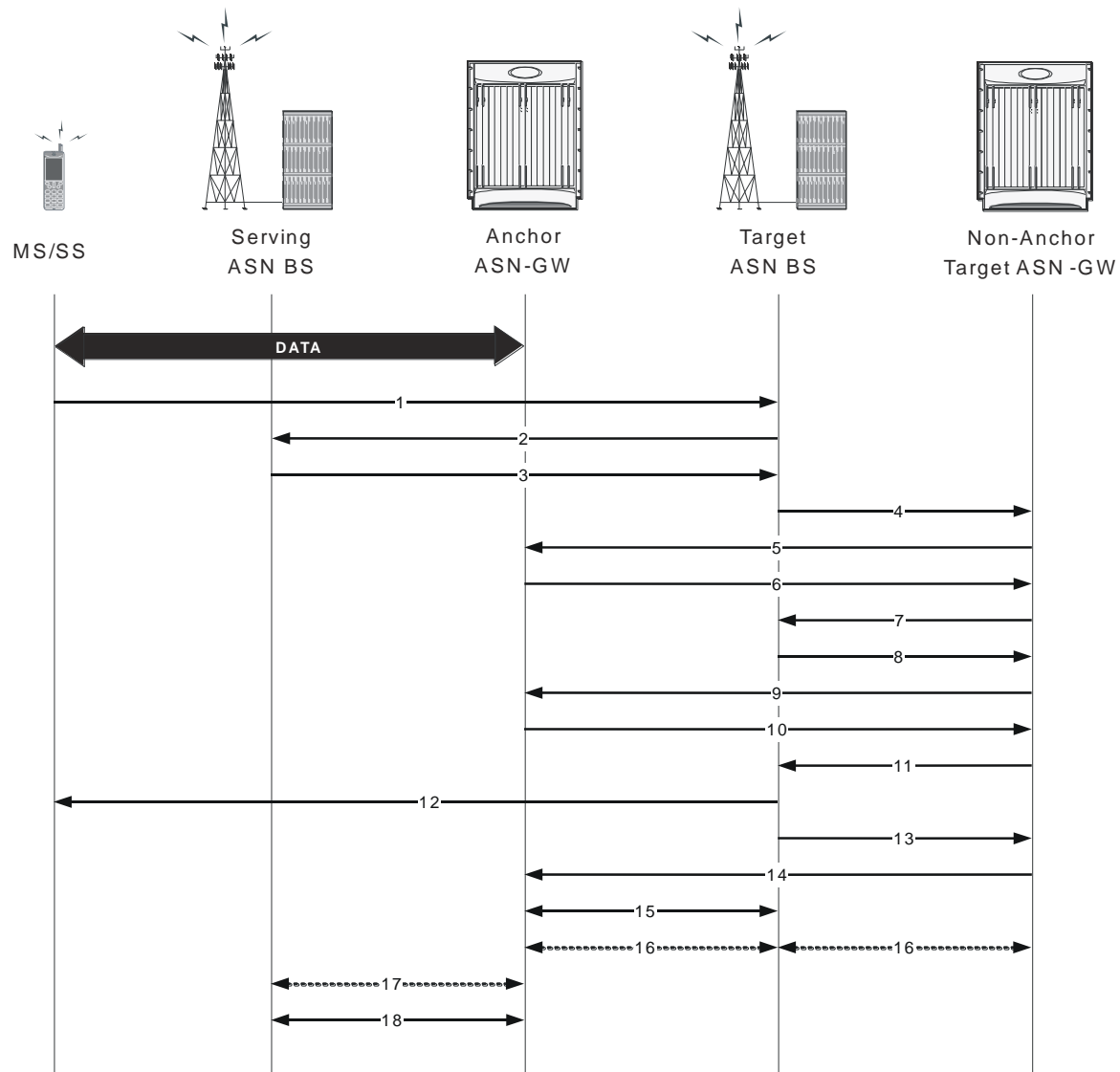
Figure 21. Controlled Inter-ASN Gateway Handover Procedure - Action Phase**Table 11. Controlled Inter-ASN Gateway Handover Procedure - Action Phase Description**

Step	Description
1	MS sends a MOB_MSHO-IND message to the serving ASN BS.
2	Serving ASN BS sends a Handover Confirm message to the target ASN BS.
3	Target ASN BS sends a Handover Acknowledge message to the serving ASN BS.
4	MS moves off of the serving ASN Gateway and re-enters the network through target ASN BS.
5	Target ASN BS sends a Path Registration Request message to the target non-anchor ASN Gateway.
6	Target non-anchor ASN Gateway forwards the Path Registration Request message to the anchor ASN Gateway.
7	Anchor ASN Gateway sends a Path Registration Response message to the target non-anchor ANS GW.
8	Target non-anchor ASN Gateway forwards the Path Registration Response message to the target ASN BS.
9	Target ASN BS sends a Path Registration Acknowledge message to the target non-anchor ASN Gateway.

Step	Description
10	Target non-anchor ASN Gateway forwards the Path Registration Acknowledge message to the anchor ASN Gateway.
11	Target non-anchor ASN Gateway sends/receives CMAC Key Count Update and Acknowledge messages to/from anchor ASN Gateway.
12	Target ASN BS sends a Handover Complete message to the serving ASN BS.
13	Anchor ASN Gateway sends/receives Path De-Reg Req/Rsp/Ack messages (to release the data path) to/from Serving BS.
14	R6 GRE data path terminated between Serving ASN BS and Anchor ASN Gateway.

Uncontrolled Anchor ASN Gateway to Non-Anchor ASN Gateway Handover

The following figure and table provides a high-level view of the steps involved in an uncontrolled inter-ASN Gateway handover of an SS/MS from an anchored gateway to a non-anchored gateway.

Figure 22. Uncontrolled Inter-ASN Gateway Handover Procedure**Table 12. Uncontrolled Inter-ASN Gateway Handover Procedure Description**

Step	Description
1	MS sends RNG-REQ message to target ASN BS.
2	Target ASN BS sends Context-Request message to serving ASN BS.
3	Serving ASN BS sends Context-Report message with MS context information to target ASN BS.
4	Target ASN BS sends Context-Request message to target non-anchor ASN Gateway.
5	Target non-anchor ASN Gateway forwards Context-Request message to anchor ASN Gateway.
6	Anchor ASN Gateway sends Context-Report message with MS context information to target non-anchor ASN Gateway.

Step	Description
7	Target non-anchor ASN Gateway forwards Context-Report message to target ASN BS.
8	Target ASN BS sends Path Registration Request to target non-anchor ASN Gateway.
9	Target non-anchor ASN Gateway forwards Path Registration Request to anchor ASN Gateway.
10	Anchor ASN Gateway replies with Path Registration Response to target non-anchor ANS GW.
11	Target non-anchor ASN Gateway forwards Path Registration Response to target ASN BS.
12	Target ANS BS sends ranging response with RNG_RSP message to MS.
13	Target ASN BS sends Path Registration Acknowledge to target non-anchor ASN Gateway.
14	Target non-anchor ASN Gateway forwards Path Registration Acknowledge to anchor ASN Gateway.
15	R6 GRE data path established between Target ASN BS and anchor ASN Gateway. Data flow starts.
16	Target ASN BS sends/receives CMAC Key Count Update and Acknowledge messages to/from anchor ASN Gateway via target non-anchor ASN Gateway.
17	Anchor ASN Gateway sends/receives Path De-Reg Req/Rsp/Ack messages to release data path to/from serving BS.
18	R6 GRE data path terminated between Serving ASN BS and anchor ASN Gateway.

RADIUS-based Prepaid Accounting for WiMax

Online accounting is set up by the exchange of RADIUS Access-Request and Access-Accept packets. The initial Access-Request packet from the ASN GW and/or the home agent includes a prepaid accounting capability (PPAC) vendor specific attribute too the prepaid server (PPS). This indicates support for online accounting at the ASN and/or the home agent. If the subscriber's session requires online charging, the PPS assigns a prepaid accounting quota (PPAQ) to the PPC with RADIUS Access-Accept packets. As the session continues, the PPC and the PPS replenish the quotas by exchanging RADIUS packets.

Note the following:

- ASN GW operates as the prepaid client (PPC).
- In the case of a mobile IP call, both the ASN GW and the home agent work independently as the prepaid client. Both the ASN GW and the home agent send online access requests to the configured RADIUS servers independently.
- Only session-based online accounting is supported.

Obtaining More Quota after the Quota is Reached

The following figure and table provide a high-level view of the steps involved in allocating additional quotas for prepaid calls once the original quota is reached.

Figure 23. Call Flow Showing How Additional Quota is Obtained

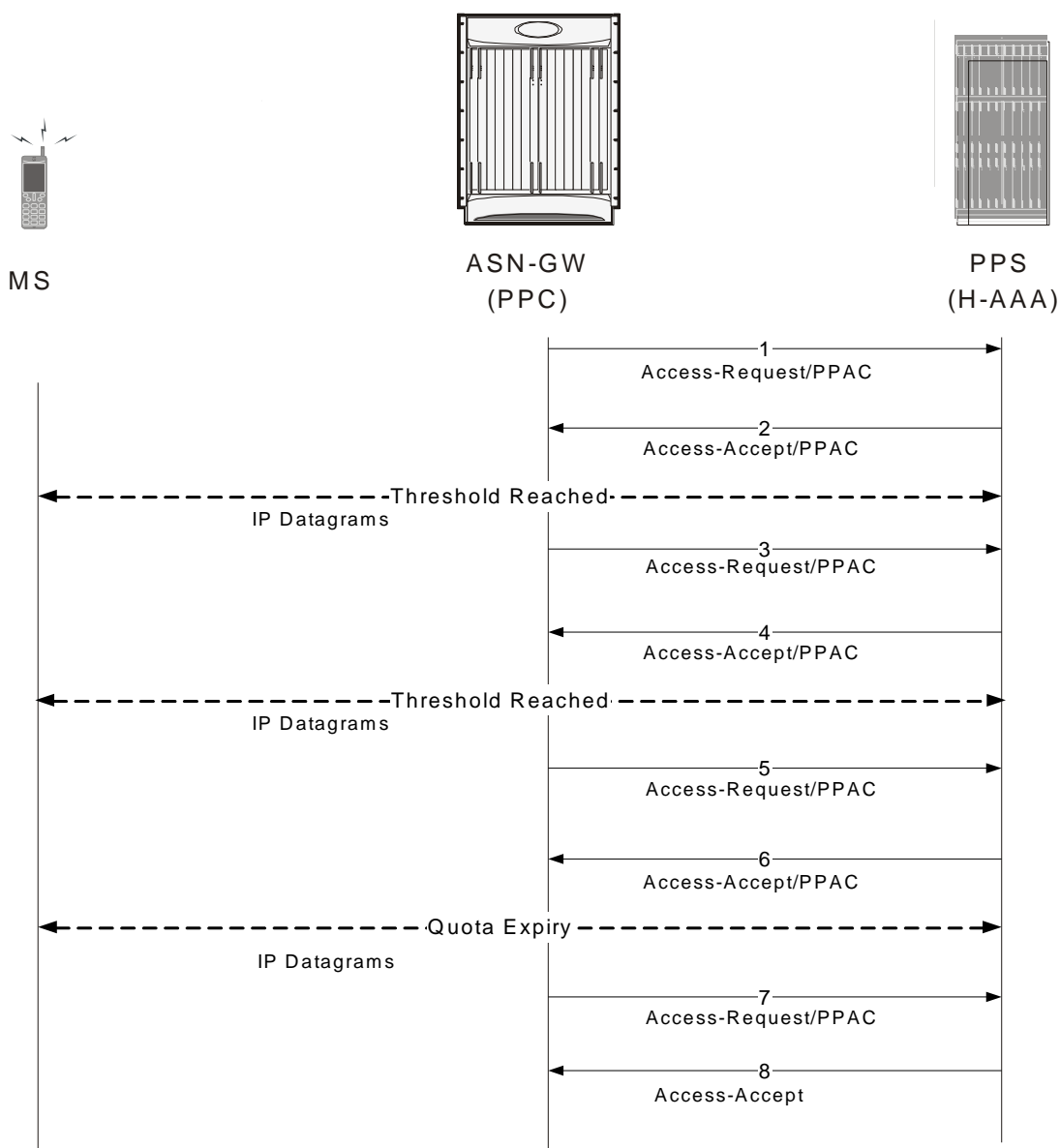


Table 13. Call Flow Showing How Additional Quota is Obtained

Step	Description
1	During network entry, a NAS sends an Access-Request packet to the HCSN. If the NAS supports a PPC, the NAS includes the PPAC attributes, indicating it prepaid capabilities.
2	If the subscriber session is a prepaid session, the PPS (HAAA) assigns the initial prepaid quota(s) by including one or more PPAQ attributes in the Access-Accept packet.
3	Once the threshold for the quota(s) is reached, the PPC sends an Authorize-Only Access-Request to request additional quota. The request contains one or more PPAQs that indicate which quota(s) need to be replenished to the PPS.

Step	Description
4	The PPS responds with an Access-Accept packet that contains one or more replenished quotas.
5	Once again, a threshold is reached for one or more of the quotas. The PPC sends an Authorize-Only Access-Request to the PPS to request more quota.
6	The PPS responds with the final quota in an Access-Accept. The final quota is indicated by the presence of the Terminate-Action subtype. The Terminate-Action subtype includes the action for the PPC to take once the quota is reached.
7	The quota expires. The PPC sends an Authorize-Only Access-Request packet to indicate that the quota has expired.
8	The PPS responds with an Access-Accept. If there are additional resources, the PPS allocates additional quotas and the service continues.

Applying HTTP Redirection Rule when Quota is Reached

The following figure and table provide a high-level view of the steps showing how the HTTP Redirection Rule is applied once a quota is reached.

Figure 24. Call Flow for Applying HTTP Redirection Rule on Quota-Reach

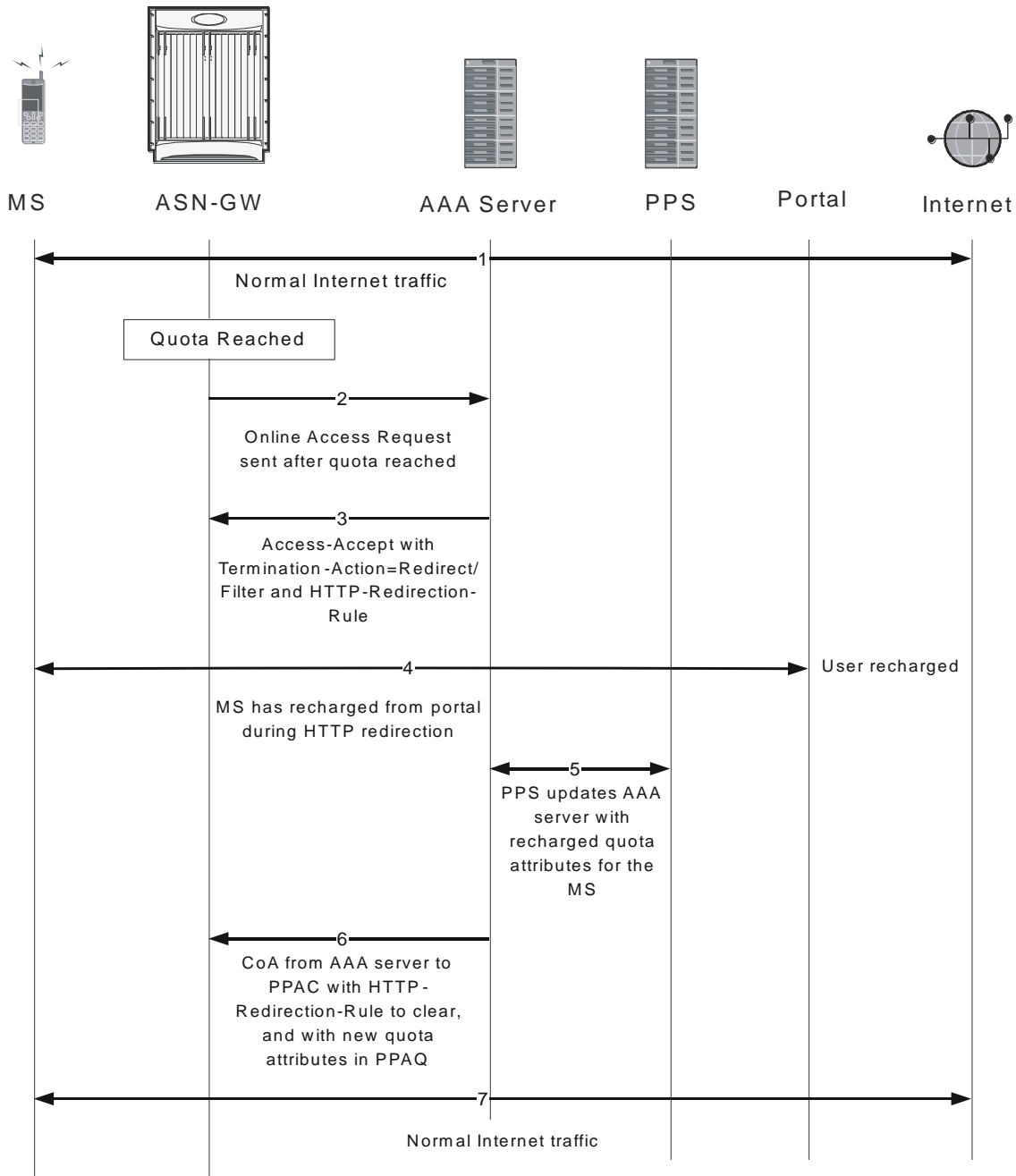


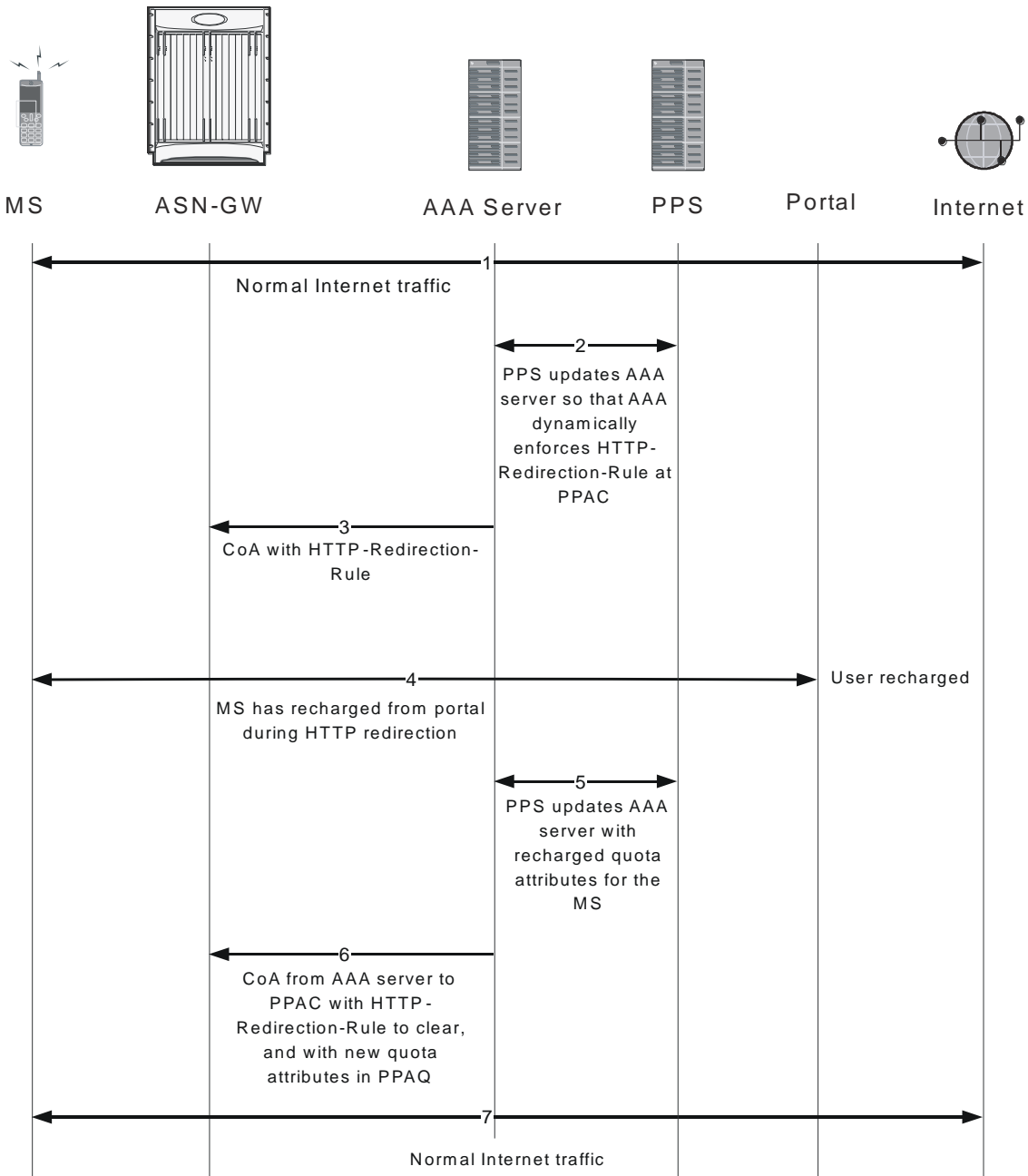
Table 14. Call Flow for Applying HTTP Redirection Rule on Quota-Reach

Step	Description
1	The Volume or Duration quota is reached. The Termination-Action is Request More Quota.
2	The PPC sends an Online Access Request to the AAA server and waits for Access-Accept.

Step	Description
3	The Access-Accept is received. It contains no additional quota attributes. The Termination-Action is Redirect/Filter. There is an HTTP Redirection Rule with redirect rule present in the Access-Accept.
4	The PPC (home agent) applies the HTTP Redirection Rule for the HTTP traffic. All other traffic is dropped. During this period, the MS recharges from the portal.
5	The PPC sends updated quota attributes to the AAA server based on the MS recharge from the portal.
6	The AAA server sends a CoA message to the PPC (home agent) with the new quota attributes in PPAQ and also sends the HTTP Redirection Rule to clear the HTTP Redirection rule at the PPC.
7	Normal traffic, including HTTP traffic, is allowed, per the new quota attributes.

Applying HTTP Redirection Rule CoA is Received

The following figure and table show the steps involved in applying the HTTP Redirection Rule when the PPAC receives a change of authorization (CoA) from a AAA server.

Figure 25. Call Flow for Applying HTTP-Redirection Rule when CoA is Received**Table 15. Call Flow for Applying HTTP-Redirection Rule Received by CoA**

Step	Description
1	The PPS updates the AAA server so that the AAA server dynamically enforces HTTP Redirection Rule at the PPC.
2	The AAA server sends a CoA message to the PPC (home agent) with the HTTP Redirection Rule.

Step	Description
3	The PPC (home agent) applies the HTTP Redirection Rule for the HTTP traffic. All other traffic is dropped. During this period, the MS is recharged from the portal.
4	The PPC sends updated quota attributes to the AAA server based on the MS recharge from the portal.
5	The AAA server sends a CoA message to the PPC (home agent) with the new quota attributes in PPAQ and also sends the HTTP Redirection Rule to clear the HTTP Redirection rule at the PPC.
6	Normal traffic, including HTTP traffic, is allowed, per the new quota attributes.

Terminating the Call when Quota is Reached

The following figure and table provide a high-level view of the steps involved in allocating additional quotas for prepaid calls once the original quota is reached.

Figure 26. Call Flow for Terminating the Call on Quota-Reach

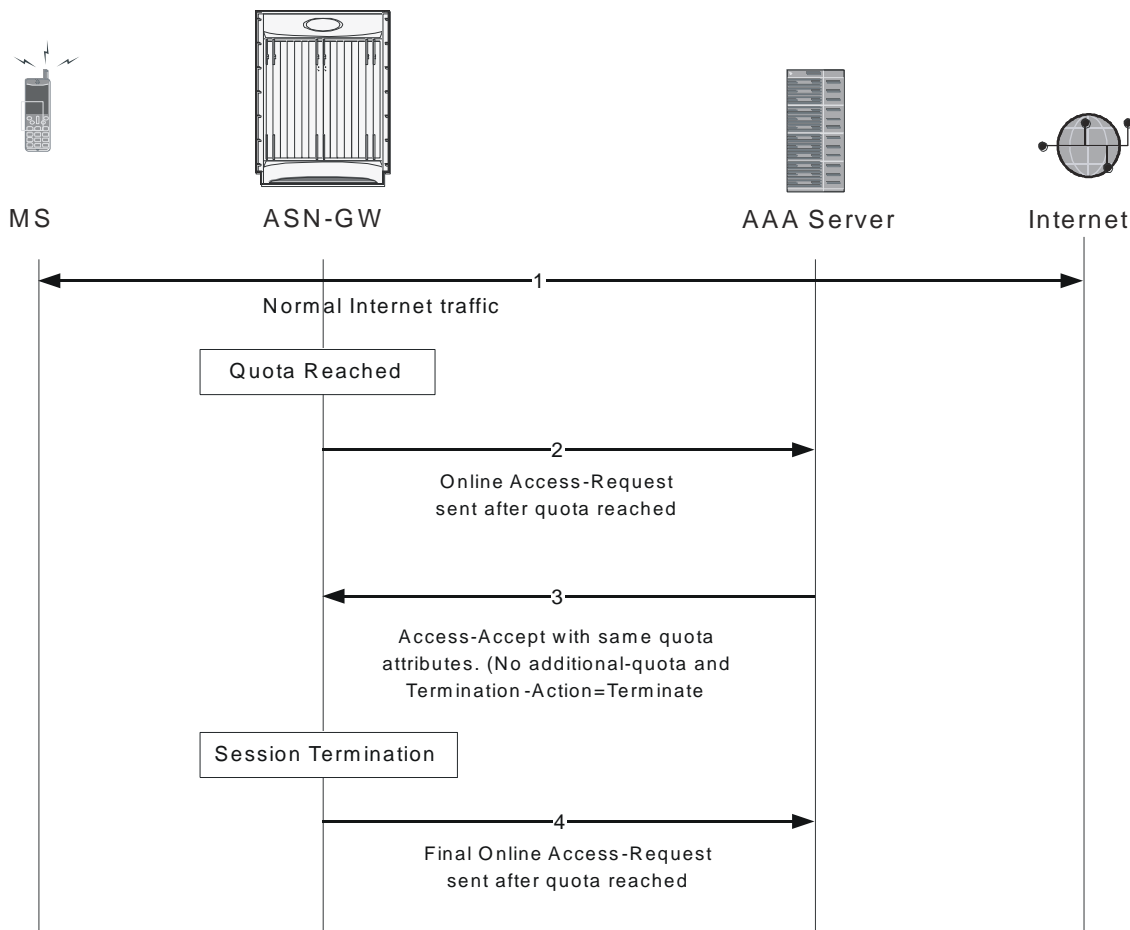


Table 16. Call Flow for Terminating the Call on Quota-Reach

Step	Description
1	Volume or Duration quota is reached. If the termination-action is Request-More-Quota, step 2 occurs next. If termination-action is Terminate, step 4 occurs next.
2	If the termination-action is Request-More-Quota, the PPC sends an Online-Access-Request to the AAA server and waits for Access-Accept.
3	The PPC receives the Access-Accept, which contains no additional quota attributes.
4	Session is terminated at the PPC (home agent) and at the ASN GW.
5	The PPC sends the final Online-Access-Request.

CSN Procedure Flows

This section provides an overview of CSN procedure and working of ASN Gateway in CSN procedure.

Following procedures are discussed in this section:

PMIP4 Connection Setup and Call Flow with DHCP Proxy

This section describes the CSN procedure of simple IP with DHCP proxy triggering PMIPv4 for a WiMAX subscriber.

The following figure and table provide a high-level view of the steps involved in PMIP4 connection and call flow of an SS/MS.

Figure 27. PMIP4 Connection Setup Call Flow

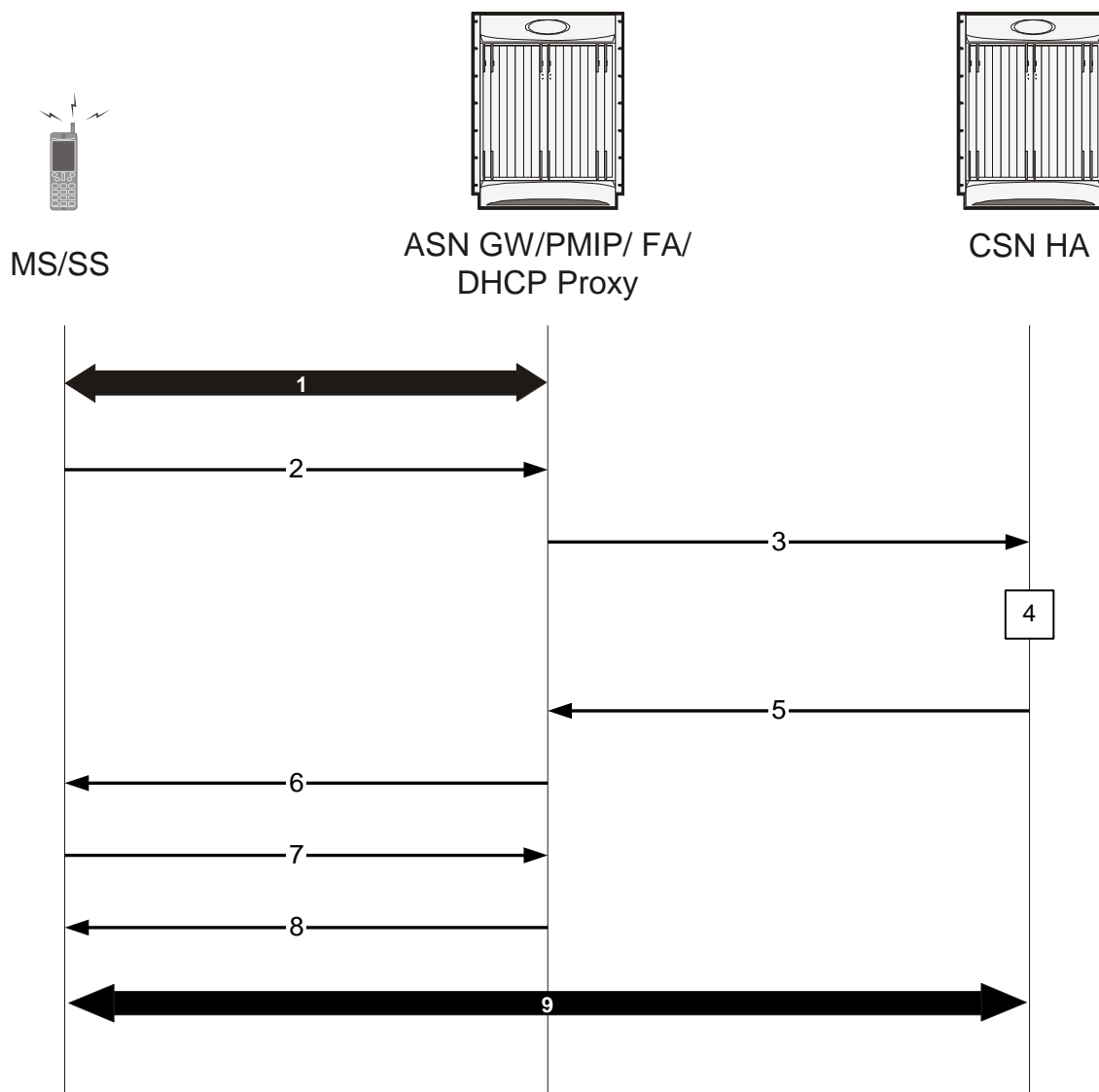


Table 17. PMIP4 Connection Setup Call Flow Description

Step	Description
1	Initial network entry completed as described in ASN Procedures.
2	MS sends DHCP DISCOVER message to DHCP Proxy (co-located with ASN Gateway) to discover a DHCP server for IP host configuration.
3	Upon receiving the DHCP DISCOVER message, the DHCP Proxy in the NAS triggers the PMIP4 client to initiate the Mobile IPv4 Registration procedure. The PMIP4 client uses the HoA information and constructs a Mobile IPv4 Registration Request message and sends the Mobile IPv4 Registration Request to the FA address. The FA forwards the registration request to the CSN HA.

Step	Description
4	CSN HA processes the MIPv4 Registration Request.If a HoA is 0.0.0.0 in the Mobile IP Registration Request message, the HA assigns a HoA. Otherwise, the HoA in the Mobile IP Registration Request message is used.
5	The HA responds with the Mobile IP Registration Response message.The source address for this Mobile IPv4 message over R3 is HA, and the destination address is FA-CoA.The FA forwards the message to the PMIP4 client. The PMIP4 client passes this information to the DHCP proxy.
6	The DHCP proxy sends the DHCP OFFER message to the MS.
7	MS sends a DHCP REQUEST to the DHCP Proxy with the information received in the DHCP OFFER.
8	The DHCP Proxy acknowledges the use of this IP address and other configuration parameters by sending the DHCP ACK message.
9	WiMAX session established between MS and CSN HA.

PMIP4 Session Release

This section describes the CSN procedure of PMIPv4 session release during a WiMAX subscriber session.

The following figure and table provide a high-level view of the steps involved in PMIPv4 session release and termination of connection an SS/MS.

Figure 28. PMIP4 Session Release Call Flow

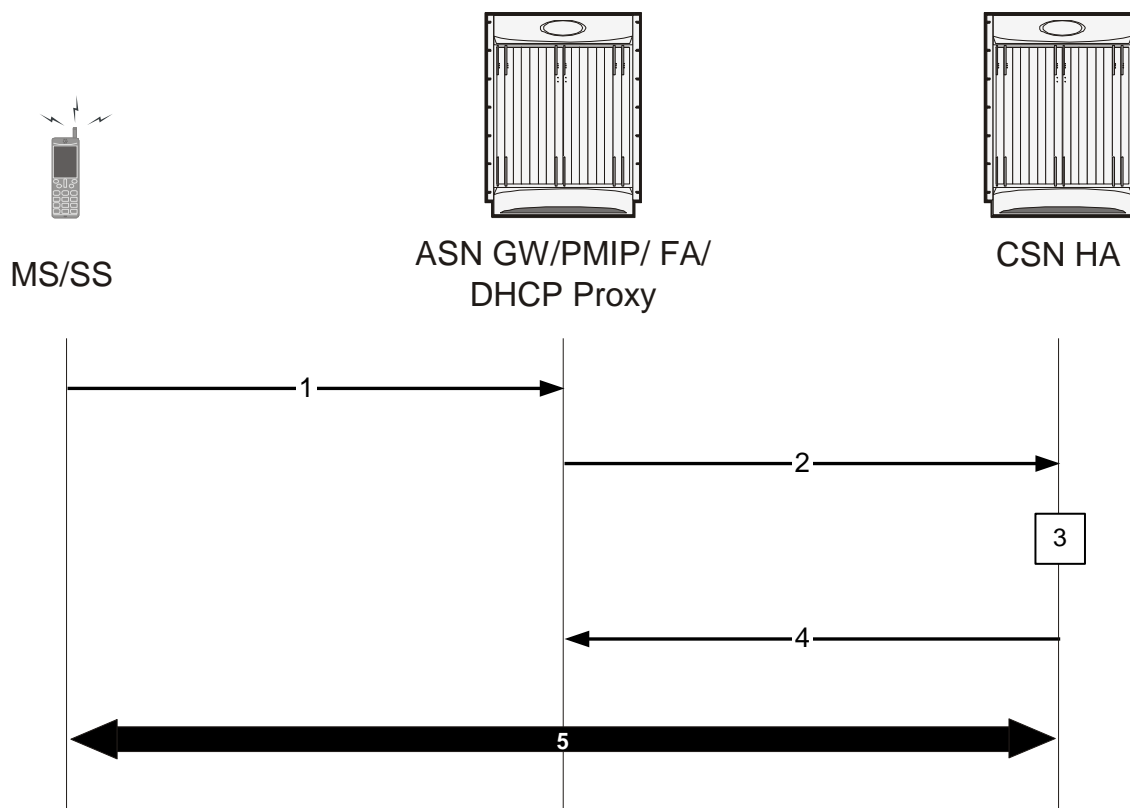


Table 18. PMIP4 Session Release Call Flow Description

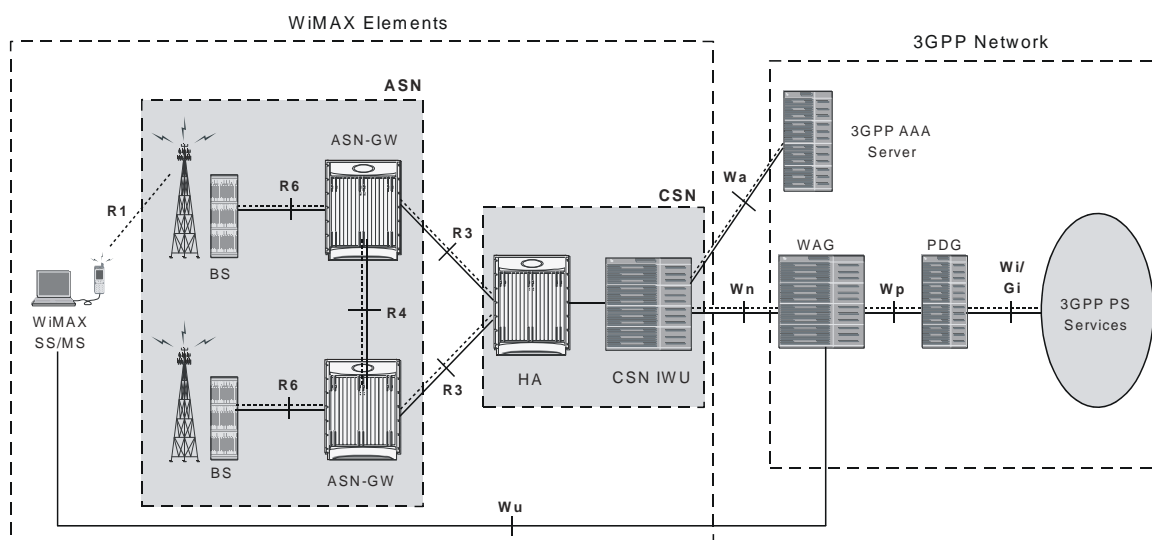
Step	Description
1	The session release trigger send by MS sending DHCP-Release message to the ASN GS or DHCP proxy has expired on lease time or FA initiates session release.
2	ASN Gateway initiates the session release with PMIPv4 client by sending FA_Revoke_Req and sends PMIP De-Reg RRQ (Registration Revocation) message to CSN HA.
3	CSN HA starts release of MIP binding.
4	CSN HA sends PMIP De-Reg RRQ (Registration Revocation) message to ASN Gateway and PMIP client sends GA_Revoke_Rsp message to ASN Gateway.
9	WiMAX session terminated between MS and CSN HA.

WiMAX Deployment with Legacy Core Networks

ASN Gateway Interoperability with 3GPP Overlay

The following figure shows a typical interoperability scenario between WiMAX and 3GPP legacy networks with reference points and interfaces.

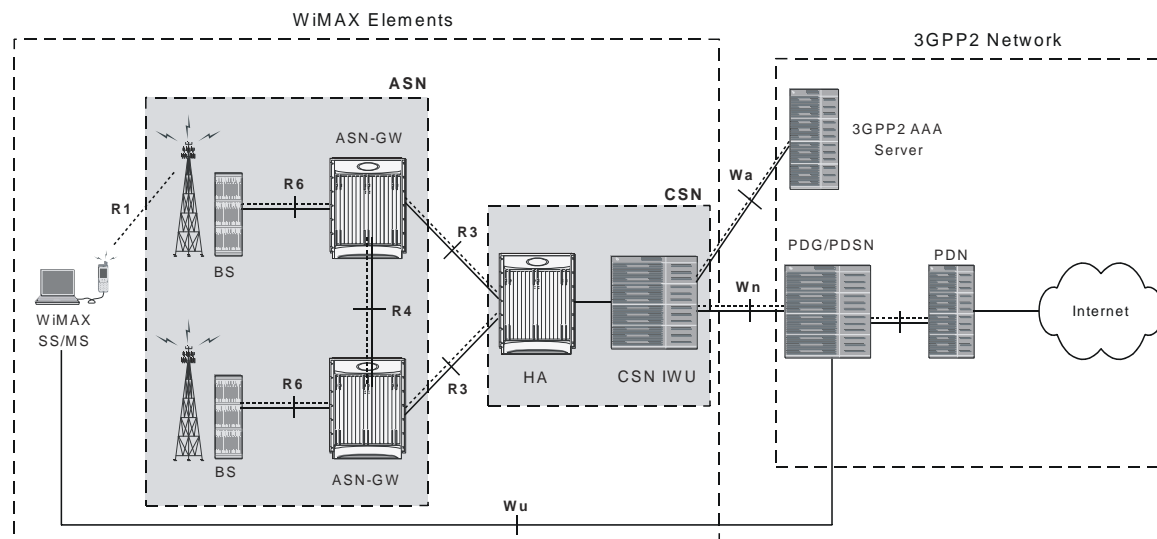
Figure 29. ASN Gateway with 3GPP Overlay



ASN Gateway Interoperability with 3GPP2 Overlay

The following figure shows a typical interoperability scenario between WiMAX and 3GPP2 legacy networks with reference points and interfaces.

Figure 30. ASN Gateway with 3GPP2 Overlay



Session Continuity Support for 3GPP2 and WiMAX Handovers

This feature provides seamless 3GPP2 session mobility for WiMAX subscribers and other access technology subscribers. With the implementation of this feature, the HA can be configured for:

- 3GPP2 HA service
- 3GPP HA service
- WiMAX HA service
- A combination of 3GPP2 and WiMAX HA services

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 impact from a user 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

For more information on this support, refer to the HA Administration Guide.

Supported Standards

WiMAX/IEEE References

- WiMAX ASN Profiles, WiMAX Forum
- Initial Network Entry Stage 3 Draft Specification WiMAX Forum
- Procedures and Messages for ASN Anchored Mobility with Profile C: Stage 3 draft, WiMAX Forum
- Procedures for CSN Anchored Mobility Stage 3 draft, WiMAX Forum
- “WiMAX End-to-End Network Systems Architecture: Stage 2 Draft Specification”, Release 1.0.0 Draft, March 28, 2007, WiMAX Forum
- “WiMAX End-to-End Network Systems Architecture: Stage 3: Detailed Protocols and Procedures”, Release 1.0.0 Draft, March 28, 2007, WiMAX Forum

IEEE Standards

- IEEE 802.16e/D12 September 2005, Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Feb 2006.
- 802.1Q VLAN Standard

IETF References

- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-2131, Dynamic Host Configuration Protocol (DHCP), March 1997
- RFC-2794, Mobile NAI Extension
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-3012, Mobile Ipv4 Challenge/Response Extensions, November 2000
- RFC-3024, Reverse Tunneling for Mobile IP, revised, January 2001
- RFC-3046, DHCP Relay Agent Information Option, January 2001
- RFC-3344, Mobile IP support for Ipv4, August 2002

Supported Standards

- RFC-3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), September 2003
- RFC-3588, Diameter Base Protocol, September 2003
- RFC-3748, Extensible Authentication Protocol, June 2004
- RFC 1918, NWG, Stage 2 Architecture, 121505
- RFC 3115, Mobile IP Vendor/Organization-specific Extensions

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group

Chapter 2

ASN Gateway Service Operation and Configuration

Access Service Network Gateway (ASN Gateway) provides wireless carriers with a flexible solution that supports both Simple IP and Mobile IP applications, independently or simultaneously, within a single scalable platform. Simple IP and Mobile IP applications are described in detail in the System Overview Guide.

To support Simple IP data applications, the system is configured to perform the role of an ASN Gateway within the carrier's WiMAX data network. The ASN Gateway provides IP access to mobile subscribers and routes data to and from the Connectivity Service Network (CSN). The CSN may consist of Wireless Application Protocol (WAP) servers or the Internet.

To support Mobile IP and/or Proxy Mobile IP data applications, the system is configured to perform the role of the ASN Gateway/Foreign Agent (FA) and/or the Home Agent (HA) within the CSN of the carrier's WiMAX data network. When functioning as an HA, the ASN Gateway can be located within the carrier's WiMAX network or in the CSN of an external enterprise or ISP network. In either case, the ASN Gateway/FA terminates the mobile subscriber's call session, and then routes subscriber data to and from the appropriate HA.

The ASN Gateway also serves as the Extensible Authentication Protocol (EAP) authenticator and mobility key holder for subscriber connections and the RADIUS clients to attached AAA servers.

Before you connect to the command line interface (CLI) and begin the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information to consider before you configure the system.

Terminology

This section defines some of the terms used in the chapters that follow.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network.

The ASN Gateway supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context is created, administrative users configure services, logical IP interfaces, subscribers, and so on, for that context. Administrative users then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, so that if a subscriber's domain name matches one of the configured alias names for that context, that context is used.

Context categories are:

- **Source context:** Also referred to as the ingress context, the source context provides the subscriber's point-of-entry in the system. The source context is also the context in which services are configured. For example, in a WiMAX network, the radio network containing the ASN base stations communicates with the system through R6 interfaces configured within the source context as part of the ASN Gateway service.
- **Destination context:** Also referred to as the egress context, the destination context is where a subscriber is provided services such as access to the Internet. Destination contexts are typically named after particular domains. For example, the system's destination context is configured with the interfaces that facilitate subscriber data traffic to and from the Internet, a VPN, or other CSN.
- **AAA context:** The AAA context provides authorization, authentication, and accounting (AAA) functionality for subscriber and administrative user sessions. The AAA context contains context-specific AAA policies, the logical interfaces for communicating with AAA servers, and records for locally configured subscribers and administrative users.



Important: Note that you can configure source, destination, and AAA functionality within the same context or as separate contexts. As a general rule however, if the carrier owns and operates the AAA server, it is recommended that AAA functionality be configured within the source context. Conversely, if a home network other than the carrier's own operates the AAA server, it is recommended that AAA functionality be configured within the destination context. To ensure scalability, do not configure AAA functionality for subscriber sessions in the local context.

- **Local context:** This is the default context on the system that provides out-of-band management functionality. The local context is described in the Command Line Reference.

AAA Realms

An AAA realm is the location within the AAA context where you define subscriber-specific templates that are applied to subscribers who match that realm. An AAA realm is considered part of the AAA context, and the AAA context itself is also considered a realm. You may define many different AAA realms within a single AAA context.

As an example of a realm, within a source context named ingress, there could be a domain alias of domain1.com, another domain alias of domain2.com, and a single AAA configuration used by the entire system. In this example, the source context is also serving as a AAA context. There are three specific AAA realms in this case; ingress, domain1.com, and domain2.com, since all three could have their own defined subscriber templates.

The primary purpose of a AAA realm is to host a subscriber template for each realm that provides AAA attributes that may be used if an authenticated subscriber's access-accept message from RADIUS fails to contain certain attributes. In this case, the default attributes contained in the realm-based subscriber template are used. However, if the RADIUS authentication message contains an attribute from that subscriber's RADIUS user profile, then that information will be used to overwrite any default attribute parameters that are contained in the subscriber template.

More information about subscriber templates will be provided later in this chapter when subscribers are discussed.

Each realm must have a unique name since each realm name can only be used in one context in one system.

Authenticator

The authenticator function is part of the ASN gateway. This function performs the role of an anchored authenticator for a specific subscriber for the duration of the session. For example, as a subscriber moves between base stations served by the ASN gateway, the authenticator anchor remains stationary. If a subscriber moves to a base station served by a new ASN Gateway, the anchor authenticator is hosted at the new ASN Gateway. A full re-authentication of the subscriber is required.

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

EAP Profile

EAP profiles are the group of EAP authentication methods, network and subscriber parameters, and other authentication configurations for a subscriber. The Extensible Authentication Protocol (EAP) is an authentication framework used in wireless networks and point-to-point connections. EAP provides multiple authentication methods that can be tailored to an operator's preference for user-level, device-level, or user and device level network authorization.

Device level authentication is beneficial in a roaming application at the H-AAA server in Home Network Service Provider (H-NSP) to guard against unauthorized network access by users with stolen access devices.

Ports

Ports are the physical interfaces on the ASN Gateway's Ethernet line cards. Ethernet port configuration addresses traffic profiles, data encapsulation methods, media types, and other information for physical connectivity between the system and the rest of the network.

Ports are identified by the chassis slot number in which the line card resides, 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.

You must associate ports with contexts through binding. See the *Bindings* section that follows for more information. You can configure each physical port to support multiple logical IP interfaces each with up to 17 IP addresses, one primary and up to 16 secondary.

Logical Interfaces

You must associate ports with a virtual circuit or tunnel called a logical interface. A logical interface within the system is the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Configure interfaces as part of the VPN context, independent of the physical port that will bridge the virtual interfaces to the network.

Logical interfaces are associated with services through binding. Bind services to an IP address configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to an ASN Gateway service, it functions as an R6 interface between the ASN Gateway service and the ASN base station. Services are defined later in this section.

There are several types of logical interfaces you must configure to support Simple and Mobile IP data applications:

- **Management interface:** This interface provides the system's point of attachment to the management network. The interface supports remote access to the system's CLI, Common Object Request Broker Architecture (CORBA)-based management via the Web Element Manager application, and event notification via the Simple Network Management Protocol (SNMP).

Define management interfaces in the local context and bind them only to the ports on the Switch Processor Input/Output (SPIO) cards.

- **ICC interface:** Inter-context communication (ICC) interfaces are only required when multiple services are configured in the same context. As mentioned previously, services are bound to interfaces. Creating an ICC interface provides a communication path between the services. For example, if you configure an FA and HA service in the same context, you need to bind the FA service to an address assigned to the ICC interface and the HA service to a secondary address on the same ICC interface. This provides a communications path between the two services.

You must configure the ICC interface with multiple addresses (one per service that it is facilitating) and bind them to a physical port.

- **AAA interface:** The AAA interface is the connection between the ASN Gateway and/or HA and the network servers that perform AAA functions. With this release of the system, the Remote Authentication Dial-In User Service (RADIUS) Protocol is used for communication on this interface.

Bind AAA interfaces to ports on the Ethernet line cards. However, you can also bind AAA interfaces to the local context and to ports on the SPIO to provide AAA functions for subscribers, and for context-level administrative users.

- **DHCP:** This is the interface used by the ASN Gateway to communicate with a Dynamic Host Control Protocol (DHCP) Server. You can configure the system to dynamically provide IP addresses for contexts from the DHCP server.

Bind DHCP interfaces to ports on the Ethernet line cards.

- **Reference Point R3:** This is the interface between the ASN and the CSN that supports AAA, policy enforcement, and mobility management capabilities. It also encompasses the bearer plane methods (for example, tunneling) to transfer user data between the ASN and the CSN. R3 supports three types of clients: PMIPv4, CMIPv4, and CMIPv6. CMIPv6 is IPv4 and IPv6 support for Proxy Mobile IP (PMIP) and Client Mobile IP (CMIP).
- **Reference Point R4:** This is the interface between the ASN Gateways and consists of the set of control and bearer plane protocols originating and terminating in various functional entities of an ASN. R4 coordinates mobile station mobility between ASNs and ASN Gateways. R4 is the only interoperable RP between similar or heterogeneous ASNs.
- **Reference Point R6:** This the interface used between the ASN base station and ASN Gateway and consists of the set of control and bearer plane protocols for communication between the base station and the ASN Gateway. The bearer plane consists of an intra-ASN data path between the ASN and ASN gateway. The control plane includes protocols for data path establishment, modification, and release control, in accordance with mobile station mobility events. R6, in combination with R4, may serve as a conduit for the exchange of MAC state information between base stations that cannot inter-operate over R8.
- **Reference Point R7:** R7 consists of the optional set of control plane protocols (for example, AAA and Policy coordination) in the ASN Gateway, and other protocols, that co-ordinate the two groups of functions identified in R6.

Bindings

A binding is an association between elements within the system. There are two types of bindings: static and dynamic.

Use static binding to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (that is, support the protocols) required by the service. For example, an ASN Gateway service bound to a logical interface causes the logical interface to take on the characteristics of an RP (R6) interface within a WiMAX network.

Use dynamic binding to associate a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Services

Services are configured within a context and enable certain functionality. The system supports multiple Mobile IP configurations. A single system can perform the function of an ASN Gateway only, FA only, an HA only, or a combined ASN Gateway/FA/HA.

The following services can be configured on the system:

- **ASN Gateway services:** Required for both Simple IP and Mobile IP applications, ASN Gateway services define ASN Gateway functionality for the system. You must bind the ASN Gateway service to a logical interface within the same context. Once bound, the interface takes on the characteristics of an R6 interface. You can bind multiple services to the same logical interface. Therefore, a single physical port can facilitate multiple R6 interfaces.

The system treats the connection between the ASN base station and the ASN Gateway service as a subscriber session. Individual R6 sessions are identified on this connection by the flow IDs, ASN base station address, the ASN Gateway interface address, and the subscriber session ID.

- **ASN FA services:** Configure ASN FA services to support Mobile IP and define FA functionality on the system.

Configure the ASN FA service in a different context from the ASN Gateway service. However, if the FA service will be communicating with an ASN HA that is a separate network element, configure it within the same context as, and bind it to, the R3 interfaces that allow it to communicate with the ASN HA. Depending on your configuration, the FA service can create and maintain the R3 interface between the ASN Gateway/FA and the ASN HA or it can communicate with an HA service configured within the same context.

- **ASN Gateway HA services:** ASN HA services are configured to support Mobile IP and define HA functionality on the system. Depending on your configuration, the HA service can terminate the R3 interface from the FA or it can communicate with an FA service configured in the same context.

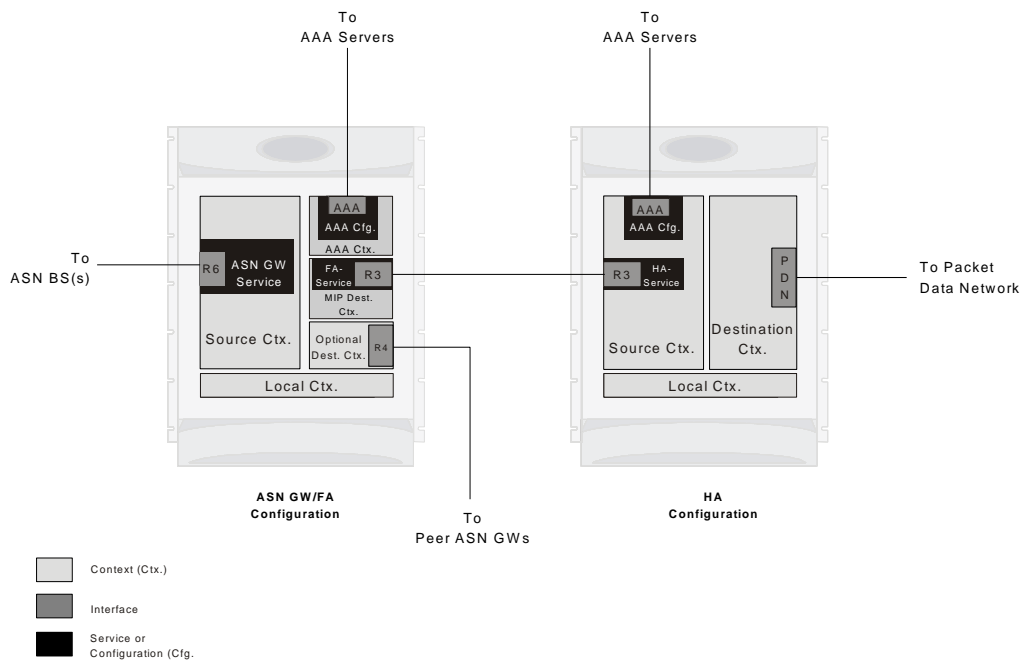
If you configure the HA service within the same system as the ASN Gateway/FA, it should also be configured within the same context as the FA service. This context facilitates the ASN interfaces to the data network.

If you configure the HA service in a separate system, it should be configured in the same context as and bound to the R3 interfaces that allow it to communicate with the ASN FA.

- **LAC services:** LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within WiMAX networks to provide secure tunneling to an L2TP network server (LNS) on a remote CSN.
- **DHCP services:** DHCP services are configured on a system to provide dynamic assignment of IP address to ASN contexts through the use of the Dynamic Host Configuration Protocol (DHCP).

The following figure shows the relationship between services, interfaces, and contexts within the system for WiMAX networks.

Figure 31. Services, Interfaces, and Context Relationship Within the System for WiMAX Networks



AAA Servers

For most configurations, AAA servers store profiles, perform authentication, and maintain accounting records for each mobile data subscriber. The AAA servers communicate with the system over the AAA interface. The system supports the configuration of up to 128 AAA servers.

It is important to note that for Mobile IP, there can be foreign AAA (FAAA) and home AAA (HAAA) servers. The FAAA server(s) typically resides in the carrier's network. The HAAA server(s) could be owned and controlled by either the carrier or the home network. If the HAAA server is owned and controlled by the home network, accounting data can be transferred to the carrier via a AAA proxy server.

Subscribers

Subscribers are the end-users of the service who gain access to the Internet, their home network, or a public network through the system. There are three primary types of subscribers/users:

- **RADIUS-based Subscribers:** The most common type of subscriber, these users are identified by their International Mobile Subscriber Identity (IMSI) number, an Electronic Serial Number (ESN), or by their domain name or user name. They are configured on and authenticated by a RADIUS AAA server.

Upon successful authentication, various attributes contained in the subscriber profile, are returned that dictate such things as session parameter settings (for example, protocol settings and IP address assignment method), and privileges, such as Simple IP or Mobile IP.



Important: Attribute settings received by the system from a RADIUS AAA server take precedence over local-subscriber attributes and parameters configured on the system.

- **Local Subscribers:** These are subscribers, primarily used for testing purposes, that are configured and authenticated within a specific context. Unlike RADIUS-based subscribers, the local subscriber's user profile (containing attributes similar to those used by RADIUS-based subscribers) is configured within the context where they are created.

When local subscriber profiles are first created, attributes for that subscriber are set to the system's default settings. The same default settings are applied to all subscriber profiles, including the subscriber named default (created automatically by the system for each system context. Refer to the *Default Subscribers and Realm-based Subscriber Templates* section for more information. When configuring local profile attributes, the changes are made on a subscriber-by-subscriber basis.



Important: Attributes configured for local subscribers take precedence over context-level parameters. However, they could be over-ridden by attributes returned from a RADIUS AAA server.

- **Management Subscribers:** A management user is an authorized user who can monitor, control, and configure the system through its command line interface (CLI) or Web Element Manager application. This management can be performed either locally, through the system's console port, or remotely through the use of the Telnet or secure shell (SSH) protocols. Management users are typically configured as a local subscriber within the local context, which is used exclusively for system management and administration. Configure the management subscriber's user profile within the context where they are created (in this case the local context). Management subscribers may also be authenticated remotely via RADIUS, if a AAA configuration exists within the local context.

Default Subscribers and Realm-based Subscriber Templates

Used for RADIUS-based subscribers, default subscribers are created on a per context basis and subscriber templates, optionally created on a per realm basis, contain default AAA attributes that can be used by subscribers who are remotely authenticated within a specific context or domain alias (AAA realm) when needed.

For RADIUS-based subscribers, default subscribers are created on a per context basis. Subscriber templates are optionally created on a per realm basis. Both contain default AAA attributes that can be used by subscribers who are remotely authenticated within a specific context or domain alias (AAA realm) when needed.

Default Subscriber

When each context is created, the system automatically creates a subscriber named default. There is only one default subscriber per context. The profile for the subscriber named default provides a configuration template of attribute values

for subscribers who are remotely authenticated in that context. Any subscriber information that is not included in a RADIUS-based subscriber's user profile is configured according to the defaults defined for the default subscriber.

No matter where created all default subscribers initially have the same attributes set. The attributes for the default subscriber in each context can be changed from the CLI on a context by context basis.



Important: Local subscribers, who are authenticated locally within the context where they were created, cannot use any attributes that are defined for subscriber default. Rather, each local subscriber must have any attributes configured for them individually.

Realm-based Subscriber Templates

A context can have numerous domain aliases that allow a single context to serve numerous subscribers who have different domain names. When assigned, these domain aliases become AAA realms within the context.

Since each realm is used for a specific group of subscribers (for example, corporate subscribers who have access to a specific corporate network protected by a virtual private network), each realm must define which AAA attributes to apply to these different subscriber groups. This is done through realm-based subscriber templates.

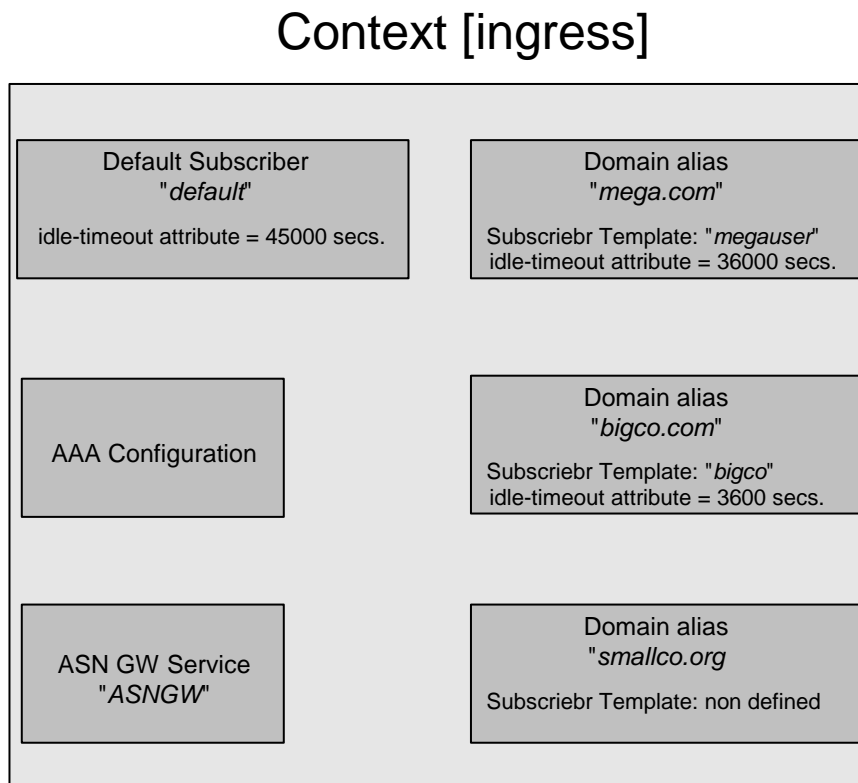
A subscriber template contains defined attributes that are specific to a select subscriber who belongs to that realm. As in the case of the default subscriber (subscriber named default) who has a context-level set of configuration attributes, the subscriber template provides default attribute values that may be used should a RADIUS user profile for a subscriber belonging to the specific realm fail to contain a needed attribute.



Important: If a realm-based subscriber template is not created for a specified realm, then the system will use the attributes configured for default subscriber (named default) within the context where the AAA realm exists.

Below is an example of how realm-based subscriber templates may be used.

Figure 32. Realm-based subscriber template example



As depicted in the figure above, a context named “ingress” contains:

- an ASN Gateway service named ASN Gateway.
- an AAA configuration to communicate with an external RADIUS server.
- a default subscriber for the context named default. This default subscriber has an idle timeout attribute value of 45000 seconds.
- three additional realms, based on the following domain alias names:
 - mega.com, which has a realm-based subscriber template named megauser. This template contains an idle timeout attribute value of 36000 seconds.
 - bigco.com, which has a realm-based subscriber template named bigco. This template contains an idle timeout attribute value of 3600 seconds.
 - smallco.com, which has no realm-based subscriber template defined.

For this example, we will assume that all subscribers enter the system through the ASN Gateway service defined in the [ingress] context. Configuration procedures and context selection methods are provided in other sections in this document.

If a subscriber enters the system with a domain name that matches the context name ingress (example: user1@ingress), then the [ingress] context is used for authentication. If the RADIUS server authenticates the subscriber and returns no value for the idle-timeout attribute, this subscriber is assigned the value contained in the subscriber default configuration.

If a subscriber named user@mega.com enters the system with a domain name that matches a configured domain alias within the [ingress] context, in this case mega.com, the [ingress] context is used for authentication. However, since a

realm-based subscriber template named `megauser` is defined within this AAA realm, should the RADIUS server return no value for the `idle-timeout` attribute, this subscriber is assigned the value contained in the `megauser` subscriber template.

If a subscriber named `user@bigco.com` enters the system with a domain name that matches a configured domain alias within the `[ingress]` context, in this case `bigco.co`, the `[ingress]` context is used for authentication. However, since a realm-based subscriber template name `bigco` is defined within this AAA realm, any attributes not returned could be assigned from this subscriber template. In this example, the RADIUS server returns an `idle-timeout` of 18000 seconds. Because the RADIUS user profile contained a value for this attribute, the system uses that value (18000) rather than the value defined in the subscriber template.

If a subscriber name `user@smallco.org` enters the system with a domain name that matches a configured domain alias within the `[ingress]` context, in this case `smallco.org`, the `[ingress]` context would be used for authentication. Note that the `smallco.org` domain alias does not have a realm-based subscriber template defined. In this case, the system obtains any attribute values not returned from the RADIUS server from the subscriber default configuration. So if no attribute value was returned from RADIUS, `user@smallco.org` is assigned an `idle-timeout` value of 45000 seconds.

How the System Selects Contexts

The previous section of this chapter defined what a context is and how it is used within the system. This section describes the process that determines which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of the number of contexts and interfaces you need to configure.

Context Selection for Context-level Administrative User Sessions

The system comes configured with a context called local that should be used specifically for management purposes. The context selection process for context-level administrative users (those configured within a context) is simplified because the management interface(s) on the SPIO are only associated with the local context. Therefore, the source and destination contexts for a context-level administrative user responsible for managing the entire system should always be the local context.

Although this is not commonly done, a context-level administrative user can also connect through other interfaces on the system and still have full system management privileges.

For more detailed information on the context selection for context-level administrative user session, refer System Administration Guide.

Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is dependant on the mapping of ASN base stations to ASN Gateways. Depending on this mapping and a subscriber's location in the network, the same subscriber may initiate several different data sessions throughout the day and have their session serviced by several different source contexts.

The AAA and destination context selection is determined by the services provided to the subscriber. For example, a carrier may only offer wireless Internet access and therefore be responsible for performing AAA functions for a subscriber session and for providing the network interfaces to the Internet. In this example, the carrier may choose to combine the source and AAA contexts into one and provide a separate destination context. Another carrier may choose to provide both wireless Internet access and VPN service to a corporate or Internet Service Provider (ISP) network. The system is flexible enough to simultaneously support these services because of the unique way it determines how to provide AAA functionality and route the session to the appropriate destination.

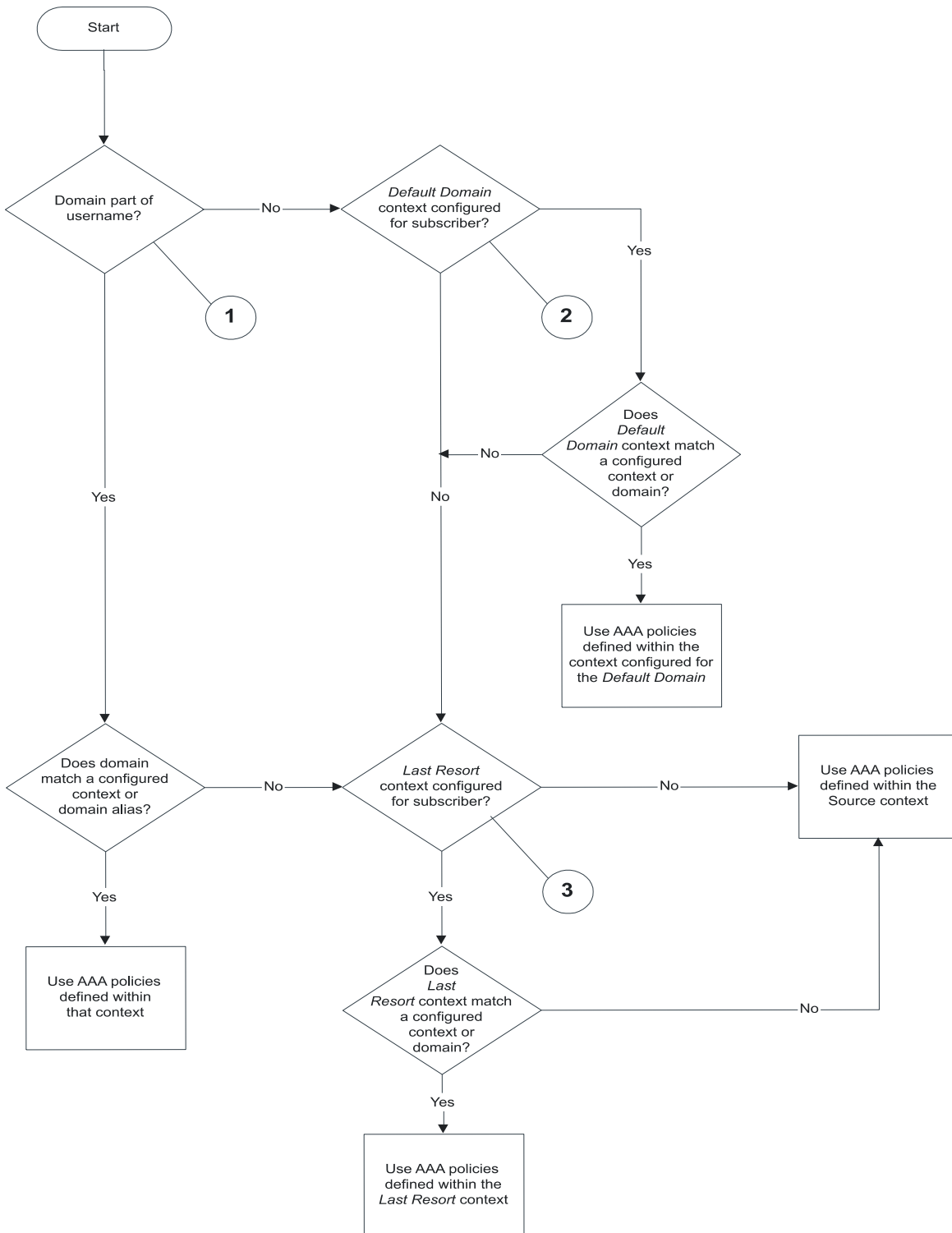
The following two sections provide details on how the system determines the correct AAA and destination contexts for a subscriber session.

AAA Context Selection for Subscriber Sessions

The following figure and table describe the process that the system uses to select an AAA context for a subscriber.

Table 19. Subscriber AAA Context Selection

Item	Description
1	<p>During authentication, the system determines if a domain was received as part of the username.</p> <p>If there is a domain and it matches the name of a configured context or domain alias, the AAA configuration within that context is used.</p>
2	<p>If there was no domain specified in the username, the system determines if an AAA Subscriber Default Domain was configured. The AAA Subscriber Default Domain parameter is a system-wide AAA parameter that provides the system with the name of a context or domain that can provide AAA functions.</p> <p>If the AAA Subscriber Default Domain is configured and it matches a configured context or domain, the AAA configuration within the AAA Subscriber Default Domain context is used.</p> <p>If the AAA Subscriber Default Domain is not configured or does not match a configured context or domain, the system determines if an AAA Subscriber Last Resort is configured.</p>
3	<p>If a domain is specified as part of the username but it does not match a configured context domain, the system determines if an AAA Subscriber Last Resort is configured. The AAA Subscriber Last Resort parameter is a system-wide AAA parameter that provides the system with the name of a context or domain that can provide AAA functions in the event that all other options fail.</p> <p>If the AAA Subscriber Last Resort is configured and it matches a configured context or domain, then the AAA configuration within the AAA Subscriber Last Resort context is used.</p> <p>If the AAA Subscriber Last Resort is not configured or does not match a configured context or domain, then the AAA configuration within the source context is used.</p>

Figure 33. Subscriber AAA Context Selection

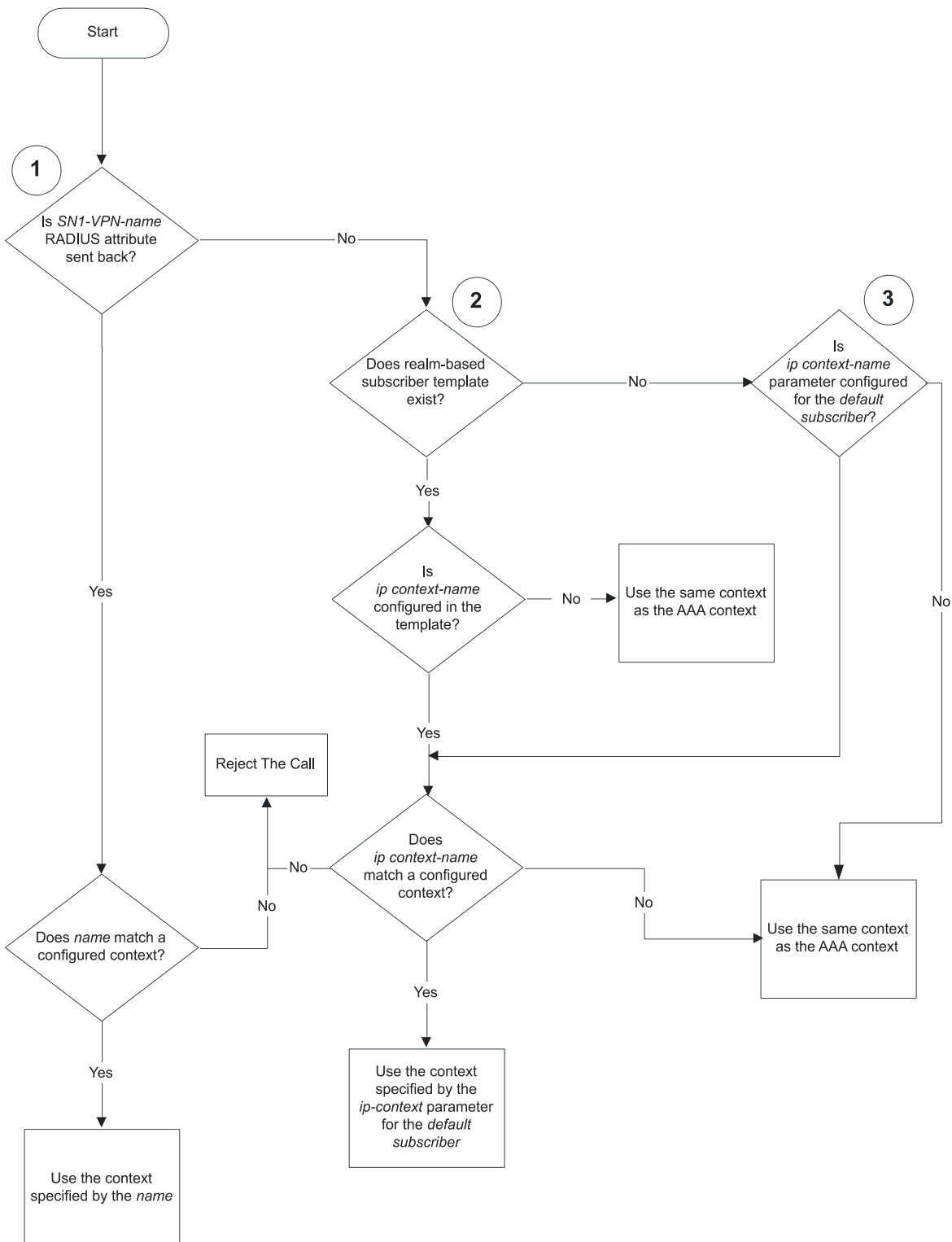
Destination Context Selection for Subscriber Sessions

This section provides information on how a destination context is selected for subscribers whose profiles are configured on a RADIUS AAA server, and those whose profiles are locally configured. Note that the destination context for context-level administrative users is always the local context.

The following table and figure describe the process that the system uses to select a destination context for a RADIUS-based subscriber whose profile is configured on a RADIUS AAA server and for a subscriber whose profile is configured within a specific context.

Table 20. Subscriber Destination Context Selection

Item	Description
1	<p>The system supports a RADIUS attribute called SN1-VPN-name (or SN-VPN-name in some dictionaries). This attribute specifies the name of the subscriber's destination context. If configured in the subscriber's RADIUS user profile, it is returned as part of the Access Accept message.</p> <p>If the SN1-VPN-Name attribute is returned, and it matches a configured context, then that context is used as the destination context.</p> <p>If the SN1-VPN-Name attribute is returned, and it does not match a configured context, the call is rejected.</p> <p>If the SN1-VPN-Name attribute is not returned with a value, go to item 2 in this table.</p>
2	<p>The system attempts to use the ip context name parameter configuration for the realm-based subscriber template or context-level default subscriber configured within the AAA context.</p> <p>If a realm-based subscriber template does not exist, go to item 3 in this table.</p> <p>If a realm-based subscriber template exists, the system checks to see if ip context-name is configured in the template.</p> <p>If ip context-name is not configured in the template, the AAA context is used for the destination context.</p> <p>If ip context-name is configured in the template, a check is made to see if it matches the name of a configured context.</p> <p>If ip context-name is configured in the template, but does not match the name of a configured context, the call is rejected.</p> <p>If ip context-name is configured in the template, and matches the name of a configured context, the destination context is set to the ip name-context f or the default subscriber.</p>
3	<p>The local default subscriber profile contains an attribute called ip context-name. This attribute specifies the destination context to use for a local subscriber.</p> <p>If ip context-name is not configured, the AAA context is used for the destination context.</p> <p>If ip context-name is configured, a check is made to see if it matches the name of a configured context.</p> <p>If ip context-name is configured, but does not match the name of a configured context, the AAA context is used for the destination context.</p> <p>If ip context-name is configured, and matches the name of a configured context, the destination context is set to the ip name-context for the default subscriber.</p>

Figure 34. Subscriber Destination Context Selection

Chapter 3

ASN Gateway Simple IP Configuration Examples

This chapter provides configuration examples you can implement on the system to support Simple IP data services.

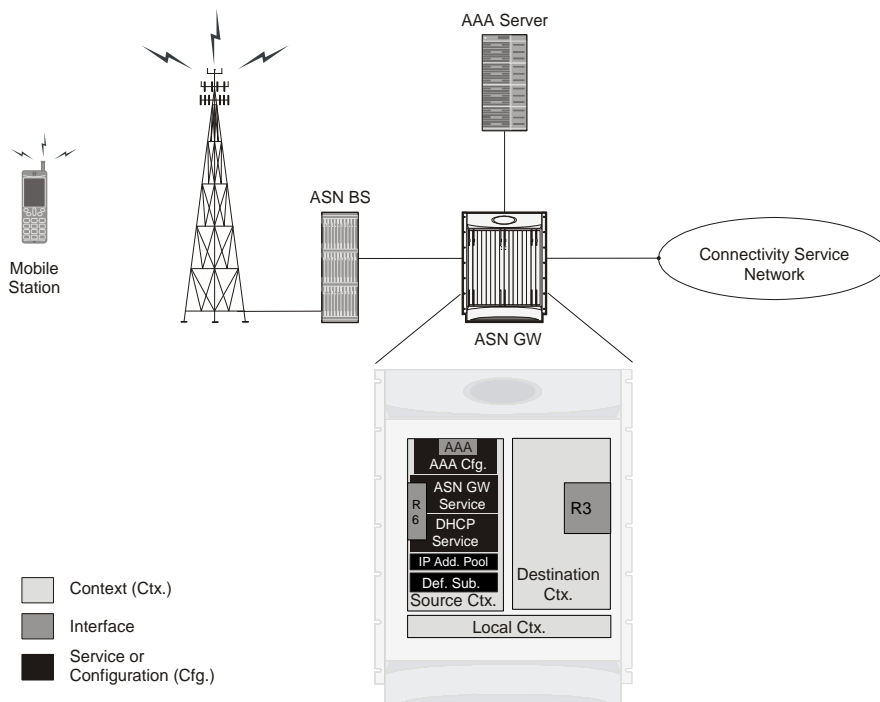


Important: This chapter does not discuss the configuration of the local context. Refer to the System Administration Guide.

Simple IP Support with Single Source and Destination Context

The most simple configuration to support Simple IP data applications requires that you configure two contexts (one source and one destination) on the system, as shown in the example in the figure below.

Figure 35. Simple IP Support Using a Single Source and Destination Context



The source context facilitates the ASN Gateway service(s) and the R6 and AAA interfaces. The source context is also configured to provide AAA functionality for subscriber sessions. The destination context facilitates the packet data network interface(s).

In this configuration, the wireless carrier provides the function of an Internet Service Provider (ISP) to its subscribers. The ASN Gateway service in the source context terminates WiMAX subscriber sessions and routes its data traffic through the destination context to and from a packet data network, such as the Internet.

Information Required

Before you configure the system as shown in this example, gather the following source and destination context information.

Source Context Configuration

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

Table 21. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the source context is recognized by the system.
R6 Interface Configuration	
R6 interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Give each interface a unique name. Configure R6 interfaces in the source context.
IP address and subnet	Assigned to the R6 interface. A separate address and/or subnet is required for each configured interface.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the line card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system. Define a description for each port you use. Configure physical ports within the source context to bind logical R6 interfaces.
Gateway IP address	Use to configure static routes from the R6 interface(s) to a specific network.
ASN Gateway service Configuration	
ASN Gateway service name	An identification string between 1 and 63 characters (alpha and/or numeric) by which the ASN Gateway service is recognized by the system. Give each ASN Gateway a unique name. Configure ASN Gateway services in the source context.
UDP port number for R6 traffic	Specifies the port used by the ASN Gateway service and the ASN BS for communications. The UDP port number is any integer between 1 and 65535. The default is 2231.
Authentication method	Specifies how the system handles authentication: using EAP protocol (such as single EAP), or not requiring any authentication.
Service Policy Information	Policy to handle unexpected re-entry of MS: Specifies the policy to handle unexpected re-entry of an MS in ASN. Options are allow or disallow.
	Policy to handle mismatch in MSID and DHCP client hardware address: Specifies the policy to handle mismatch in Mobile Subscriber Identifier (MSID) and DHCP client hardware address (CHADDR). Options are allow or disallow.

Required Information	Description
	Policy to create non-anchor mode session: Specifies the policy to create a non-anchor ASN Gateway session based on the data path registration request. Options are allow or disallow.
Setup timeout	Specifies the setup timeout duration in seconds for R6 control packets. Configure the time in seconds to any integer between 1 and 100000, or disable the timer to set an infinite lifetime. The default value is 60 seconds.
AAA Interface Configuration	
AAA interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Give each interface a unique name. AAA interfaces are configured in the source context.
IP address and subnet	Assigned to the AAA interface. Configure separate addresses and/or subnets for each interface.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the line card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system. Define a description for each port used. Configure physical ports within the source context 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 communicates with to provide subscriber authentication functions. Use a separate address for each configured RADIUS server. Configure RADIUS authentication servers within the source context. Assign a priority to each server.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key exchanged between the RADIUS authentication server and the source context. Define a shared secret for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number is any integer 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 communicates with to provide subscriber accounting functions. Use a separate address for each configured RADIUS server. Configure RADIUS accounting servers within the source context. Assign each server a priority.

Required Information	Description
	<p>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. Define a shared secret for each configured RADIUS server.</p> <p>UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number is an integer between 1 and 65535. The default value is 1813.</p>
RADIUS attribute NAS Identifier	Specifies the name by which the source context is identified in the Access-Request message(s) it sends to the RADIUS server. Define a name between 1 and 32 alpha and/or numeric characters. The name is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. Optionally, configure a secondary IP address interface.
ASN packet data flow identifier	Specifies the unique packet data flow identifier for a WiMAX subscriber session. The ASN packet data flow identifier is an integer from 1 through 65535.
ASN service data flow identifier	Specifies the unique service data flow identifier for a WiMAX subscriber session. The ASN service data flow identifier is an integer from 1 through 65535.
ASN service profile identifier	Associates the unique ASN service profile identifier for a WiMAX subscriber session. The ASN service profile identifier is an integer from 1 through 65535. Configure the identifier in the destination context with the ASN service profile configuration.

Destination Context Configuration

The following table lists the information required to configure the destination context. This information is required for each domain.

Table 22. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context is recognized by the system.</p> <p>NOTE: For this configuration, the destination context name should not match the domain name of a specific domain.</p>
CSN Interface Configuration	
CSN interface name (R3)	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.</p> <p>Define a separate name for each configured interface.</p> <p>Configure CSN interfaces in the destination context.</p>
IP address and subnet	<p>Assigned to the CSN (R3) interface.</p> <p>Define a separate address and/or subnets for each configured interface.</p>

Required Information	Description
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the line card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system. Define a separate description for each port used. Configure physical ports within the destination context to bind logical CSN interfaces.
Gateway IP address(es)	Used when configuring static routes from the CSN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name(s)	If IP address pools are configured in the destination context(s), names or identifiers are needed for them. The pool name is 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 consists 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.
Traffic Class Map Configuration (optional)	
Class-map name(s)	If traffic class map is configured in the destination context(s), names or identifiers are needed for them. The class-map name is between 1 and 31 alpha and/or numeric characters and is case sensitive.
Traffic matching criteria	A matching criteria is configured for traffic flow on the basis of different parameters or without classification. Configurable parameters are 5-tuple (source address, source port, destination address, destination port, protocol), packet size, IP ToS value, and IPSec SPI.
ASN Service Profile Identifier Configuration (optional)	
ASN service profile identifier(s)	If an ASN service profile identifier is configured in the destination context(s), an identifier is needed for them. The ASN service profile identifier is an integer from 1 through 65535. Configure the ASN service profile for uplink or downlink or for both direction of traffic.
QoS descriptor identifier(s)	An identifier for the QoS descriptor is configured in the ASN service profile. The ASN service profile identifier is an integer from 1 through 255. Configure the ASN service profile for uplink and downlink direction of traffic.
Traffic classifier(s)	A class map identifier for uplink/downlink traffic is associated with this ASN service profile. Configure the class map identifier in the traffic class map configuration. Configure the classifier for uplink and downlink direction of traffic.
ASN QoS Descriptor Identifier Configuration (optional)	
ASN QoS descriptor identifier(s)	If ASN QoS descriptor identifier is configured in the destination context(s), an identifier is required for them. The QoS descriptor identifier is an integer from 1 through 65535.

Required Information	Description
Service class name	<p>If a service class name is associated in the ASN QoS descriptor configuration, an identifier is required for them.</p> <p>The service class name is a string of 2 through 128 ASCII characters.</p> <p>A service class name is a group of QoS parameters defined at the BS. It is referenced by a service flow to apply certain QoS parameters.</p>
Global service class name	<p>If a global service class name is associated in the ASN QoS descriptor configuration, an identifier is required for them.</p> <p>The service class name is a string of 1 through 6 ASCII characters.</p> <p>A global service class name is similar in function to the service class name except that 1) global service class name use may not be modified by a BS, 2) global service class name remains consistent among all BS, and 3) global service class name is a rules-based naming system and contains referential QoS parameter codes.</p>
AAA Interface Configuration	
AAA interface name	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system.</p> <p>Configure a separate name for each interface.</p> <p>Configure AAA interfaces in the source context.</p>
IP address and subnet	<p>Assigned to the AAA interface.</p> <p>Configure a separate address for each interface.</p>
Physical port number	<p>Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the line card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>
Physical port description	<p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system.</p> <p>Define a separate description for each port.</p> <p>Physical ports are configured within the source context and are used to bind logical AAA interfaces.</p>
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	<p>IP Address:</p> <p>Specifies the IP address of the RADIUS authentication server the source context communicates with to provide subscriber authentication functions.</p> <p>Define an address for each RADIUS server.</p> <p>Configure RADIUS authentication servers within the source context. Assign each server a priority.</p>
	<p>Shared Secret:</p> <p>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.</p> <p>Define a shared secret for each configured RADIUS server.</p>
	<p>UDP Port Number:</p> <p>Specifies the port used by the source context and the RADIUS authentication server for communications.</p> <p>The UDP port number is an integer between 1 and 65535. The default value is 1812.</p>

Required Information	Description
RADIUS Accounting server	IP Address: Specifies the IP address of the RADIUS accounting server that the source context communicates with to provide subscriber accounting functions. Define an address for each configured RADIUS server. 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. Define a shared secret for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number is an integer 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 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.

System-Level AAA Configuration

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

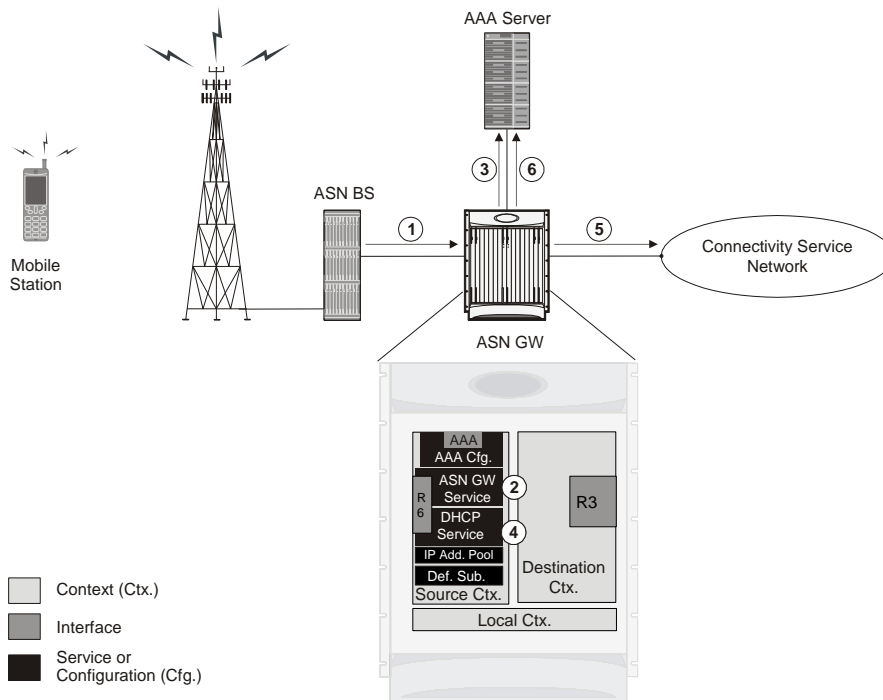
Table 23. Required Information for System-Level AAA Configuration

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 is 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 provides AAA functions in the event that the domain-part of the username is present but does not match the name of a configured destination context. This parameter is applied to all subscribers if their specified domain does not match a configured destination context, regardless of what domain they are accessing. NOTE: The last-resort context name can be the same as the source context.

Required Information	Description
Subscriber username format	<p>Specifies the format of subscriber usernames as to whether the username or domain is specified first and which character separates them. The separator characters are:</p> <ul style="list-style-type: none"> • @ • % • - • \ • # • / <p>Specify up to six username formats. The default is username @.</p> <p>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.</p>

How This Configuration Works

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

Figure 36. Call Processing Using a Single Source and Destination Context

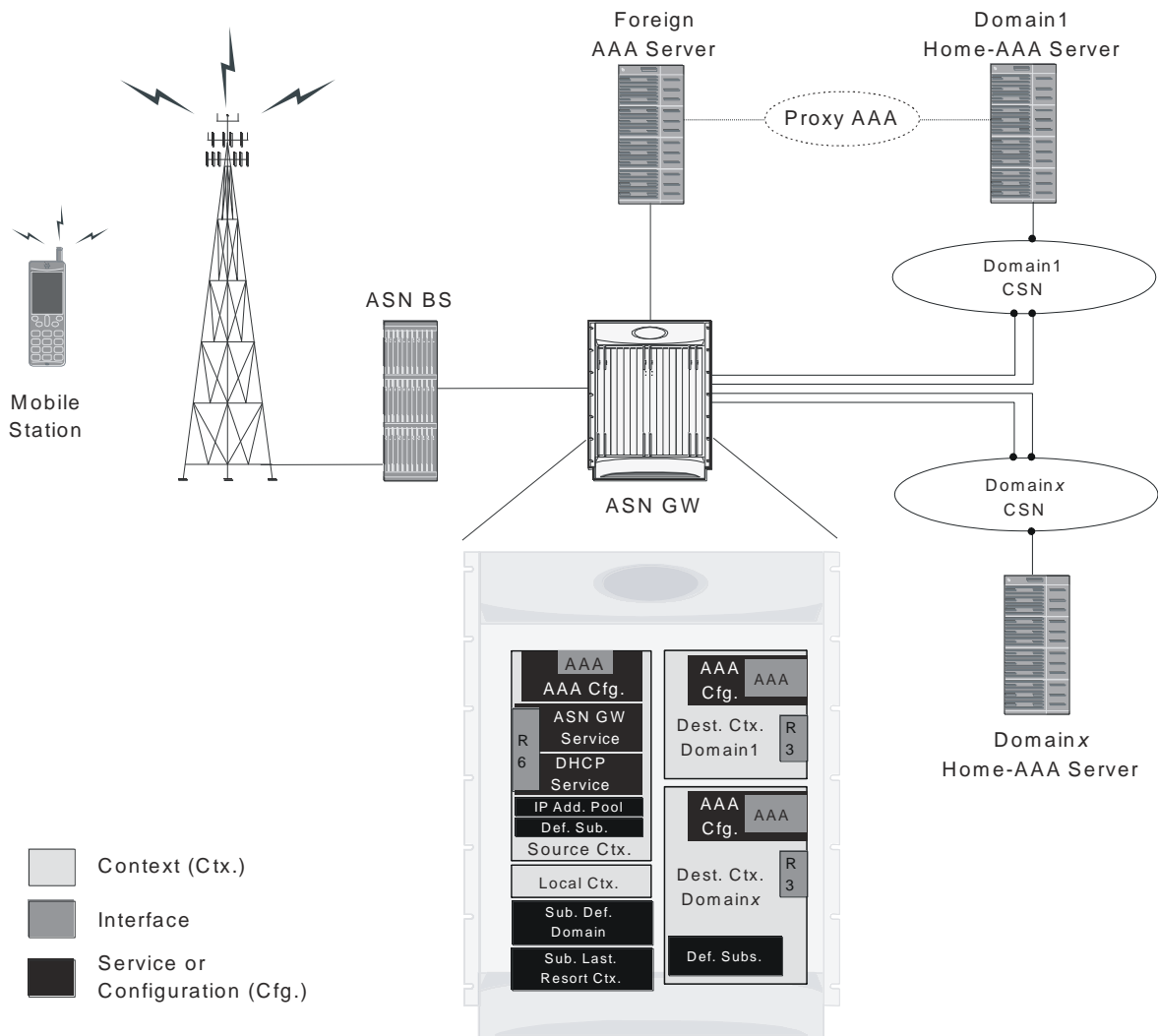
- Step 1** A subscriber session from the ASN base station is received by the ASN Gateway service over the R6 interface. The ASN Gateway service determines which context to use in providing AAA functionality for the session. This process is described in the How the System Selects Contexts section of the ASN Gateway Service Operation and Configuration chapter of this reference.
- For this example, the result of this process is that ASN Gateway service determined that AAA functionality should be provided by the Source context.
- Step 2** The system communicates with the AAA server specified in the source context's AAA configuration to authenticate the subscriber.
- Step 3** Upon successful authentication, the system determines which egress context to use for the subscriber session. This process is described in the How the System Selects Contexts section of ASN Gateway Service Operation and Configuration chapter of this reference.
- The system determines that the egress context is the destination context based on the configuration of either the Default subscriber's ip-context name or from the SN-VPN-NAME or SN1-VPN-NAME attributes that is configured in the subscriber's RADIUS profile.
- Step 4** Data traffic for the subscriber session is routed through the PDN interface in the Destination context.
- Step 5** Accounting information for the session is sent to the AAA server over the AAA interface.

Single Source and Multiple Outsourced Destination Contexts

The system allows a wireless carrier to generate additional revenue by providing separate context configurations that can then be leased or outsourced to various enterprises or ISPs, each with a specific domain.

In order to support multiple outsourced domains, configure the with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers can be owned or maintained by either the carrier or the domain. If they are owned by the domain, the carrier receives the AAA information via proxy.

Figure 37. Simple IP Support Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context facilitates the ASN Gateway service(s), and the R6 interface(s). Configure the source context with AAA interface(s) to provide AAA functionality for subscriber sessions. Each destination context is configured to

In addition to the source and destination contexts, there are system-level AAA parameters to configure.

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

subscriber1@Domain1

subscriber2

subscriber3@Domain37

ASN BS

ASN GW

Foreign AAA Server

Proxy AAA

Domain1 Home AAA Server

Domain1 CSN

Domainx CSN

Domainx Home AAA Server

1

2

AAA Cfg. AAA Cfg. AAA

ASN GW Service Est. Ctx. Domain1 R 3

DHCP Service

IP Add. Pool Def. Sub. Source Ctx. AAA Cfg. AAA

Local Ctx. Dest. Ctx. Domainx R 3

Sub. Def. Domain

Sub. Last. Resort Ctx. Def. Subs.

4a-c

5a-c

7a-c

Context (Ctx.)

Interface

Service or Configuration (Cfg.)

- Default subscriber domain name = Domainxx
- Subscriber username format = username @
- No subscriber last-resort context name was configured.

Cisco ASR 5000 Series Access Service Network Gateway Administration Guide

- Within the Source context, the IP context name is configured as Domainx.
- Within the Domainx context, the IP context name is configured as Domainx.

Step 3 Sessions are received by the ASN Gateway service from the ASN BS over the R6 interface for subscriber1@Domain1, subscriber2, and subscriber3@Domain37.

Step 4 The ASN Gateway service attempts to determine the domain names for each session.

Step a For subscriber1, the ASN Gateway service determines that a domain name is present and is Domain1.

Step b For subscriber2, the ASN Gateway service determines that no domain name is present.

Step c For subscriber3, the ASN Gateway service determines that a domain name is present and is Domain37.

Step 5 The ASN Gateway 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 of ASN Gateway Service Operation and Configuration chapter of this reference.

Step a For subscriber1, the ASN Gateway service determines that a context is configured with a name that matches the domain name specified in the username string (Domain1). Therefore, Domain1 is used.

Step b For subscriber2, the ASN Gateway service determines that Domainx is configured as the subscriber default domain name. Therefore, Domainx is used.

Step c For subscriber3, the ASN Gateway service determines that no context was configured that matched the domain name specified in the username string (Domain37). Because no subscriber last-resort context name is configured, the source context is used.

Step 6 The system then communicates with the AAA servers specified in each of the selected context's AAA configuration to authenticate the subscriber.

Step 7 Upon successful authentication of all three subscribers, the ASN Gateway service determines which destination context to use for each of the subscriber sessions. This process is described in the How the System Selects Contexts section of ASN Gateway Service Operation and Configuration chapter of this reference.

Step a For subscriber1, the ASN Gateway service receives the SN-VPN-NAME or SN1-VPN-NAME attribute equal to Domain1 as part of the authentication accept message from the AAA server on Domain1's network. Therefore, Domain1 is used as the destination context.

Step b For subscriber2, the ASN Gateway service determined that the SN-VPN-NAME or SN1-VPN-NAME attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured for the Default subscriber within the Domainx context. Because this parameter is configured to Domainx, the Domainx context is used as the destination context.

Step c For subscriber3, the ASN Gateway service determines that the SN-VPN-NAME or SN1-VPN-NAME attribute was not returned with the Authentication Accept response, and determined the Default subscriber IP context name configured within the Source context. Because this parameter is configured to Domainx, the Domainx context is used as the destination context.

Step 8 Data traffic for the subscriber session is routed through the CSN interface in each subscriber's destination context.

Step 9 Accounting messages for the session are sent to the AAA servers over the AAA interfaces.

■ Single Source and Multiple Outsourced Destination Contexts

Chapter 4

ASN Keep Alive BS Monitoring

The keep alive mechanism is based on two-way transactions consisting of keep alive request and keep alive response message exchanges. The keep alive mechanism is used over R6/ R4 reference points so that each side can detect a failure and restart its peer. The ASN GW that detects a failure and restarts its peer may take appropriate actions, such as cleaning up the corresponding mobile station contexts. The trigger for sending keep alive request messages is based on the configuration in the ASN GW service.

Keep alive request and keep alive response messages have a mandatory TLV (Time-Length-Value) of LRT (Last Reset Time). Based on this TLV value, the ASN GW or base station knows whether the peer node has been restarted during the time interval from the last keep alive interrogation.

Keep Alive Request and Response Overview

The mechanism for detecting a base station restart is as following:

- In the initial keep alive interrogation with its peer, the ASN GW stores the LRT value of its peer nodes. The ASN GW that supports the keep alive functionality, generates the LRT and caches it internally. The ASN GW sends the LRT value in the keep alive Request or Response message. This value is interpreted by the keep alive receiver to detect the peer's restart.
- In subsequent keep alive interrogations, the ASN GW compares the received LRT value with the stored value. If the received LRT value does not match the stored value for the peer node, the ASN GW considers that the peer node has passed restart during the time interval from the last keep alive interrogation. The ASN GW takes an appropriate action. The action may be implementation-specific, such as purging the corresponding MS contexts, or triggering MS Network Exit for the affected MSs.
- If the restart preserves the MS contexts that were stored before the reboot, the ASN GW does not change its LRT value after the reboot. Otherwise, the ASN GW does change its LRT value to inform the peer node of its reboot. The ASNGW that detects the peer node restart stores the new LRT value for this peer node.

The ASN GW monitors the base stations that are directly connected to it. The ASN GW does not monitor the base station that is connected to the non-anchor.

If a keep alive request or response is received from the legacy base station, it is dropped.

Keep Alive Request Sender

If you enable the keep alive-based base station monitoring feature for a particular ASN GW service, that ASNGW service starts monitoring the list of base stations from which it has received any R4/R6 traffic from previous sessions, including non-active sessions.

The monitoring occurs in the following stages:

- Step 1** When a base station entry is created through call setup (the initial network entry), or a successful data path is created during a handoff, the ASN GW starts sending keep alive Request messages and waits for keep alive responses. The keep alive request messages are addressed to the base station's R6 address endpoint. The source address of the keep alive Request messages are the ASN GW service's IP address. The base station receives keep alive requests from the ASN GW only when there are sessions established with that base station. The ASN GW stops monitoring base station when there are no active sessions as a result of a handoff to another base station or session termination from this base station. No peer base station configuration is needed for the base station list.
- Step 2** If the ASN GW does not receive a keep alive response messages after timeout (T), the ASN GW retransmits the keep alive request message as many times as is configured (num-retry (N)) times. If the ASN GW receives no response after N retries, the base station is considered out of service.
- Step 3** When the maximum number of retransmissions specified in num-retry (N), for a given base station have been exhausted, the ASN GW Manager sends a clear subscriber message to all the session manager tasks in the system. The session managers delete the sessions that correspond to the non-responsive base station and generate Accounting Stop records for The de-registration, network exit, and Accounting-Stop messages are sent in a paced manner.

- Step 4** Only the ASNGW that is directly connected to a base station can monitor the base station. For example, a non-anchor GW that is between the base station and the anchor GW monitors the base station (if enabled), but not the Anchor GW.

Keep alive Request Receiver

If the ASN GW/ASN PC receives a keep alive request from the base station, it responds with a keep alive response, whether or not you have enabled keep alive-based base station monitoring in the ASN GW/ASN PC service.

If the ASN GW/ASN PC is configured as legacy node and Keep Alive request message is received from the Base Station, the ASNGW/ASNPC will discard that Keep Alive request.

Table 24. Keep Alive Response

IE	M/O	Notes
Failure Indication	O	--
LRT	M	The time stamp of the keep alive RSP sender's last boot up; the value generated during

Note: MSID in the Keep Alive Request and Response will be all zeros.

Operation, Administration and Monitoring (OA & M)

Config command

Use this command to enable or disable the R6-based keep alive feature. The default is Disabled.

This command is not used to enable the BS Initiated Keep Alive Mechanism. If ASNGW/ASNPC receives the keep alive request, a response will be sent.

```

config
  context <context-name>
    asngw-service <asngw-service-name>
      [no | default] bs-monitor {icmp | keep-alive}
      bs-monitor interval <30-36000 seconds>
      bs-monitor num-retry <1-100>
      bs-monitor timeout <1-10 seconds>

```

Command Mode

```
config asngw-service
```

Keyword/Variable	Description
interval	Specifies the interval in seconds at which the keepalive Request messages are sent to the base station. Default is 60 seconds.
num-retry	Specifies the number of retries before the system determines that the base station is unreachable. Default is 5 retries.
timeout	Specifies the timeout value in seconds for retransmitting the keepalive Request message. Default is 3 seconds.

Show Commands

Use the show asngw-service command to view the status of active-base stations as either alive or unknown (inactive).

```
show asngw-service (all | (name <name>))
{bs-status {(address <ip-addr> |
(filter (all | monitored | no-calls | summary | up))}}
```

Example: Base Station Status

```
[local]st40# show asngw-service name asngw1 bs-status filter all    Service name:
asngw1
```

```
Context: asngweap
```

```
Bind: Done Max Subscribers: 2500000
```

```
IP address: 218.248.72.229 UDP Port: 2231
```

```
Service Status: Started GRE MTU: 1500 bytes
```

```
Mode : Non-legacy
```

```
Authentication: Single EAP
```

```
Policy msid-dhcp-chaddr-mismatch : DISALLOW
```

```
Policy ms-unexpected-network-reentry : ALLOW
```

```
Policy asngw-initiated-reauth : DISALLOW
```

```
Policy non-anchor-mode : ALLOW
```

```
Policy Newcall : NONE
```


Policy Overload : REJECT

Mobile IP FA context :

Maximum number of retransmissions : 3

Retransmission timeout : 3 secs

Setup timeout : 60 secs

Active-relay timeout : 15 secs

Handover anchor data-path termination timeout : 0 secs

Handover anchor data-path pre-registration termination timeout: 5 secs

Handover non-anchor data-path termination timeout : 5 secs

Handover non-anchor data-path pre-registration term timeout : 10 secs

Handover max number of data-path pre-registrations : 3

Idle-mode entry timeout : 60 secs

Idle-mode exit timeout : 60 secs

Idle-mode timeout : 4096 secs

Policy transaction-id-validation : ALLOW

Policy zero-function-type : DISALLOW

Transaction Id. Seed : 1

Peer ASNGW or ASNPC addresses(SIP Re-anchoring Flag) :

218.248.72.239(No) non-legacy

Maximum Number of Secondary IP Hosts : 0

Ran Peer Map Name : None

Mobile-IPv6 MAG context :

Mobile-IPv6 MAG service :

BS Monitor Config : Keep-Alive

Interval : 60 secs

Timeout : 3 secs Number of retries : 5

Total BSs : 1

Active BSs : 1

```

    Alive BSs : 0 ICMP/Keep-alive Monitored BSs : 1

    Inactive BSs : 0

    No Calls BSs : 0 Going Down BSs : 0

    BS status
    ----
    icmp/keepalive monitored

```

Example: Statistics

```
[local]st40# show asngw-service statistics function-type generalR6 Keep Alive
Req Msg:
```

```

    Total Sent: 14 Retransmissions Sent: 0

    Total Send Failures: 0

    Total Received: 0 Total Accepted: 0

    Total Relayed: 0

    Total Denied: 0 Total Discarded: 0

    Badly Formed: 0 Decode Error: 0

    Unspecified Error: 0 Missing Mandatory TLV: 0

    TLV Value Invalid: 0 Unknown TLV: 0

    Duplicate TLV Found: 0 No Session Found: 0

    No Resource Drops: 0 Admin Prohibited: 0

    Transaction Id. Error: 0

```

```
R6 Keep Alive Rsp Msg:
```

```

    Total Sent: 0 Retransmissions Sent: 0

    Total Send Failures: 0

    Total Received: 14 Total Accepted: 14

    Total Relayed: 0

    Total Denied: 0 Total Discarded: 0

    Badly Formed: 0 Decode Error: 0

```

Unspecified Error: 0 Missing Mandatory TLV: 0

TLV Value Invalid: 0 Unknown TLV: 0

Duplicate TLV Found: 0 No Session Found: 0

No Resource Drops: 0 Admin Prohibited: 0

Transaction Id. Error: 0

Total Sessions Connected: 1

```
[local]st40# show asnpc-service statistics function-type general
```

R6 Keep Alive Request Msg:

Total Received: 0 Total Accepted: 0

Total Relayed: 0

Total Denied: 0 Total Discarded: 0

Badly Formed: 0 Decode Error: 0

Unspecified Error: 0 Missing Mandatory TLV: 0

TLV Value Invalid: 0 Unknown TLV: 0

Duplicate TLV Found: 0 No Session Found: 0

No Resource Drops: 0 Admin Prohibited: 0

Transaction Id. Error: 0

R6 Keep Alive Response Msg:

Total Sent: 0 Retransmissions Sent: 0

Total Send Failures: 0

Total Sessions Connected: 0

SNMP Traps

The following SNMP traps indicate whether the base station is reachable.

- starBSReachable: This trap is sent if the base station is reachable from the ASN GW.
- starBSUnreachable: This trap is sent if the base station is not reachable from the ASN GW.

Chapter 5

WiMAX PMIPv6 Operation

Proxy Mobile IPv6 (PMIPv6) is network-based mobility for IPv6 nodes that uses and extends Mobile IPv6 signaling and home agent functionality.

The mobile node is not required to exchange signaling messages between itself and the home agent. Instead, a proxy mobility agent in the network performs the signaling with the home agent and performs the mobility management on behalf of the mobile node attached to the network.

Mobile Access Gateway Processing

The mobile access gateway (MAG) is a PMIPv6 term for the function that initiates the PMIP tunnel toward local mobility anchor (LMA). As far as WiMAX architecture is concerned, the MAG resides with the ASN GW and the LMA resides in the CSN.

The network access server or mobile access gateway obtains the Home Network Prefix before sending the first Router Advertisement. The HNP is received from the AAA server, or assigned by the LMA via PBU-PBA exchange.

The MAG sets related address configuration flags in the (un)solicit Router Advertisement sent to the MS corresponding to the address configuration mode associated with the MS's IP session.

Managing Binding Update List

Every mobile access gateway maintains a Binding Update List, which includes:

- The identifier of the attached mobile node: the MN-Identifier acquired during the mobile node's attachment to the access link.
- The link-layer identifier of the mobile node's connected interface: This is acquired from the received Router Solicitation messages from the mobile node or during the mobile node's attachment to the access network. This is typically a link-layer identifier conveyed by the mobile node.
- The IPv6 home network prefix of the attached mobile node: This is acquired from the mobile node's local mobility anchor through the received Proxy Binding Acknowledgement messages. The IPv6 home network prefix also includes the corresponding prefix length.
- The Link-local address of the mobile node on the interface attached to the access link.
- The IPv6 address of the local mobility anchor serving the attached mobile node: This address is acquired from the mobile node's policy profile or from other means.
- The Interface identifier (If-Id) of the access link where the mobile node is currently attached: This is internal to the mobile access gateway and is used to associate the Proxy Mobile IPv6 tunnel to the right access link where the mobile node is attached.
- The interface identifier (If-Id) of the bi-directional tunnel between the mobile node's local mobility anchor and the mobile access gateway: This is internal to the mobile access gateway. The tunnel interface identifier is acquired during the tunnel creation.
- A flag indicating whether GRE encapsulation is enabled and the reverse and forward GRE key identifier used in GRE encapsulation.

Other MAG Functions

The following lists other functions that are performed as part of MAG or access-side service:

- Detection of the mobile node's movements on the access link and for initiating the mobility signaling with the mobile node's local mobility anchor.
- Emulation of the mobile node's home link on the access link by sending Router Advertisements with the mobile node's home network prefix information and responding to Router Solicitations.
- Setting up the data path to enable the mobile node to configure an address from its home network prefix and use it from its access link.
- Tunnelling of Mobile Nodes' data traffic to the LMA and delivering or receiving data traffic from the Mobile Node.
- Revocation Support between MAG and LMA.

LMA Operation

The LMA supports in-band protocol security. The received PBU that entails signaling protection in the form of valid authentication option receives a PBA that uses the same protection mechanism. The PBUs received without embedded signaling protection are processed and acknowledged only if the source MAG is trusted and Authentication Options (AO) are not enforced for that PMIPv6 peer. When the in-band signaling protection is enabled, the LMA participates in the PMIPv6 key derivation and management process.

If the R3 reference point is completely IPv4-based, the LMA accepts the registration of IPv4 Proxy CoA to the MS's BCE. The LMA verifies that the PMIPv6 mobility management for the attaching IPv4 MS is permitted at the time of processing the initial PBU through the AAA query.

Managing Binding Cache Entry Data Structure

LMA is similar in its functions to a Mobile IPV6 Home Agent. One of the major differences between PMIPv6 and Mobile IPV6 is the use of a Home Network Prefix in PMIPv6 as opposed to the fully-qualified 128-bit HoA in Mobile IPV6. PMIPv6 only supports the Per-MN-Prefix model and does not support Shared-Prefix model. There is a unique home network prefix assigned to each mobile node, and no other node shares an address from that prefix.

Access Authentication

The LMA uses the MN-Identifier option to authenticate and load a subscriber profile. The MN-Identifier option is mandatory in a PBU request.

Proxy Binding Update Processing in LMA

Proxy Binding Update (PBU) uses messages similar to Binding Updates in Mobile IPV6. The messages are processed in a way that is similar to BU processing in MIPv6 HA. The following are the main differences between BU and PBU processing.

- The Home Address Destination Option is not present in PBU, but is a required option in MIPv6 BU.
- Authenticate Proxy BU requests use the security parameters index (SPI) in the IPSEC header.

Sequencing PBU processing

A timestamp option is supported in LMA that enables or disables the use of a timestamp for PBU re-sequencing. It is enabled by default. When enabled, the sequence number based re-sequencing will not be preformed in the LMA.

Other LMA Functions

The LMA supports the following functions:

- Static/Dynamic Home Network Prefix (HNP) Support. For a static HNP prefix, the LMA assigns the HNP in the Home Network Prefix option, if it is available to the subscriber through subscriber's available static pools.
- Multi-homing support.
- Tunneling packets matching MN's HNP to MAG using IP6-in-6:
 - IPv6 header (src= LMAA, dst= Proxy-CoA /* Tunnel Header */
 - IPv6 header (src= CN, dst= MN-HOA) /* Packet Header */
- Tunneling packets matching MN's HNP to MAG using GRE if in GRE Mode:
 - IPv6 header (src= LMAA, dst= Proxy-CoA /* Tunnel Header */
 - GRE header /* Packet Header */
- Revocation Support to delete a binding in MAG.

BCE (Binding Cache Entry) lookup on LMA

The following parameters are used as key to look up a session in the LMA:

- IPv6 Home Address (from HNP mobility option)
- MN-ID (from MN-Identifier option)
- IPv4 Home Address (when IPv4 Home address Option is present)

MN-ID option must always be present in the PBU/PBA. Either the HNP or IPv4 HoA option must be present in a PBU request. If the HNP/IPv4 HoA is present in the initial PBU, they are present in all the remaining PBU requests for session lookup.

When the HNP or IPv4 HoA option is zero, the MN-ID is used for BCE lookup.

Fallback Mechanism between PMIPv6 and PMIPv4

This section briefly describes the fallback mechanism from PMIPv6 to PMIPv4. The following assumptions must be taken into consideration:

- fa-service is configured and running.
- The AAA server supports the SN1-Proxy-MIP = Enabled RADIUS attribute in Access-Accept or the subscriber configuration has the proxy-mip flag set to allow.
- The AAA server does not support the Service Info attribute and therefore, does not send the attribute in the Access-Accept messages

The following table shows the network access server's (NAS) behavior based on whether:

- The SN1-Proxy-MIP is present in Access-Accept messages
- The SN1-Proxy-MIP is configured locally in subscriber templates
- The Service Info attribute is present or absent in Access-Accept messages during the authentication and authorization phase.

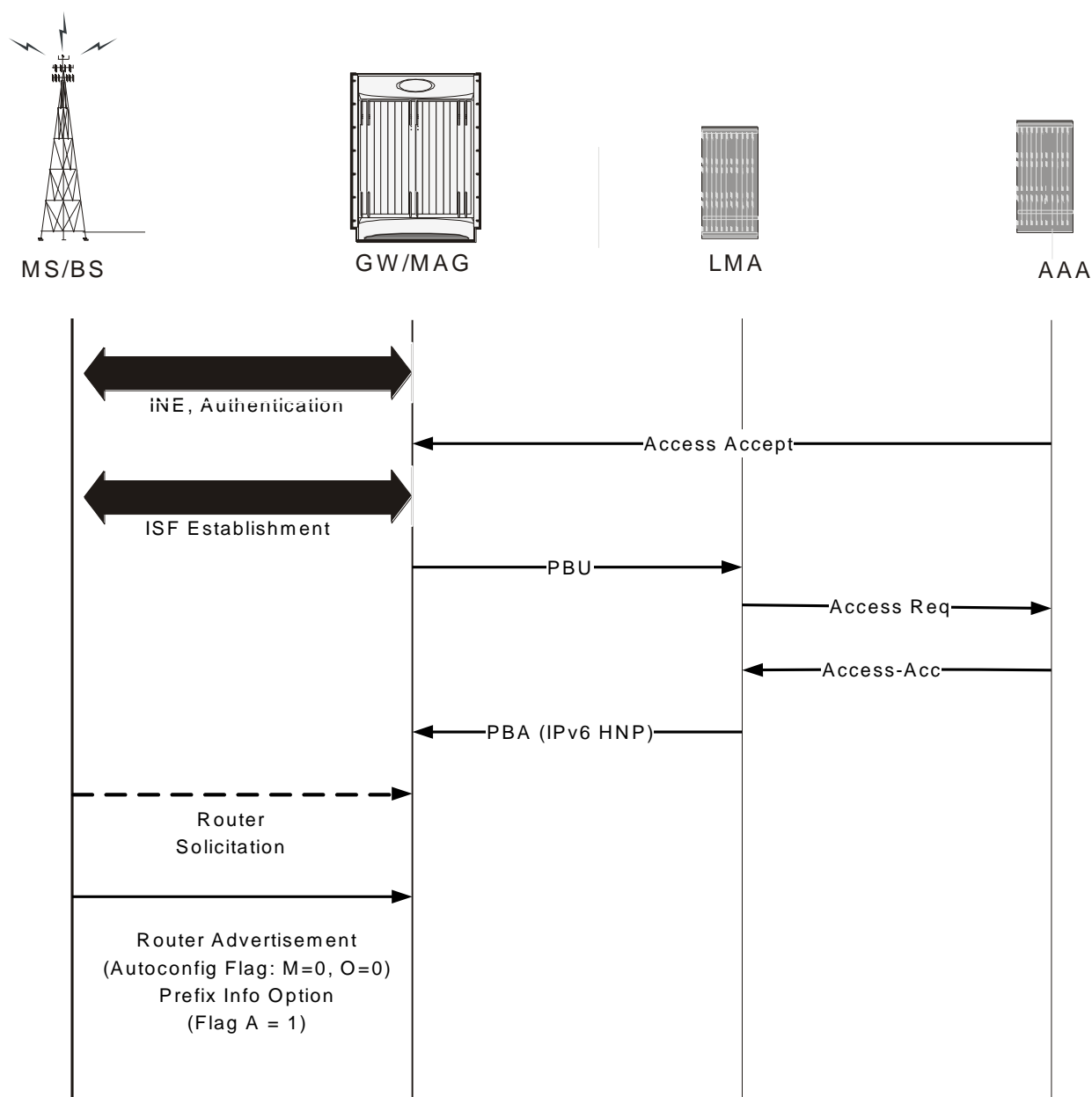
Table 25. NAS Behavior Based on SN1-Proxy-MIP and Service Info Attribute

SN1-Proxy-MIP	Service Info, if received in Access-Accept	NAS Behavior
0	0	Treated as an SIPv4 call.
0	1	This is a success scenario. PMIPv6 is triggered. The acquisition of the home address is based on the bit set in the Service Info attribute.
1	0	This is a success scenario. PMIPv4 is triggered. The acquisition of the home address is IPv4.
1	1	This is a success scenario. PMIPv6 is triggered. The acquisition of the home address is based on the bit set in the Service Info attribute.

PMIPv6 Call Flows: Connection Setup

The following illustrations show call flows of IPv4/IPv6 acquisition by MSs using PMIPv6.

Figure 39. Stateless IPv6 Address Auto-configuration



PMIPv6 Call Flow-renew

Session renewal in the case of PMIPv6 service is about extending both the address lifetime of the MS and PMIPv6 session lifetime of the LMA.

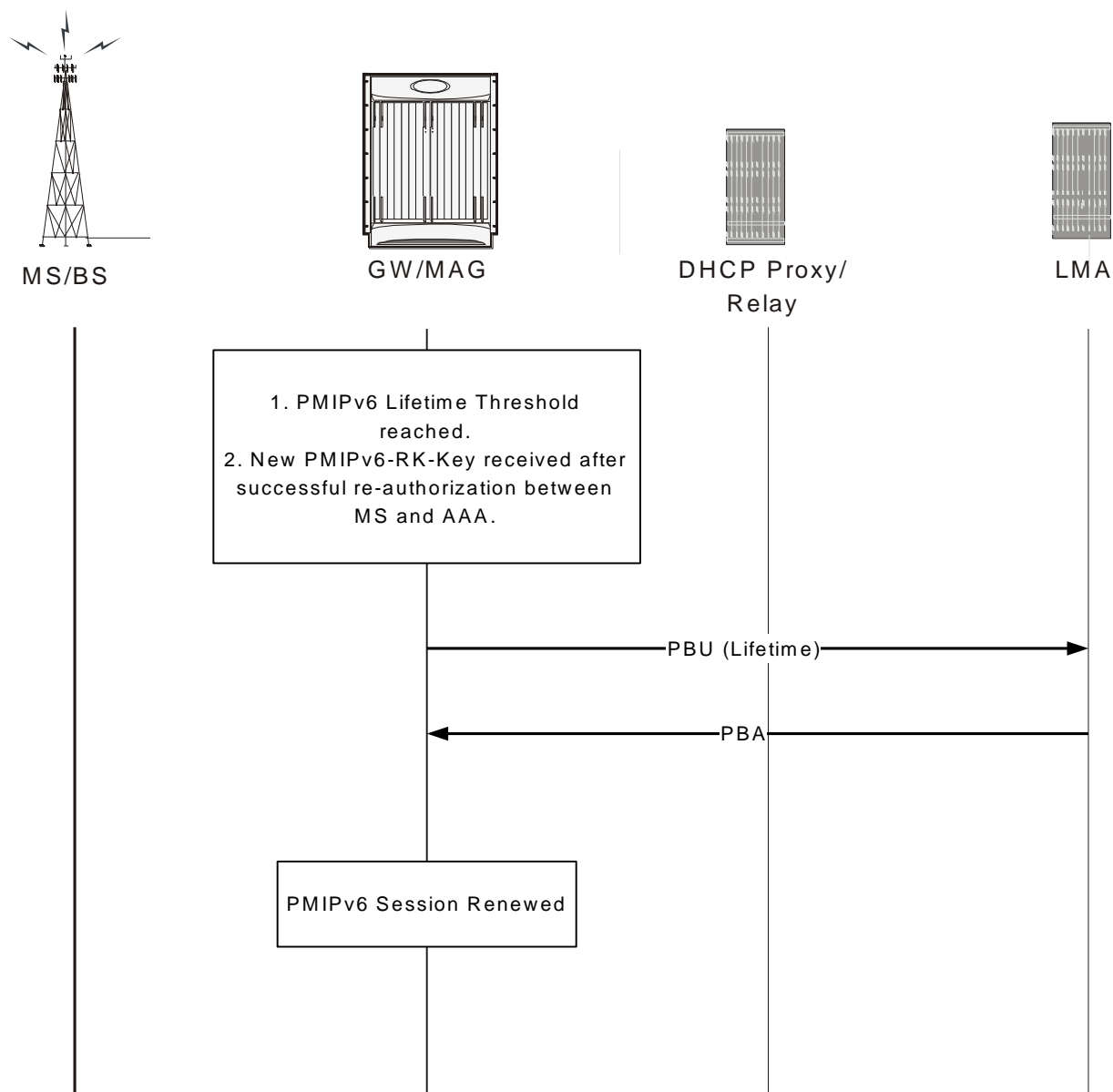
To extend the lifetime of an existing binding at the LMA, the AR/MAG ASN sends a Proxy Binding Update message with the Handoff indicator option set to a value of 5 (Re-registration) and a new specific lifetime. Upon accepting the PBU request for extending the lifetime of a currently active binding, the LMA updates the lifetime for that binding and sends a PBA message to the MAG ASN.

There are two triggers for PMIPv6 renewal:

- Once the re-auth is completed successfully on MSK lifetime expiry and new PMIPv6-RK-Key and SPI is available on ASNGW/MAG.
- Expiry of the Reg lifetime. Usually, renew happens before the expiry of the lifetime. This is configurable on MAG service and by default, after 75% of regular lifetime expiry, renew occurs.

Session-Timeout received on LMA is treated as absolute timeout and LMA trigger revocation after absolute timeout expires.

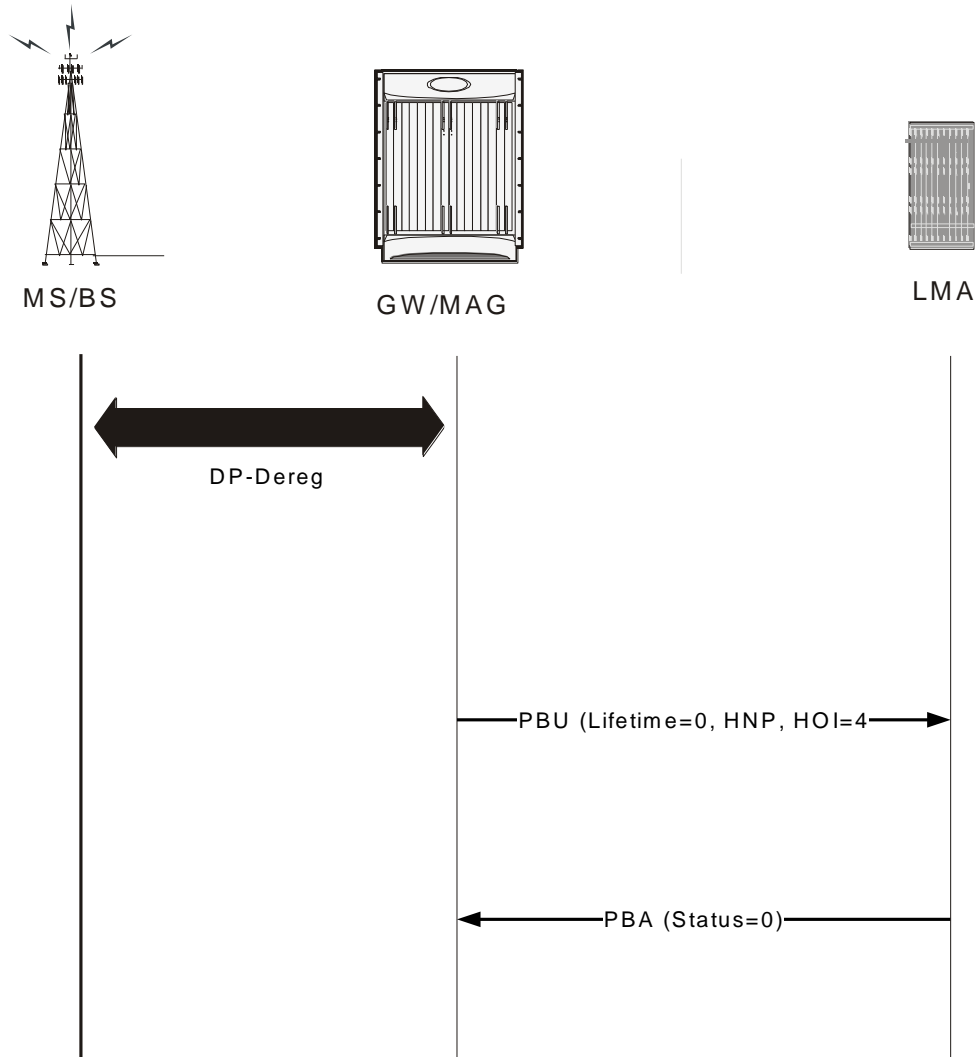
Figure 40. PMIPv6 Call Flow-renew



PMIPv6 Call Flow: Connection Teardown

If the ASN GW detects a reason for PMIPv6 session termination, it initiates data path de-registration along the R4/R6 path with the serving BS.

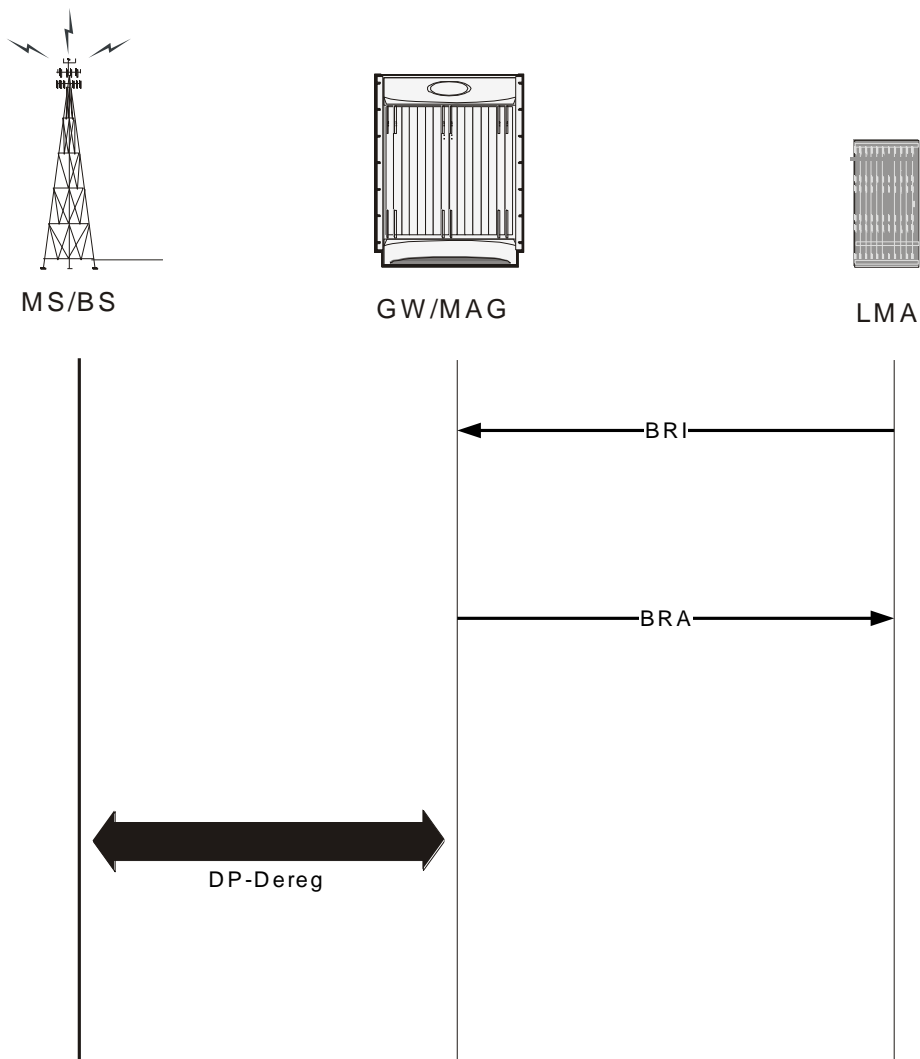
The MS initiates the IP session release by performing the DHCPv6 Release Procedure (DHCPv4 Release in the case of an IPv4 MS) either self-initiated (MS triggered termination) or in response to the DP-Dreg directive received (ASNGW triggered).

Figure 41. MS/BS Initiated Connection Release

PMIPv6 Call Flow: Connection Release by LMA

If the MS's mobility binding expires or is terminated, the LMA initiates PMIPv6 session release by sending the Binding Revocation Indication (BRI) message to the AR/MAG (Proxy-CoA) for the MS attached to it. In response, MAG/GW triggers the R6 teardown process and sends back the BRA (Binding Revocation Acknowledgement).

Figure 42. PMIPv6 Connection Release by LMA



Operation, Administration, and Maintenance

You must configure Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG) to support PMIPv6. Note that for WiMAX PMIPv6, you are reusing the LMA and MAG service.

ASNGW Service Configuration Commands

```
config

context <context-name>

[context-name]st40(config-asngw-service)# [no]mobile-access-gateway context
<name> [mag-service <name>]

#exit

end
```

MAG Service Configuration Commands

The MAG service is responsible for PMIPv6 signaling. MAG service establishes and maintains a bi-directional tunnel for the subscriber traffic with the LMA.

```
config

context <context-name>

[no] mag-service <mag-service-name> [-no-confirm]

bind address <ipv6-address> [max-subscribers 0..3000000 ]

[default] renew-percent-time <1..100> /* Configures percentage of lifetime at
which renewal is sent (range 1 to 100). Default is 75 */

[default] retransmission-timeout <100..100000> /* Configures retransmission
timeout of PMIP6 BUs (range 100 to 100000 mseconds).

Default is 3 */

[default] max-retransmissions < 1 .. 100> /* Configures maximum number of
retransmissions of PMIP6 Bus range 1 to 4294967295).Default is 5 */

[default] reg-lifetime [<1..262140>] /* in units of second. Max will be
(65535*4). Default will be 600 secs. */

[default] encapsulation [gre|ipip] /* Default is GRE */
```



```
[default] information-element-set [standard | custom1]

/*Changes the set of Information Elements included in PBUs. When set to
standard, the Information elements specified in 3gpp2 29.275 will be
included in PBUs. Custom options are for customer specific set of IEs */

#exit

end
```

A configurable in the access-technology service configuration specifies the context of MAG service and also option to use specific to mag-service from the context.

```
Config

Context <context-name>

    asngw-service <service-name> /* asngw that needs PMIPv6 service */

    mobility-access-gateway context <context-name> mag-service
<service-name>

    #exit

#exit

Config

context <context-name>

subscriber <subscriber-name>

    [no|default] asn-service-info mobility [ipv4 | ipv6 | ipv6-ipv4]

    #exit

#exit

#end
```

show subscribers

The **show subscribers** command on MAG displays the network type as using PMIPv6 for IPv4 or IPv6 PDN.

Example

```
[local]st40# show sub all

Access (S) - pdsn-simple-ip (M) - pdsn-mobile-ip (H) - ha-mobile-ip
```

```

Type: (P) - ggsn-pdp-type-ppp (h) - ha-ipsec (N) - lns-l2tp
      (I) - ggsn-pdp-type-ipv4 (A) - asngw-simple-ip (G) - IPSP
      (V) - ggsn-pdp-type-ipv6 (B) - asngw-mobile-ip (C) - cscf-sip
      (R) - sgw-gtp-ipv4 (O) - sgw-gtp-ipv6 (Q) - sgw-gtp-ipv4-ipv6
      (W) - pgw-gtp-ipv4 (Y) - pgw-gtp-ipv6 (Z) - pgw-gtp-ipv4-ipv6
      (s) - sgsn (p) - sgsn-pdp-type-ppp
      (4) - sgsn-pdp-type-ip (6) - sgsn-pdp-type-ipv6
      (L) - pdif-simple-ip (K) - pdif-mobile-ip (o) - femto-ip
      (F) - standalone-fa (J) - asngw-non-anchor
      (e) - ggsn-mbms-ue (i) - asnpc (R) - pdg-direct-ip
      (E) - ha-mobile-ipv6 (u) - Unknown (Q) - pdg-ttg
      (f) - hnbgw (g) - hnbgw-ue (x) - s1-mme
      (a) - phsgw-simple-ip (b) - phsgw-mobile-ip
      (j) - phsgw-non-anchor (c) - phspc
      (E) - ha-mobile-ipv6 (X) - HSGW
      (l) - pgw-pmip (u) - Unknown
      |
      |+Access (X) - CDMA 1xRTT (E) - GPRS GERAN (I) - IP
      ||Tech: (D) - CDMA EV-DO (U) - WCDMA UTRAN (W) - Wireless LAN
      ||(A) - CDMA EV-DO REVA (G) - GPRS Other (M) - WiMax
      ||(C) - CDMA Other (N) - GAN (O) - Femto IPSec
      ||(P) - PDIF (S) - HSPA (L) - eHRPD
      ||(T) - eUTRAN (Q) - PDG (F) - FEMTO UTRAN
      ||(H) - PHS (.) - Other/Unknown
      |||+Call (C) - Connected (c) - Connecting
      |||State: (d) - Disconnecting (u) - Unknown
      ||| (r) - CSCF-Registering (R) - CSCF-Registered
      ||| U) - CSCF-Unregistered
      |||

```

```

|||+--Access (A) - Attached (N) - Not Attached
||| CSCF (.) - Not Applicable
||| Status
|||
|||+--Link (A) - Online/Active (D) - Dormant/Idle
|||| Status:
||||
|||||+Network (I) - IP (M) - Mobile-IP (L) - L2TP
|||||Type: (P) - Proxy-Mobile-IP (i) - IP-in-IP (G) - GRE
||||| (V) - IPv6-in-IPv4 (S) - IPSEC (C) - GTP
||||| (A) - R4 (IP-GRE) (T) - IPv6 (u) - Unknown
||||| (W) - PMIPv6(IPv4) (Y) - PMIPv6(IPv4+IPv6) (R) - IPv4+IPv6
||||| (v) - PMIPv6(IPv6)
|||||
|||||
vvvvvvv CALLID MSID USERNAME IP TIME-IDLE
-----

1MCNAT 00e52fe1 - {am=2}eap-user1@test.com baaa::e52f:e101 00h00m03s
AMCNAP 017dc661 0000000012345 {am=2}eap-user1@test.com baaa::1:2345:0 00h00m05s

```

show subscribers summary

The **show subscribers summary** command shows the number of subscribers on PMIPv6 for IPv4 or IPv6 PDN.

Example

```

[local]st40# show subscribers summary

Total Subscribers: 2

Active: 2

Dormant: 0

```

pdsn-simple-ipv4: 0

pdsn-simple-ipv6: 0

pdsn-mobile-ip: 0

ha-mobile-ipv6: 0

hsgw-ipv6: 0

hsgw-ipv4 : 0

hsgw-ipv4-ipv6: 0

pgw-pmip-ipv6 : 1

pgw-pmip-ipv4 : 0

pgw-pmip-ipv4-ipv6 : 0

pgw-gtp-ipv6 : 0

pgw-gtp-ipv4 : 0

pgw-gtp-ipv4-ipv6 : 0

sgw-ipv6 : 0

sgw-ipv4 : 0

sgw-ipv4-ipv6 : 0

mme : 0

ipsg-rad-snoop : 0

ipsg-rad-server : 0

ha-mobile-ip: 0

ggsn-pdp-type-ppp: 0

ggsn-pdp-type-ipv4: 0

lms-l2tp: 0

ggsn-pdp-type-ipv6: 0

ggsn-mbms-ue-type-ipv4: 0

pdif-simple-ipv4: 0

pdif-simple-ipv6: 0

pdif-mobile-ip: 0

```
pdg-direct-ip: 0
pdg-ttg: 0
femto-ip : 0
sgsn: 0
sgsn-pdp-type-ppp: 0
sgsn-pdp-type-ipv4: 0
sgsn-pdp-type-ipv6: 0
type not determined: 0
asngw-simple-ipv4: 0
asngw-simple-ipv6: 1
asngw-mobile-ip: 0
asngw-non-anchor: 0
phsgw-simple-ipv4: 0
phsgw-simple-ipv6: 0
phsgw-mobile-ip: 0
phsgw-non-anchor: 0
```

show asngw-service session full

Use the **show asngw-service session full** command to see a detailed report of a session.

Example

```
[local]st40# show asngw-service session full

Username: {am=2}eap-user1@test.com Callid: 00004e23

Pseudoname: n/a

MSID: 000000012345 Home Address(IPv4): n/a

ASNGW Service Address: 218.248.72.229 Session Type: Anchor

Authenticator Address: 218.248.72.229 Anchor Address: 218.248.72.229

Data Path Status: Active PCLR Address: n/a
```

```
CMAC Key Count: 1 Home Address(IPv6): baaa:0:0:6::  
MSK Lifetime: 00h01m00s Remaining MSK Lifetime: 00h00m55s  
Number of Re-authentications: 0  
Authentication Mode: Device(Single EAP)  
EAP-Type: EAP-PSK
```

show mag all

Example

```
[local]st40# show mag all  
  
Service name: mag-v6-1  
Context: asngweap  
Bind: Done Max Sessions: 2500000  
Local IPv6 Address: bbbb::101:1  
Lifetime: 00h10m00s  
PMIP Max Retransmissions: 5  
PMIP Retrans Timeout: 3000(msecs)  
PMIP Retrans Policy: exponential-backoff  
PMIP Renew Percent Time: 75%  
Encapsulation Type: GRE  
IE-set Type: standard  
Service Status: Started  
Newcall Policy: None  
Total MAG Sessions: 2
```

show mag statistics

MAG statistics are maintained per service and display the statistics for the particular service if the service name is specified. Use **show mag statistics** to display the statistics for all the services in the context. If you enter the

command in the local context, the command returns the cumulative statistics for all the MAG services in all the contexts.

Example

```
#show mag statistics [mag-service <name>] -- will display mag stats
```

```
MAG Service: mag-v6-1
```

```
Binding Updates Sent:
```

```
Total: 6
```

```
Init Request Xmit: 3 Init Request Re-Xmit: 0
```

```
Renew Request Xmit: 2 Renew Request Re-Xmit: 0
```

```
Dereg Request Xmit: 1 Dereg Request Re-Xmit: 0
```

```
Binding Acknowledgement Rcvd:
```

```
Total: 6 Errors: 0
```

```
Accepted: 6 Denied: 0
```

```
Init Reply Rcvd: 3 Renew Reply Rcvd: 2
```

```
Dereg Reply Rcvd: 1
```

```
Denied by LMA:
```

```
Insufficient Resources: 0 Mismatched ID: 0
```

```
MN Auth Failure: 0 Admin Prohibited: 0
```

```
Msg ID Required: 0 DAD Failed: 0
```

```
Not Home Subnet: 0 Sequence Out Of Window: 0
```

```
Reg Type Change Disallowed: 0 Unspecified Reason: 0
```

```
Service-Authorization Failed:0 Proxy Reg Not Enabled: 0
```

```
Timestamp Mismatch: 0 Timestamp Lower Than
```

```
Expected:0
```

```
Missing MN-ID Option: 0 Missing HNP Option: 0
```

```
Missing Access Tech Option: 0 Missing Handoff Ind Opt: 0
```

```
Not Authorized For HNP: 0 Not LMA For Mobile: 0
```

```
Not Authorized For Proxy Reg:0 BCE Prefix No Match: 0
```

GRE Key Option Required: 0

Binding Acknowledgement Error Reason:

Missing HNP: 0 Missing NAI: 0

Home Address Conflict: 0 Match Request Not Found: 0

Badly Formed: 0 Checksum Error: 0

Session Not Found: 0

Binding Revocation:

Sent: 0 Retries Sent: 0

Ack Rcvd: 0 Not Acknowledged: 0

Rcvd: 2 Ack Sent: 2

Received Binding Revocation Trigger Reasons:

Reserved: 0 Unspecified: 0

Administrative Reason: 2 Inter-MAG Handoff-Same ATT: 0

Inter-MAG - Unknown Handoff: 0 Inter-MAG Handoff-Diff ATT: 0

Per-Peer Policy: 0 Revoking Node Local Policy: 0

User Initiated Session Term: 0 Access Network Session Term: 0

IPv4 HoA Binding Only: 0 Out-of Sync BCE State: 0

Unknown: 0

Sent Revocation ACK Status:

Success: 2 Partial-Success: 0

Binding-Does-Not-Exist: 0 No IPv4-HoA-Bind: 0

Global-Revoc-Not-Authorized: 0 Cannot-Identify-Binding: 0

Revoc-Failed-MN-Attached: 0 Unknown: 0

Binding Revocation Indication Discarded:

Total: 0

Session Not Found: 0 Badly Formed Request: 0

Decode Error: 0 Checksum Error: 0

Invalid Message Type: 0 No Memory: 0

Tunnel Data Received:


```
Total Packets : 10
6in6: 0 4in6: 0
IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 10
Total Bytes : 1280
6in6: 0 4in6: 0
IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 1280
Errors:
Protocol Type Error: 0 Invalid Pkt Length: 0
No Session Found: 0
Tunnel Data Sent:
Total Packets: 10
6in6: 0 4in6: 0
IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6) 10
Total Bytes: 1760
6in6: 0 4in6: 0
IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6) 1760
Total Disconnects/Failures: 3
Lifetime expiry: 0 Access Initiated Term: 1
Admin Drops: 0 Other Reasons: 0
LMA Revocations: 2
```

Example

```
config
context <context-name>
[no] pgw-service <pgw-service-name> [-no-confirm]
[no] associate lma-service [<lma-svc-name>]
exit
```

Example

```

config

context <context-name>

[no] lma-service <lma-service-name> [-no-confirm] bind <ipv6-address> [max-
subscribers 0..3000000 ]

[default] reg-lifetime [<1..262140>] /* in units of second. Max will be
(65535*4) .

Default will be 600 secs.

[no|default] sequence-number-validate /*By default it will be enabled */

[no|default] refresh-advice-option /*By default this option will be disabled */

[default] refresh-interval-percent <1-99> /* Default will be 75percent*/

[default] simul-bindings [1..3] /* Default number of binding supported will be
1 */

[no | default] aaa accounting /*Default accounting will be enabled */

[no] default subscriber <template-name> /* To set name of default subscriber
template to be used for the service */

[no|default] setup-timeout [1..1000000] /* Setup timeout config for the service
*/

[no|default] sequence-number-validate mode [timestamp|seq-no]/* By default it
will be enabled to timestamp mode */

[default] timestamp-replay-protection tolerance [0..65535] /* Default will be
replay protection using timestamp with default tolerance of 7 sec. Timestamp
tolerance 0 Indicates infinite tolerance.*/

[default] revocation max-retransmission [0..10] /* Default value 3 */

[default] revocation retransmission-timeout [500..10000] /* timeout in msec.
Default value 3 sec */

[no|default] revocation enable /* Config to enable revocation from LMA

Default Disabled */

#exit

#exit

End

```

Example

```

config
    context <context-name>
    subscriber <subscriber-name>
    [no|default] asn-service-info mobility [ipv4 | ipv6 | ipv6-ipv4]
    #exit
#exit
#end

```

LMA Service Configuration Commands

For an LMA service to start a PGW service, they must be configured in the same context and point to the lma-service.

The P-GW service can associate with either LMA or EGTP service to function as PMIP/GTP PGW respectively. Any common configuration for a PGW functionality is available in the PGW service. Protocol-specific configuration is available in the EGTP/LMA service.

Show Commands

In the case of multiple PDNs per subscriber, each PDN connection is displayed on separate lines in the **show subscriber** output.

```

Access (S) - pdsn-simple-ip (M) - pdsn-mobile-ip (H) - ha-mobile-ip
Type: (P) - ggsn-pdp-type-ppp (h) - ha-ipsec (N) - lns-l2tp
(I) - ggsn-pdp-type-ipv4 (A) - asngw-simple-ip (G) - IPSP
(V) - ggsn-pdp-type-ipv6 (B) - asngw-mobile-ip (C) - cscf-sip
(R) - sgw-gtp-ipv4 (O) - sgw-gtp-ipv6 (Q) - sgw-gtp-ipv4-ipv6
(W) - pgw-gtp-ipv4 (Y) - pgw-gtp-ipv6 (Z) - pgw-gtp-ipv4-ipv6
(s) - sgsn (p) - sgsn-pdp-type-ppp
(4) - sgsn-pdp-type-ip (6) - sgsn-pdp-type-ipv6
(L) - pdif-simple-ip (K) - pdif-mobile-ip (o) - femto-ip
(F) - standalone-fa (J) - asngw-non-anchor
(e) - ggsn-mbms-ue (i) - asnpc (R) - pdg-direct-ip

```

```

(E) - ha-mobile-ipv6 (u) - Unknown (Q) - pdg-ttg
(f) - hnbgw (g) - hnbgw-ue (x) - s1-mme
(a) - phsgw-simple-ip (b) - phsgw-mobile-ip
(j) - phsgw-non-anchor (c) - phspc
(E) - ha-mobile-ipv6 (X) - HSGW
(l) - pgw-pmip (u) - Unknown
|
|Access (X) - CDMA 1xRTT (E) - GPRS GERAN (I) - IP
|Tech: (D) - CDMA EV-DO (U) - WCDMA UTRAN (W) - Wireless LAN
|A) - CDMA EV-DO REVA (G) - GPRS Other (M) - WiMax
|(C) - CDMA Other (N) - GAN (O) - Femto IPsec
|(P) - PDIF (S) - HSPA (L) - eHRPD
|(T) - eUTRAN (Q) - PDG (F) - FEMTO UTRAN
|(H) - PHS (.) - Other/Unknown
||
||+ Call (C) - Connected (c) - Connecting
||| State: (d) - Disconnecting (u) - Unknown
||| (r) - CSCF-Registering (R) - CSCF-Registered
||| (U) - CSCF-Unregistered
|||
|||+--Access (A) - Attached (N) - Not Attached
||| CSCF (.) - Not Applicable
||| Status
|||
|||+--Link (A) - Online/Active (D) - Dormant/Idle
||| Status:
|||
|||+Network (I) - IP (M) - Mobile-IP (L) - L2TP
|||Type: (P) - Proxy-Mobile-IP (i) - IP-in-IP (G) - GRE

```

```

||||| (V) - IPv6-in-IPv4 (S) - IPSEC (C) - GTP
||||| (A) - R4 (IP-GRE) (T) - IPv6 (u) - Unknown
||||| (W) - PMIPv6(IPv4) (Y) - PMIPv6(IPv4+IPv6) (R) - IPv4+IPv6
||||| v) - PMIPv6(IPv6)
|||||
|||||

vvvvvvv CALLID MSID USERNAME IP TIME-IDLE

----- 1MCNAT
004c9962 -{am=2}eap-user1@test.com baaa::5:0:0:4c99:6201 00h00m03s

AMCNAP 017dc664 000000012345 {am=2}eap-user1@test.com baaa::5:0:1:2345:0
00h00m04s

Total subscribers matching specified criteria: 2

```

show subscriber summary

Use this command to display the number of MAG PMIPv6 sessions.

Example

```

# show subscribers summary

Total Subscribers: 2

Active: 2

Dormant: 0

pdsn-simple-ipv4: 0

pdsn-simple-ipv6: 0

pdsn-mobile-ip: 0

ha-mobile-ipv6: 0

hsgw-ipv6: 0

hsgw-ipv4 : 0

hsgw-ipv4-ipv6 : 0

pgw-pmip-ipv6 : 1

```

```
pgw-pmip-ipv4 : 0
pgw-pmip-ipv4-ipv6 : 0
pgw-gtp-ipv6 : 0
pgw-gtp-ipv4 : 0
pgw-gtp-ipv4-ipv6 : 0
sgw-ipv6 : 0
sgw-ipv4 : 0
sgw-ipv4-ipv6 : 0
mme : 0
ipsg-rad-snoop : 0
ipsg-rad-server: 0
ha-mobile-ip: 0
ggsn-pdp-type-ppp: 0
ggsn-pdp-type-ipv4: 0
lms-l2tp: 0
ggsn-pdp-type-ipv6: 0
ggsn-mbms-ue-type-ipv4: 0
pdif-simple-ipv4: 0
pdif-simple-ipv6: 0
pdif-mobile-ip: 0
pdg-direct-ip: 0
pdg-ttg: 0
femto-ip : 0
sgsn: 0
sgsn-pdp-type-ppp: 0
sgsn-pdp-type-ipv4: 0
sgsn-pdp-type-ipv6: 0
type not determined: 0
asngw-simple-ipv4: 0
```

```
asngw-simple-ipv6: 1
asngw-mobile-ip: 0
asngw-non-anchor: 0
phsgw-simple-ipv4: 0
phsgw-simple-ipv6: 0
phsgw-mobile-ip: 0
```

show lma all

The following command lists all the LMA sessions on the PGW.

Example

```
# show lma all -.
Service name: lma-v6
Context: asngweap
Bind: Done Max Subscribers: 4000000
Local IPv6 Address: dddd::200:1
Lifetime: 00h10m00s Simul Bindings: 1
Setup Timeout: 60 sec
Sequence Number Validation: Enabled
Refresh Advice Option: Disabled Refresh Interval Percent: 75
Timestamp Replay Protection: Enabled Timestamp Tolerance: 7 sec
Binding Revocation: Enabled
Bind-Revocation Max Retries: 3 Bind-Revocation Timeout: 3000(msecs)
Default Subscriber: None AAA accounting: Disabled
Service Status: Started
Newcall Policy: None
PGW(LMA) session license limit: OK
```

show lma-service full

Use the following command to see a detailed report of a session.

Example

```
# show lma-service session full

Username: {am=2}eap-user1@test.com

Callid: 004c9962

Home Address: baaa:0:0:5::/64

LMA Address: dddd::200:1

BSID: n/a

ESN: n/a

MEID: n/a

Charging ID: 9336887

Binding #1:

MAG Address: bbbb::101:2

Lifetime: 00h00m55s Remaining Life: 00h00m31s

Sess-Delete Timer Running: NO Remaining Sess-Time: n/a

Encapsulation Type: IPv6-GRE

GRE Key(Fwd): 264641 GRE Key(Rev): 52929

RAT Type: IEEE 802.16e
```

show lma-service statistics name lma-v6

LMA statistics are maintained per service and display the statistics for the particular service if the service name is specified.

Example

```
[local]st40# show lma-service statistics name lma-v6

LMA Service: lma-v6
```


MIP AAA Authentication:

Attempts: 11 Success: 11

Total Failures: 0

Actual Auth Failures: 0 Misc Auth Failures: 0

Binding Updates Received:

Total Received: 12 Total Accepted: 12

Total Denied: 0 Total Discarded: 0

Initial Binding Update Requests:

Received: 6 Accepted: 6

Denied: 0

Refresh Binding Update Requests:

Received: 5 Accepted: 5

Denied: 0

DeReg Requests:

Received: 1 Accepted: 1

Denied: 0

Handoff Requests:

Received: 0 Accepted: 0

Denied: 0

Binding Acknowledgements Sent:

Total: 12 Accepted Reg: 11

Accepted DeReg: 1 Denied: 0

Send Error: 0

Binding Update Deny Reasons:

Insufficient Resources: 0 Mismatched ID: 0

MN Auth Failure: 0 Admin Prohibited: 0

Msg ID Required: 0 DAD Failed: 0

Not Home Subnet: 0 Sequence Out Of Window: 0

Reg Type Change Disallowed: 0 Unspecified Reason: 0

Service-Authorization Failed:0 Proxy Reg Not Enabled: 0
Timestamp Mismatch: 0 Timestamp Low ThanExpected:0
Missing MN-ID Option: 0 Missing HNP Option: 0
Missing Access Tech Option: 0 Missing Handoff Ind Option: 0
Not Authorized For HNP: 0 Not LMA For Mobile: 0
Not Authorized For Proxy Reg:0 BCE Prefix Do Not Match: 0
GRE Key Option Required: 0
Update Denied - Insufficient Resource Reasons:
No Session Manager: 0 No Memory: 0
Session Manager Rejected: 0 Input-Q Exceeded: 0
Simul Bindings Exceeded: 0 Address Alloc Failed: 0
Update Denied - Admin Prohibited Reasons: MN-AAA Auth Option Missing: 0 H-bit
Not Set: 0
Invalid MN-AAA Option SPI: 0 Invalid MN-HA Option SPI:0
Congestion Control Denied: 0 Policy Rejected: 0
HoA Not Authorized: 0 No Permission: 0
Bad Request: 0
Binding Updates Discard Reasons:
Congestion Discarded: 0 Checksum Error: 0
Initial Auth Pending: 0 Session Not Found: 0
HAMGR Not Ready: 0 Decode Failure: 0
Invalid Buffer Length: 0 Revocation Pending: 0
Binding Revocation:
Sent: 5 Retries Sent: 0
Ack Rcvd: 5 Not Acknowledged: 0
Rcvd: 0 Ack Sent: 0
Sent Revocation Trigger Reasons:
Reserved: 0 Unspecified: 0
Administrative Reason: 5 Inter-MAG Handoff-Same ATT: 0

```
Inter-MAG - Unknown Handoff: 0 Inter-MAG Handoff-Diff ATT:0
Per-Peer Policy: 0 Revoking Node Local Policy: 0
User Initiated Session Term: 0 Access Network Session Term:0
IPv4 HoA Binding Only: 0 Out-of Sync BCE State: 0
Unknown: 0

Received Revocation ACK Status:

Success: 5 Partial-Success: 0

Binding-Does-Not-Exist: 0 No IPv4-HoA-Bind: 0

Global-Revoc-Not-Authorized: 0 Cannot-Identify-Binding:0
Revoc-Failed-MN-Attached: 0 Unknown: 0

Binding Revocation ACK Discarded:

Total: 0

Session Not Found: 0 Badly Formed Request: 0

Decode Error: 0 Checksum Error: 0

Invalid Message Type: 0 HAMGR Not Ready: 0

Matching Request Not Found: 0 Invalid Buffer Length: 0

Tunnel Data Received:

Total Packets: 10

6in6: 0 4in6: 0

IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 10

Total Bytes: 1280

6in6: 0 4in6: 0

IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 1280

Errors:

Protocol Type Error: 0 Invalid Pkt Length: 0

No Session Found: 0

Tunnel Data Sent:

Total Packets: 10

6in6: 0 4in6: 0
```

```

IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 10
Total Bytes: 1760
6in6: 0 4in6: 0
IPv6 GRE(IPv4): 0 IPv6 GRE(IPv6): 1760
Tunnel ICMPV6 Packets:
Packet Too Bigs Rcvd: 0 Packet Too Bigs Dropped:0
Packet Too Bigs Relayed: 0
Total Disconnects: 6
Lifetime expiry: 0 Deregistrations: 1
Admin Drops: 0 Other Reasons: 5

```

Monitoring Global Protocols

The mobile-ipv6 option in LMA displays the PMIPv6 control packe

```

ts.MONITOR GLOBAL PROTOCOLS:
11 - SNMP 21 - L2TP (Admin only)
12 - RADIUS Authentication (Admin only) 22 - L2TPMGR (Admin only)
13 - RADIUS Accounting (Admin only) 23 - L2TP Data Admin only)
14 - A11 (R-P Interface) (Admin only) 24 - GTPC (Admin only)
15 - Mobile IPv4 (Admin only) 25 - GTPCMGR (Admin only)
16 - A11MGR (Admin only) 26 - GTPU (Admin only)
17 - PPP (Admin only) 27 - GTPP (Admin only)
18 - A10 (Admin only) 28 - DHCP (Admin only)
19 - User L3 (Admin only) 29 - CDR (Admin only)
31 - RADIUS COA (Admin only) 30 - DHCPV6 (Admin only)
51 - SCTP (Admin only)
32 - MIP Tunnel (Admin only) 52 - M3UA (Admin only)
33 - L3 Tunnel (Admin only) 53 - SCCP (Admin only)
34 - CSS Data (Admin only) 54 - TCAP (Admin only)

```

```

35 - CSS Signaling (Admin only) 55 - MAP Admin only)
36 - EC Diameter (Admin only) 56 - RANAP (Admin only)
37 - SIP (IMS) (Admin only) 57 - GMM (Admin only)
38 - IPsec IKE Only (Admin only) 58 - GPRS-NS (Admin only)
59 - BSSGP (Admin only)
40 - IPsec IKEv2 Only (Admin only)
41 - IPSG RADIUS Signal (Admin only) 61 - SSCOP (Admin only)
42 - ROHC (Admin only) 62 - SSCFNNI (Admin only)
43 - WiMAX R6 (Admin only) 63 - MTP3 (Admin only)
44 - WiMAX Data (Admin only) 64 - LLC (Admin only)
45 - SRP (Admin only) 65 - SMDCP (Admin only)
46 - BCMCS SERV AUTH (Admin only)
47 - RSVP (Admin only)
> 48 - Mobile IPv6 (Admin only)
98 - GSS GCDR (Admin only) 99 - Geog Red (Admin only)
(B)egin Protocol Decoding, (Q)uit, <ESC> Prev Menu

```

Subscriber Configuration

Subscriber configuration support has been added to trigger PMIPv6. The mobility type support bit in the Service-Info attribute is set with this command.

```
[local]st16(config)#
```


```
[local]st16(config)# context asngweap
```

```
[asngweap]st16(config-subscriber)# [no|default] asn-service-info mobility
[ipv4 | ipv6 | ipv6-ipv4]
```


Chapter 6

ASN Gateway Mobile IP Configuration Examples

This chapter provides 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 the *Cisco ASR 5000 Series System Administration Guide*. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in Appendix 1, R_MIP Timer Considerations.

Mobile IP Support Using the System as ASN Gateway/FA

The system supports both Simple and Mobile IP. For Mobile IP applications, you can configure the system to perform the function of an Access Service Network Gateway/Foreign Agent (ASN Gateway/FA) and/or a Home Agent (HA). This example describes what is needed and how the system performs the role of the ASN Gateway/FA. Refer to the *Cisco Series ASR 5000 HA Administration Guide* for information on using the system to provide HA functionality.

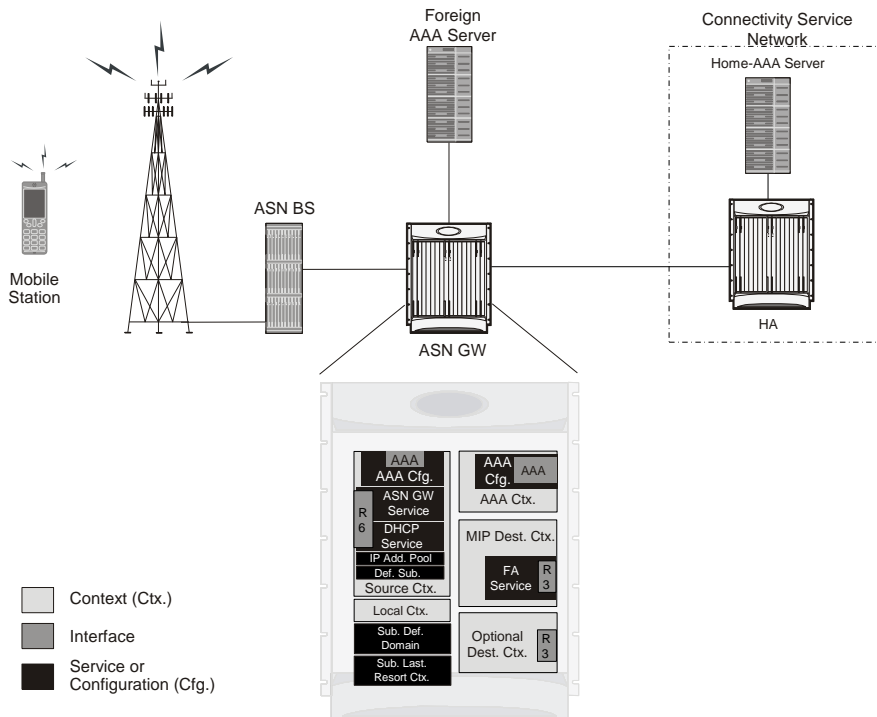
The system's ASN Gateway/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure below.

Important: You must also configure a fourth context that serves as a destination context if Reverse Tunneling is disabled in the FA service configuration. Reverse Tunneling is enabled by default.

The source context facilitates the ASN Gateway service(s), and the R6 interfaces. The AAA context provides foreign AAA functionality for subscriber sessions and facilitates the AAA interfaces. The MIP destination context facilitates the FA service(s) and the R3 interface(s) from the ASN Gateway/FA to the HA.

Use the optional destination context to route data from the mobile node to the connectivity service network by facilitating a CSN (R3) interface. Use this context only if reverse tunneling was disabled.

Figure 43. Mobile IP Support using the system as a ASN Gateway/FA



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 you need to configure the source context.

Table 26. Required Information for Source Context Configuration

Required Information	Description
R6 interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Provide a name for each interface you configure. Configure R6 interfaces in the source context.
IP address and subnet	These are assigned to the R6 interface. Multiple addresses and/or subnets are needed if multiple interfaces are configured.
Physical port number	This specifies the physical port to which the interface is 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 is recognized by the system. Provide a description for each port you use. Configure physical ports within the source context to bind logical R-P interfaces.
Gateway IP address	Use when configuring static routes from the R6 interface(s) to a specific network.
ASN Gateway service Configuration	
ASN Gateway service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the ASN Gateway service is recognized by the system. Provide a name for each ASN Gateway service you use. Configure ASN Gateway services in the source context.
UDP port number for R6 traffic	Specifies the port used by the ASN Gateway service and the ASN BS for communications. The UDP port number and can be any integer value between 1 and 65535. The default value is 2231.
Authentication method	Specifies how the system handles authentication: using the EAP protocol or not requiring any authentication.
Service Policy Information	Policy to handle unexpected re-entry of MS: Specifies the policy to handle unexpected re-entry of an MS in ASN. Set to allowed or disallowed.

Required Information	Description
	Policy to handle mismatch in MSID and DHCP client hardware address: Specifies the policy to handle mismatch in Mobile Subscriber Identifier (MSID) and DHCP client hardware address (CHADDR). Set to allowed or disallowed.
	Policy to create non-anchor mode session: Specifies the policy to create a non-anchor ASN Gateway session based on the data path registration request. Set to allowed or disallowed.
Setup timeout	Specifies the setup timeout duration in seconds for R6 control packets. Configure the time, expressed in seconds, to any integer between 1 and 100000, or disable the timer to set an infinite lifetime. The default value is 60 seconds.
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. Provide a name for each interface you configure. Configure AAA interfaces in the source context.
IP address and subnet	These are assigned to the AAA interface. Configure multiple addresses and/or subnets if you configure multiple interfaces.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number where the line card resides, 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	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system. Provide a description for each port used. Configure physical ports within the source context to bind logical AAA interfaces.
Gateway IP address	Use to configure static routes from the AAA interface(s) to a specific network.
Mobile IP FA context name	Specifies the name of the context in which the FA service is configured.

AAA Context Configuration

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

Table 27. Required Information for AAA Context Configuration

Required Information	Description
AAA context name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the AAA context is recognized by the system. NOTE: If a separate system is used to provide HA functionality, the AAA context name should match the name of the context in which the AAA functionality is configured on the HA machine.

Required Information	Description
AAA Interface Configuration	
AAA interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Provide a name for each interface you configure. Configure AAA interfaces in the source context.
IP address and subnet	Assigned to the AAA interface. Provide an address and/or subnet for each interface you configure.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number in which the line card resides, 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	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port is recognized by the system. Provide a description for each port you configure. Configure physical ports within the source context to bind logical AAA interfaces.
Gateway IP address	Use to configure static routes from the AAA interface(s) to a specific network.
Foreign RADIUS Server Configuration	
Foreign RADIUS Authentication server	IP Address: Specifies the IP address of the foreign RADIUS authentication server the source context communicates with to provide subscriber authentication functions. Provide an address for each RADIUS server you use. Configure foreign RADIUS authentication servers within the source context. Assign a priority to each server you configure.
	Shared Secret: A string between 1 and 15 alpha and/or numeric characters that specifies the key that is exchanged between the RADIUS authentication server and the source context. Provide a shared secret for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign RADIUS authentication server for communications. The UDP port number is any integer between 1 and 65535. The default value is 1812.
Foreign RADIUS Accounting server	IP Address: Specifies the IP address of the foreign RADIUS accounting server that the source context communicates with to provide subscriber accounting functions. Provide an address for each configured RADIUS servers. Configure foreign RADIUS accounting servers within the source context. Assign a priority to each configured server.
	Shared Secret: A string between 1 and 15 alpha and/or numeric characters that specifies the key exchanged between the RADIUS accounting server and the source context. Provide a shared secret for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign RADIUS Accounting server for communications. The UDP port number is any integer between 1 and 65535. The default value is 1813.

Required Information	Description
RADIUS attribute NAS Identifier	Specifies the name by which the source context is identified in the Access-Request message(s) it sends to the foreign 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. You can optionally configured a secondary address.

Mobile IP Destination Context Configuration

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

Table 28. Required Information for Destination Context Configuration

Required Information	Description
Mobile IP destination context name	An identification string between 1 and 79 alpha and/or numeric characters by which the Mobile IP destination context is 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.
R3 Interface Configuration	
R3 interface name	An identification string between 1 and 79 alpha and/or numeric characters by which the interface is recognized by the system. Provide a name are needed for each interface you configure. Configure R3 interfaces in the destination context.
IP address and subnet	Assigned to the R3 interfaces. Assign an address and/or subnet for each configured interface.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number in which the line card resides, 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	An identification string between 1 and 79 alpha and/or numeric characters by which the physical port is recognized by the system. Provide a description for each port you use. Configure physical ports within the destination context to bind logical R3 interfaces.
Gateway IP address(es)	Use to configuring static routes from the R3 interfaces to a specific network.
FA Service Configuration	
FA service name	An identification string between 1 and 63 alpha and/or numeric characters by which the FA service is recognized by the system. Provide a name for each FA services used. Configure FA services 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 is any integer between 1 and 65535. The default value is 434.

Required Information	Description
Security Parameter Index (indices) Information	HA IP address: Specifies the IP address of the HAs with which the FA service communicates. Use the FA service to create a security profile to associate with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. Configure The SPI to be integer between 256 and 4294967295. Configure an SPI if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. Configure The secret to be between 1 and 127 alpha and/or numeric characters. Configure an SPI secret for each configure SPI.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. Configure one of the following algorithms: MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. Configure a hash-algorithm for each configured SPI.
FA agent advertisement lifetime	Specify the time in seconds that an FA agent advertisement remains valid in the absence of further advertisements. Configure the time to be an integer 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 allows during call setup before it rejects the session. Configure an integer between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. Express lifetime in seconds to an integer between 1 and 65534. To configure an infinite registration lifetime, disable the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service waits for a Registration Reply from an HA. Configure the time in seconds to an integer between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that are 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 handles authentication for mobile node re-registrations. Configure the FA service to always require authentication or not. If not, the initial registration and de-registration is still handled normally.

System-Level AAA Parameter Configuration

The following table lists the information required to configure the system's system-level AAA parameters.

Table 29. 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 is 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 is 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, whether the username or domain is specified first, and the character that separates them. The separator characters are: <ul style="list-style-type: none"> • @ • % • - • \ • # • / Specify up to six username formats. The default is username @. NOTE: The username string is searched from right to left for the separator character. If there are one or more separator characters in the string, only the first recognized character is considered the actual separator. For example, if you use the default username format, for the username string user1@enterprise@isp1, the system resolves to the username user1@enterprise with domain isp1.

Optional Destination Context

The following table lists the information required to configure the optional destination context. As discussed previously, This context is required if access control lists (ACLs) are used.



Important: If you use ACLs, the destination context consists only of the ACL configuration. Interface configuration is not required.

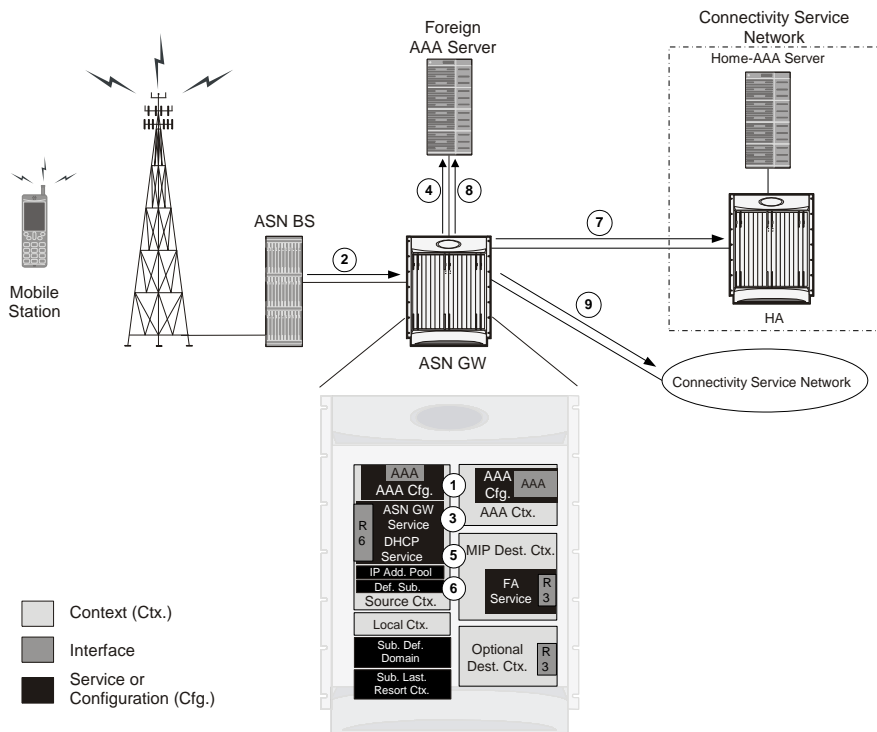
Table 30. Required Information for Destination Context Configuration

Required Information	Description
----------------------	-------------

Required Information	Description
Destination context name	An identification string between 1 and 79 alpha and/or numeric characters by which the destination context is recognized by the system. NOTE: For this configuration, the destination context name should not match the domain name of a specific domain.
CSN (R3) Interface Configuration	
CSN interface name	An identification string between 1 and 79 alpha and/or numeric characters by which the interface is recognized by the system. Configure a name for each configured interface. Configure CSN (R3) interfaces in the destination context.
IP address and subnet	Assigned to the CSN (R3) interface. Assign an address or subnet to each configured interface.
Physical port number	Specifies the physical port to which the interface is bound. Ports are identified by the chassis slot number in which the line card resides, 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	An identification string between 1 and 79 alpha and/or numeric characters by which the physical port is recognized by the system. Configure a description for each port you use. Configure physical ports within the destination context to bind logical CSN (R3) interfaces.
Gateway IP address(es)	Used when configuring static routes from the CSN (R3) interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name between 1 and 31 alpha and/or numeric characters. Case sensitive. Configure IP address pools 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 then consists of every possible address within the subnet, or all addresses from the starting address to the ending address. Configure the pool as public, private, or static.

How This Configuration Works

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

Figure 44. Call Processing When Using the system as an ASN Gateway/FA

Step 1 The system-level AAA settings are configured as follows:

- Subscriber default domain name = AAA context
- Subscriber username format = username @
- Subscriber last-resort context name = AAA context

Step 2 A subscriber session from the BS is received by the ASN Gateway service over the R6 interface.

Step 3 The ASN Gateway service determines which context to use to provide foreign AAA functionality for the session. This process is described in the How the System Selects Contexts section of ASN Gateway Service Operation and Configuration chapter of this reference.

For this example, the result of this process is that ASN Gateway service determined that foreign AAA functionality should be provided by the AAA context.

Step 4 The system then communicates with the foreign AAA server specified in the AAA context's AAA configuration to authenticate the subscriber.

Step 5 Upon successful authentication, the ASN Gateway service determines the IP address of the subscriber's HA using either an attribute returned in the Access Accept message, or the address specified by the mobile.

The ASN Gateway service uses the Mobile IP FA context name to determine what destination context is facilitating the FA service. In this example, it determines that it must use the MIP Destination context.

Step 6 The ASN Gateway service passes the HA IP address to the FA service.

Step 7 The FA service then establishes a connection to the specified HA over the Pi interface.

- Step 8** Accounting messages for the session are sent to the Foreign AAA server over the AAA interface.
- Step 9** If reverse tunneling is disabled, the subscriber data traffic is routed over the CSN interface configured in the Optional Destination context.

Chapter 7

ASN Gateway Service Configuration Examples

This chapter provides configuration information for the ASN Gateway and ASN Paging Controller and Location Registry service.



Important: For information about commands in this chapter, refer to the Command Line Interface Reference. Not all commands are available on all platforms.

The system uses a variety of parameters to perform in various wireless network environments. This chapter discusses the minimum set of parameters to make the system operational. For optional configuration commands specific to the WiMAX product, refer to *Cisco Systems ASR 5000 Command Line Interface Reference*.

This chapter contains the following procedures:

- [Overview of Standalone ASN Gateway Configuration](#)
- [Configuring ASN Gateway_FA Service](#)
- [Configuring Bulk Statistics Schema](#)
- [Managing Your Configuration](#)
- [Gathering ASN Gateway Statistics](#)

Overview of Standalone ASN Gateway Configuration

This section provides an overview of the procedures and examples for configuring the system to perform as an ASN Gateway in a test environment. Each of

- Set initial configuration parameters such as activating processing cards and creating the VPN context. Apply the example configurations in the *Initial Configuration* section of this chapter.
- Configure the system to perform as an ASN Gateway and set basic ASN Gateway parameters such as service configuration, session limits, subscriber limits, network entry, service policy, paging and location register, and session template. Apply the example configurations in the *ASN Gateway Configuration* section.
- Optional. Configure QoS and Service Profile parameters for ASN Gateway service. Apply the example configurations presented in the *ASN Gateway QoS and Service Flow Configuration* chapter.
- Add basic subscribers to the system by applying the example configuration in the *Subscriber Configuration* section.
- Optional. Configure Multi Host support for multiple hosts behind a WiMAX CPE for SOHO subscribers. Apply the example configurations presented in the *Multi IP Host Configuration* section.
- Optional. Configure ASN Gateway service to monitor all BSs associated with it. Apply the example configurations presented in the *BS Monitoring Configuration* section.



Important: Note that BS Monitoring is a license-enabled feature. You need separate feature licenses to use this.

- Optional. Configure log system activity. Apply the example configuration in the *ASN Gateway Logging Configuration* section of this chapter.
- Save the configuration by applying the example configuration in the *Save the Configuration* section of this chapter.

Initial Configuration

Only EAP-AKA authentication is supported in this release.

Step 1 Specify the role of the processing cards in the chassis. The following example configuration activates a PSC.

```
configure
    card < slot_number >
        redundancy card-mode
    exit
    card < slot_number >
```

```

mode active psc

end

```

- Step 2** Set local system management parameters. The following example sets the default subscriber and RADIUS group in the local context:

```

configure

context local

interface <interface_name>

ip address < ip_address | ip_mask >

exit

server ftpd

exit

server telnetd

exit

subscriber default

exit

aaa group default

exit

administrator name < admin_name >

password < password >

ftp

ip route < ip_address > | ip_mask > < next_hop_addr > <
ctx_intf_name >

exit

port ethernet < slot_number > < port_number >

no shutdown

bind interface < ctx_intf_name > local

end

```

- Step 3** Create the context where the service will reside. The following example creates the VPN context and interface and binds the VPN interface to a configured Ethernet port.

```

configure

  context < vpn_context_name > -noconfirm

    interface < vpn_intf_name >

      ip address address

      exit

    port ethernet < slot_number > | < port_number >

      no shutdown

      bind interface < vpn_intf_name > | < vpn_context_name >

    end

```

- Step 4** Create the service within the newly created context. The following configuration example creates the ASN Gateway service:

```

configure

  context < context_name >

    asngw-service < service_name >

  end

```

- Step 5** Configure the system to support Diameter functions such as EAP authentication and flow-based accounting. Refer to the following configuration example.

```

configure

  context <context_name>

    aaa group default

      radius attribute nas-ip-address address <ip_address>

      radius attribute nas-identifier starent

      diameter authentication dictionary aaa-custom1

      diameter accounting dictionary aaa-custom1

      diameter authentication endpoint <endpoint_name>

      diameter accounting endpoint <endpoint_name>

    end

```

ASN Gateway Configuration

Step 1 Set the system's role as an ASN Gateway server. Refer to the following configuration example:

```
configure
  context <context_name>
    asngw-service <service_name>
      bind address < ip_address > [ max-subscribers < max_subs > ]
    end
```

Step 2 Set ASN Gateway service parameters. The following example modifies the configuration of the ASN Gateway service:

```
configure
  context <context_name>
    asngw-service <service_name>
      authentication { single-eap | none }
    end
```

Optional: If you are using Diameter EAP for authentication, add the **policy asngw-initiated-reauth allow** command to the asngw-service mode above.

Step 3 Configure the default communication port and R6 connection setup parameters. The following example modifies the connection setup parameters for the ASN Gateway service:

```
configure
  context <context_name>
    asngw-service <service_name>
      ip local-port < port >
      max-retransmission < retransmission_count >
      retransmission-timout < timeout_duration >
      setup-timeout < timeout_duration >
      tid-seed < transaction_identifier >
```

```
end
```

Step 4 Configure communication with ASN service policy and network entry behavior. The following example configures ASN Gateway service behavior and network entry control:

```
context <context_name>

    asngw-service <service_name>

        policy { ms-unexpected-network-reentry | msid-dhcp-chaddr-
mismatch | transaction-id-validation | non-anchor-mode | zero-function-
type }

end
```

Subscriber Configuration

The following example configures individual local subscribers for ASN Gateway service:

```
configure
context <context_name>

    subscriber name <subscriber_name>

        password password
    exit

    subscriber name <subscriber_name>

        password password
    exit

    subscriber name <subscriber_name>

        password password
    exit

end
```

Optionally, you can configure the default subscriber to support Diameter Flow-based Accounting:

```
configure

    context <context_name>
```



```
subscriber default

  ip context-name <destination_context_name>

  ip access-group <acl_in_name>

  ip access-group <acl_out_name>

  mobile-ip home-agent <ip_address>

  radius accounting mode access-flow-based all-flows

  accounting-mode flow-based

end
```

Multi IP Host Configuration

The following example configures multiple hosts behind a WiMAX CPE for SOHO subscribers:

```
conf

  context <context_name>

    asngw-service <svc_name>

      secondary-ip-hosts <max_hosts>

    exit

  subscriber name <subscriber_name>

    ip address secondary-pool <aux_pool_name>

  end
```

BS Monitoring Configuration

The following example configures multiple hosts behind a WiMAX CPE for SOHO subscribers:

```
conf

  context <context_name>

    asngw-service <svc_name>

      bs-monitor interval <probing_interval>
```

```
bs-monitor num-retry <no_of_retries>

bs-monitor timeout <timeout_dur>

end
```

ASN Gateway Logging Configuration

The following example configures logging for the ASN Gateway add ASN PC/LR services:

```
logging active

logging filter active facility vpn level debug
logging filter active facility sessctrl level debug
logging filter active facility sessmgr level debug
logging filter active facility asngwmgr level debug
logging filter active facility asnpcmgr level debug
logging filter active facility wimax-r6 level debug
```

Configuring ASN Gateway/FA Service

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an ASN Gateway/FA with Mobile IP support in a test environment. For a more robust configuration example, refer Sample Configuration.

To configure the system to perform as an ASN HA:

- Set initial configuration parameters such as activating PACs or PSCs/PSC2s and creating the ingress and egress VPN contexts by applying the example configurations found in the *Initial Configuration* section of this chapter.
- Optional. Configure addition parameters to the ASN Gateway service by applying the example configurations presented in *ASN Gateway Configuration* section.
- Add basic subscribers to the system by applying the example configuration found in the *Subscriber Configuration* section.
- Create the FA service and associate the ASN Gateway service to FA context and Mobile IP by applying the example configuration found in the *Configuring the FA Service* section.
- Optional. Configure log system activity by applying the example configuration found in the *ASN Gateway Logging Configuration* section of this chapter.
- Save the configuration by applying the example configuration found in the *Save the Configuration* section of this chapter.

Initial Configuration

- Step 1** Specify the role of the processing cards in the chassis. The following example activates two PSCs, placing one in active mode and labeling the other as redundant:

```
configure
  card <slot_number>
    redundancy card-mode
  exit
  card <slot_number>
    mode active { pac | psc }
  end
```

- Step 2** Set local system management parameters. The following example sets the default subscriber and RADIUS group in the local context:

```

configure
  context local
    interface < interface name >
      ip address < ip_address > | < ip_mask >
      server ftpd
    exit
    telnetid
  exit      telnetid
  exit      telnetid
  exit      administrator name
    < admin_name > password < password > ftp ip route
    < ip_address > | < ip_mask > < next_hop_addr > < ctx_intf_name >      exit
port ethernet    < slot_number > | < port_number >
  no shutdown
  bind interface < ctx_intf_name > local
  exit
end

```

Step 3 Create the VPN context and interface that binds the VPN interface to a configured Ethernet port. Refer to the following example.

```

configure
  context < vpn_context_name > -noconfirm
    interface < vpn_intf_name >
      ip address < address >
    exit
  port ethernet < slot_number > | < port_number >
    no shutdown
    bind interface < vpn_intf_name > <
vpn_context_name >
  end

```

- Step 4** Create the context where the service will reside. The following example creates the ingress and egress VPN contexts and interfaces and sets the egress context's IP pool. This configuration also binds the VPN interface to a configured Ethernet port.

```

configure
  context <vpn_context_name> -noconfirm
    interface <vpn_intf_name>
      ip address <ip_address> | <ip_mask>
      exit
      dhcp-service <dhcp_svc_name>
        bind address <ip_address>
      exit
    subscriber default
      exit
      ip route 0.0.0.0.0.0.0.0 <next_hop_address> <
ingress_vpn_intf_name>
      exit
      port ethernet <slot_number> | <port_number>
      no shutdown      bind interface <ingress_intf_name> <
ingress_context_name>
      exit    context <egress_context_name>
      ip pool <ip_address> | <ip_mask>
      static interface <slot_number> | <port_number>
      ip address <ip_address> | <ip_mask>
      exit      interface <interface_name>
      ip address <ip_address>
      exit      ip route 0.0.0.0.0.0.0.0
<next_hop_address> <egress_vpn_intf_name>
      exit    port ethernet <slot_number> | <port_number>
      no shutdown      bind interface <egress_intf_name> <
egress_context_name>

```

```
end
```

Step 5 Create the service within the newly created context. The following configuration example creates the ASN Gateway service:

```
configure
  context < ingress_context_name >
    asngw-service < service_name> -noconfirm
      authentication { none | single-eap | double-eap }
    bind address < ingress_ctx_ip_addr >
  end
```

Configuring the FA Service

This section provides basic configuration examples to create and configure an FA service and to associate ASN Gateway service with it.

Step 1 Configure basic Home Agent parameters. The following configuration example creates the FA service:

```
configure
  context <ingress_context_name>
    subscriber name <name>
      password <password>
      ip context-name <egress_context_name>
    exit
  subscriber default
    exit
  fa-service <service_name>
    fa-ha-spi remote-address <ha_address>/<mask> spi-number
    <spi_num> secret <secret_key> hash-algorithm md5
    authentication mn-ha allow-noauth
    authentication aaa-distributed-mip-keys override
```

```
proxy-mip allow

revocation enable          revocation negotiate-i-bit

bind address <fa_context_ip_addr>

end
```



Important: For additional FA Service commands, refer to Command Line Interface Reference. Not all commands are available on all platforms.

- Step 2** Create the service within the newly created context. The following example modifies the configuration of the ASN Gateway service for FA and Mobile IP:

```
configure

context <context_name >

    asngw-service <service_name >


        mobile-ip foreign-agent context < fa_context_name >

end
```

Configuring Bulk Statistics Schema

The following example enables the bulk statistics schema for the AS NGW service on a chassis:

```
configure
  bulktats mode
    context schema <asngw-service> format <format_string>
  end
```

 **Important:** To configure the various parameters for the Bulk Statistics collection, refer to Configuring and Maintaining Bulk Statistics chapter in System Administration Guide prior to configuring these commands.

For more information on *format_string* variable, refer Bulk Statistics Configuration Mode Commands chapter in Command Line Interface Reference.

Save the Configuration

To save changes made to the system configuration for this service, refer Saving Your Configuration chapter.

Managing Your Configuration

This section describes how to display and review the configurations after you save them in a .cfg file as described in Saving Your Configuration chapter of this guide. Refer to the following table for commands to retrieve errors and warnings within an active configuration for a service.



Important: All commands listed here are under Exec mode. Not all commands are available on all platforms.

Output descriptions for most of the commands are located in Command Line Interface Reference.

Table 31. System Status and ASN Gateway Service Monitoring Commands

To do this:	Enter this command:
View Administrative Information	
Display Current Administrative User Access	
View a list of all administrative users currently logged on to the system	<code>show administrators</code>
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	<code>show administrators session id</code>
View information pertaining to local-user administrative accounts configured for the system	<code>show local-user verbose</code>
View statistics for local-user administrative accounts	<code>show local-user statistics verbose</code>
View information pertaining to your CLI session	<code>show cli</code>
Determine the System's Uptime	
View the system's uptime (time since last reboot)	<code>show system uptime</code>
View the Status of Configured NTP Servers	
View the status of the configured NTP servers	<code>show ntp status</code>
View the Status of System Alarms	
View the Status of System Alarms	
View the status of the system's outstanding alarms	<code>show alarm outstanding all</code>
View detailed information about all currently outstanding alarms	<code>show alarm outstanding all verbose</code>
View system alarm statistics	<code>show alarm statistics</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	

To do this:	Enter this command:
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View information for a specific subscriber	<code>show subscribers full username username</code>
View the ASN Gateway Related Information	
Display System Configuration	
View the configuration of a context	<code>show configuration context <i>name</i></code>
View configuration errors for ASN Gateway service	<code>show configuration errors section asngw-service [verbose] [{grep <i>grep_options</i> more}]</code>
Display Service Configurations	
View ASN Gateway service configuration	<code>show configuration grep <i>asngw</i></code>
View service association with subscriber	<code>show subscriber all grep <i>asngw</i></code>
View complete ASN Gateway service statistics	<code>show asngw-service statistics</code>
View all ASN Gateway services	<code>show asngw-service all</code>
View specific ASN Gateway service statistics	<code>show asngw-service <i>service_name</i></code>
Display ASN Gateway session	
View all active ASN Gateway subscriber session	<code>show asngw-service session full</code>
View all ASN Gateway data path counters	<code>show asngw-service session counters function-type data-path</code>
View ASN Gateway peer statistics	<code>show asngw-service session peer-address</code>
View all ASN Gateway MS state change statistics	<code>show asngw-service statistics function-type ms-state-change</code>
View all DHCP statistics for an MSID	<code>show dhcp full msid <i>msid_num</i></code>
View all DHCP statistics for a user name	<code>show dhcp full username <i>user_name</i></code>
View session disconnect reason	<code>show session disconnect-reasons</code>
Display ASN PC session	
View all active ASN PC subscriber session	<code>show asnpc-service session full all</code>
View all ASN PC session counters	<code>show asnpc-service session counters all</code>
View ASN PC statistics	<code>show asnpc-service session statistics verbose</code>

Gathering ASN Gateway Statistics

Use the commands below to gather the statistics for ASN Gateway services.



Important: All commands listed here are under Exec mode. For more information on these commands, refer to the “Executive Mode Commands” chapter in the Command Line Interface Reference.

Table 32. Gathering Statistics

Statistics Wanted	Action to Perform	Information to Look For
Active ASN Gateway service session related statistics on a chassis.	At the Exec Mode prompt, enter the following command: show asngw-service session full	The output of this command displays the statistics about the ASN Gateway service session in a system/service.
Detailed disconnect reasons for an ASN Gateway session.	At the Exec Mode prompt, enter the following command: show session disconnect-reasons	The output of this command displays the disconnect reasons ASN Gateway service session in a system/service.
Detailed statistics of AS NGW services.	At the Exec Mode prompt, enter the following command: show asngw-service statistics	The output of this command displays the detailed statistics ASN Gateway service in a system/service.

Chapter 8

ASN Gateway QoS and Service Flow Configuration

This chapter provides information and examples for Quality of Service (QoS) and service flow configuration that support an individual subscriber or a set of subscribers.



Important: This chapter does not discuss the configuration of the local context. Refer to the System Administration Guide.

Introduction

This section provides an introduction to Quality of Service (QoS) and service flow ID management for a subscriber.

Connection-oriented MAC Architecture

Support for QoS is a fundamental part of the WiMAX service. QoS is controlled with a connection-oriented MAC architecture. All downlink and uplink connections are controlled by the serving base station. Before any data transmission occurs, the base station and the mobile station establish a unidirectional logical link, a connection, between the two MAC-layer peers. Each connection is identified by a connection identifier (CID), which serves as a temporary address for data transmissions over the link. In addition to connections for transferring user data, the WiMAX MAC defines three management connections—the basic, primary, and secondary connections. These three management connections are used for such functions as ranging.

WiMAX Service Flow and QoS

WiMAX provides the concept of service flow. A service flow is a unidirectional flow of packets with a set of QoS parameters, identified by a service flow identifier (SFID). The QoS parameters include traffic priority, maximum sustained traffic rate, maximum burst rate, minimum tolerable rate, scheduling type, maximum delay, tolerated jitter, service data unit type and size, bandwidth request mechanism to be used, transmission PDU formation rules, and so on.

You can provision service flows through a network management system or create them dynamically through defined signaling mechanisms. The base station is responsible for issuing the SFID and mapping it to unique CIDs. You can also map service flows to DiffServ code points or MPLS flow labels to enable end-to-end IP-based QoS.

Within a WiMAX ASN, QoS enforcement is administered by the Service Flow Authorization (SFA) component in the ASN Gateway (also referred to as Anchor Policy Charging Enforcement Function, A-PCEF). The SFA component provides traffic management and QoS policy management for subscriber service flows.

With multiflow QoS, static traffic policies are established for various subscriber application-level service flows. It can be used in Simple IP or Mobile IP usage scenarios. The policies are stored in a Subscriber Policy Repository (SPR) database and retrieved as authenticated QoS profiles by the ASN Gateway. The A-PCEF negotiates via R6 with the Service Flow Manager (SFM) function on the base station. If the authorized QoS profile matches the available base station resources, the request is granted. The A-PCEF provides traffic classification, admission control, prioritization (DSCP marking), per-session/per-flow bandwidth control, and flow mapping across application-specific R6/R4 GRE tunnels.

In conjunction with multiflow QoS, the ASN Gateway provides configurable accounting on a per-session, per-R6, or per-service flow basis. Multiflow QoS enables the separation of OFDM radio access connection into multiple logical Connection IDs (CIDs), with each pair of forward and reverse sub-channels transporting one or more application flows.

The ASN Gateway supports static pre-provisioned service flows. A total of up to six bi-directional service flows per subscriber R6 or R4 session are possible.

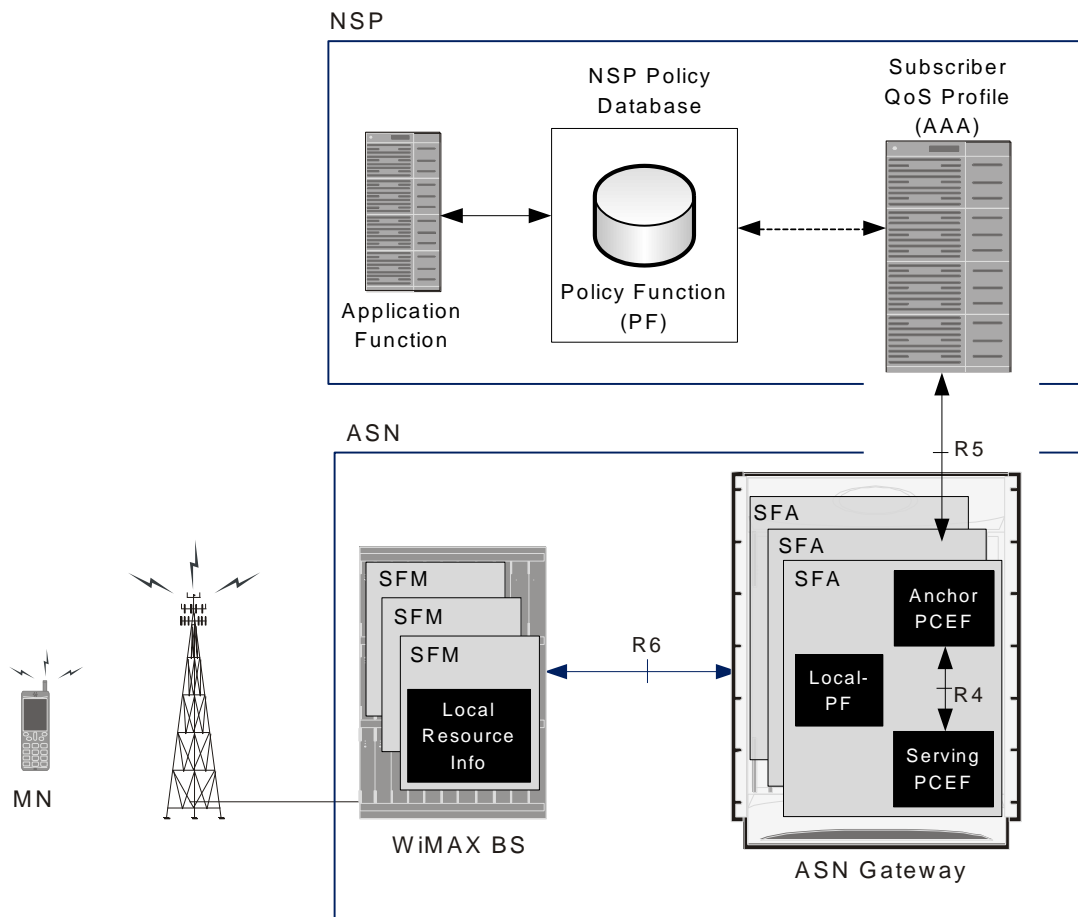
Multi-Flow QoS provides an enhanced user experience via end-to-end differentiated QoS connection-oriented services for isochronous voice and delay-sensitive multimedia applications over broadband wireless WiMAX networks. This feature also enables service convergence and provides the foundation for IMS service control.

The QoS implementation provides following supports:

- Connection-oriented service
- Data delivery services at the air interface
- QoS parameter provision for each subscriber
- Policy requirement for admitting new service flow requests

The following figure provides the high-level view of QoS functional model in WiMAX networks.

Figure 45. WiMAX QoS Functional Model



- **Policy Function:** The Policy Function (PF) and its policy database resides in NSP and maintains general policy rules as well as application-dependent policy rules. You can configure the local PF at the ASN Gateway with SFA. Additionally, AAA may provision the PF database with the user's QoS profile and associated policies. The PF evaluates service requests against these policies.
- **AAA Server:** The AAA server holds the subscriber's QoS profile and associated policy rules. The profiles and associated policy rules can be handled in one of two ways:
 - Downloaded to the SFA at network entry as part of the authentication and authorization procedure. The SFA evaluates the coming service request against the subscriber profile.

- Provisioned in the home PF.
- **Service Flow Management (SFM):** This is a logical entity in the ASN. The SFM entity creates, admits, activates, modifies, and deletes WiMAX service flows. It consists of an Admission Control (AC) function and associated local resource information. The AC determines whether a new service flow can be admitted based on existing radio and other local resource usage. The SFM entity is always located in the base station.

The SFM provides:

- Pre-provisioned service flow creation, modification, and deletion
- Initial service flow creation, modification, deletion
- MS mobility management
- **Service Flow Authorization (SFA):** This is a logical entity in the ASN. When a subscriber QoS profile is downloaded from the AAA into the SFA at the network entry phase, the SFA evaluates the service requests against the user's QoS profile. For a given ASN/NAP, an anchor SFA is assigned to each MS. The anchor SFA does not change for the duration of the MS authentication session. Optionally, there may be one or more additional SFA entities that relay QoS-related primitives and apply QoS policy for that MS. The relay SFA that communicates directly with the SFM is called the serving SFA. When there are no relays, the anchor SFA is also the serving SFA. The identity of the serving SFA, if different from the anchor, is known by the anchor SFA at all times. Similarly, the serving SFA knows the identity of the anchor SFA. The anchor and/or serving SFA perform ASN-level policy enforcement through a local policy database and an associated local policy function (LPF). The LPF enforces admission control based on available resources.

The provisioning of service flows is done by a network management system.

WiMAX QoS Parameters and Functions

This section describes the functional parameters you need for QoS and service flow configuration at the ASN Gateway level.

QoS Parameters

The QoS parameter set is required for service flows with service classes. The QoS parameter set is a group that consists of the maximum sustained data rate, committed data rate, maximum latency, maximum traffic burst, allowable jitter, and priority of traffic for a subscriber.

- **Committed data rate:** The minimum data rate committed for a subscriber data flow. The data rate is measured in bits per second in an average over time. If a user transmits data up to the committed data rate, the guarantee of throughput, latency, and jitter is maintained.
- **Maximum sustained data rate:** The maximum bandwidth allowed for a subscriber data flow. This data rate is maintained as Best-Effort (BE) service. If the user increases the data rate beyond this rate, service is not allowed.
- **Allowable jitter:** The maximum delay variation allowed for the connection.
- **Maximum traffic burst:** The burst size, in bytes, of the service flow.
- **Maximum latency:** The maximum duration of time required to retrieve the information over network interface by the system.
- **Traffic Priority:** The priority of service flow. If two service flows with the same QoS parameters are defined, the set traffic priority it considered.

Service Class

The service class consists of the QoS parameter set and is defined at the base station or ASN Gateway. Configure the service class to define each QoS parameter of service flow for different sets of subscriber.

You can explicitly define each QoS parameter for service flow in WiMAX QoS implementations, or may indirectly use a service class which defines the QoS parameter set. Service class is associated with service flow through the QoS descriptor and named as Service Class Name and Global Service Class Name.

- **Service Class Name:** A group of QoS parameters defined at the base station. The parameters are referenced by a service flow to apply certain QoS parameters for an individual or a set of subscribers.
- **Global Service Class Name:** Similar in function to the Service Class Name except that the Global Service Class Name may not be modified by a base station and remains consistent among all base stations. The Global Service Class Names is a rules-based naming system and contains referential QoS parameter codes for an individual or a set of subscribers.

To support a wide variety of applications, ASN Gateway service supports the following QoS services. These services are configured at the ASN Gateway service-level and supported by the base station MAC scheduler for data transport over a connection:

- **Unsolicited grant services (UGS):** Supports fixed-size data packets at a constant bit rate (CBR). Examples of applications that may use this service are T1/E1 emulation and VoIP without silence suppression. The mandatory service flow parameters that define this service are maximum sustained traffic rate, maximum latency, tolerated jitter, and request/transmission policy.
- **Real-time polling services (rtPS):** Supports real-time service flows such as video that generate variable-size data packets on a periodic basis. The mandatory service flow parameters that define this service are minimum reserved traffic rate, maximum sustained traffic rate, maximum latency, and request/transmission policy.
- **Non-real-time polling service (nrtPS):** This service supports delay-tolerant data streams, such as an FTP, that require variable-size data grants at a minimum guaranteed rate. The mandatory service flow parameters to define this service are minimum reserved traffic rate, maximum sustained traffic rate, traffic priority, and request/transmission policy.
- **Best-effort (BE) service:** Supports data streams, such as Web browsing, that do not require a minimum service-level guarantee. The mandatory service flow parameters to define this service are maximum sustained traffic rate, traffic priority, and request/transmission policy.
- **Extended real-time variable rate (ERT-VR) service:** Supports real-time applications, such as VoIP with silence suppression, that have variable data rates but require guaranteed data rate and delay. This is also referred to as extended real-time polling service (ErtPS).

The following table lists the supported type of QoS services and its use for typical applications.

Table 33. QoS Services and its Application

QoS Service	Description	Typical Applications
Unsolicited grant services (UGS)	Real-time data streams comprising fixed-size data packets issued at periodic intervals.	T1/E1 transport
Real-time polling services (rtPS)	Real-time data streams comprising variable-sized data packets that are issued at periodic intervals.	Video
Non-real-time polling service (nrtPS)	Delay-tolerant data streams comprising variable-sized data packets for which minimum data rate is required.	FTP with guaranteed minimum throughput
Best-effort (BE) service	Data streams for which no minimum service level is required and therefore may be handled on a space-available basis.	HTTP
Extended real-time variable rate (ERT-VR) service/ Extended real-time Polling service (ErtPS)	Real-time service flows that generate variable-sized data packets on a periodic basis.	VoIP

Service Flow

Service flow is a transport service that delivers packets and has a defined QoS parameter set that provides QoS to those packets. It is a unidirectional flow for traffic toward the subscriber or system. Service flow has a 32 bit identifier known as Service Flow ID (SFID). One service flow can be used by many packets.

There are three types of service flows, including provisioned service flows, admitted service flows, and active service flows.

- **Pre-Provisioned Service Flow:** A service flow that is provisioned but not immediately activated. This service flow can be created, admitted, and activated by default after a subscriber registers with the WiMAX network and before any IP data begins flowing. This is the minimum capability that occurs before IP address assignment via DHCP/MIP.

After successful MS registration with the WiMAX network, an anchor SFA is assigned and its location is updated with the associated PF entity. If the subscriber profile is downloaded from an AAA server during the authentication procedure of the network entry, the SFA initiates the creation, admission, and activation of the pre-provisioned service flow.

If the subscriber's QoS profile has not been downloaded from the AAA, it is the PD or the Local-PF that initiates the creation and activation of pre-provisioned service flow.

External triggers transition a provisioned service flow to an admitted service flow. This service flow is initiated when an MS enters the network through a network entry procedure. Provisioned service flow is managed by the NMS at the BS.

Either the base station or the mobile station can use the Dynamic Service Change (DSC) message to change a provisioned service flow to the admitted service flow or active service flow. In the case of the BS, the BS maps the SFID to CID and sends it to the MS in a DSC-REQ message if the DSC message is initiated the BS. The BS send a DSC-RSP message to MSs if DSC message is initiated by an MS.

- **Admitted Service Flow:** A network resource is reserved through admission control. External triggers transition an admitted service flow to an active service flow. Application triggers may effect the transition to an active service flow.

You can create an admitted service flow at the ASN Gateway with two types of authorization models: provisioned authorization model and dynamic authorization model. The QoS parameter set of admitted service flow should be a subset of provisioned service flow. For more information on service flow authorization, refer Service Flow Authorization.

- **Active Service Flow:** An active service flow that is granted uplink and downlink bandwidth for data transport. It employs an active QoS parameter set that is a subset of the Admitted QoS parameter set.

You can create active service flows at the ASN Gateway with a provisioned authorization model or dynamic authorization model. The QoS parameter set of active service flow should be a subset of admitted service flow. For more information on service flow authorization, refer Service Flow Authorization.

The service flow can contain optional parameters, depending on its type of service flow. It contains Connection Id (CID) for admitted or active service flows. Use the AdmittedQoSParameterSet parameter for admitted service flow and ActiveQoSParameterSet parameter for active service flow. For a provisioned service flow, use the ProvisionedQoSParameterSet parameter.

Each data packet has an associated service flow with exactly one SFID as parameter. If it contains a service class name, the QoS parameter set service flow is defined in the service class. For the admitted service flow and active service flow, it may contain CID as parameter.

Each connection has one associated service flow which contains a 16-bit Connection ID and QoS parameter set.

Similarly each service class has one associated service flow containing the Service Class Name as an identifier and a parameter called QoS parameter set.

Service Flow Authorization (SFA)

The ASN Gateway uses an authorization module to accept or deny any new service flow, modified QoS parameter set of service flow, or change of service flow type. Service Flow Authorization supports two types of authorization models:

- Provisioned (static) authorization
- Dynamic authorization

Provisioned Authorization Model

In the provisioned authorization model, ASN Gateway keeps all the provisioned QoS parameter sets of service flow. When the base station uses the DSC message to admit service flow or to activate service flow, the authorization module ensures that it is the subset of provisioned service flow in the first phase and the subset of admitted service flow in second phase. The MS is not allowed to create provisioned service flow.

Provision service flows at the base station with an NMS. The base station configures and registers service flows through the Service Flow Management (SFM) module and assigns SFID to it. The base station sends service flows to the MS through DSA-REQ. The MS sends DSA-RSP after accepting it, and the base station sends DSA-ACK to complete the transaction.

Subscriber Policy and QoS Profile

The subscriber policy consists of:

- Subscriber QoS profile information accessible to the SFA function.
- Local policy information (Local-PF) available to the SFA function.
- Admission control policies accessible to the SFM function.

Subscriber QoS Profile

The subscriber QoS profile is a per-subscriber basis parameter. The subscriber is identified by the network access identifier (NAI) which is included by the NAS in the AAA messages to the HAAA. For each subscriber, the QoS profile includes the permissible number and schedule type of WiMAX service flow and permissible range of values for associated QoS parameters.

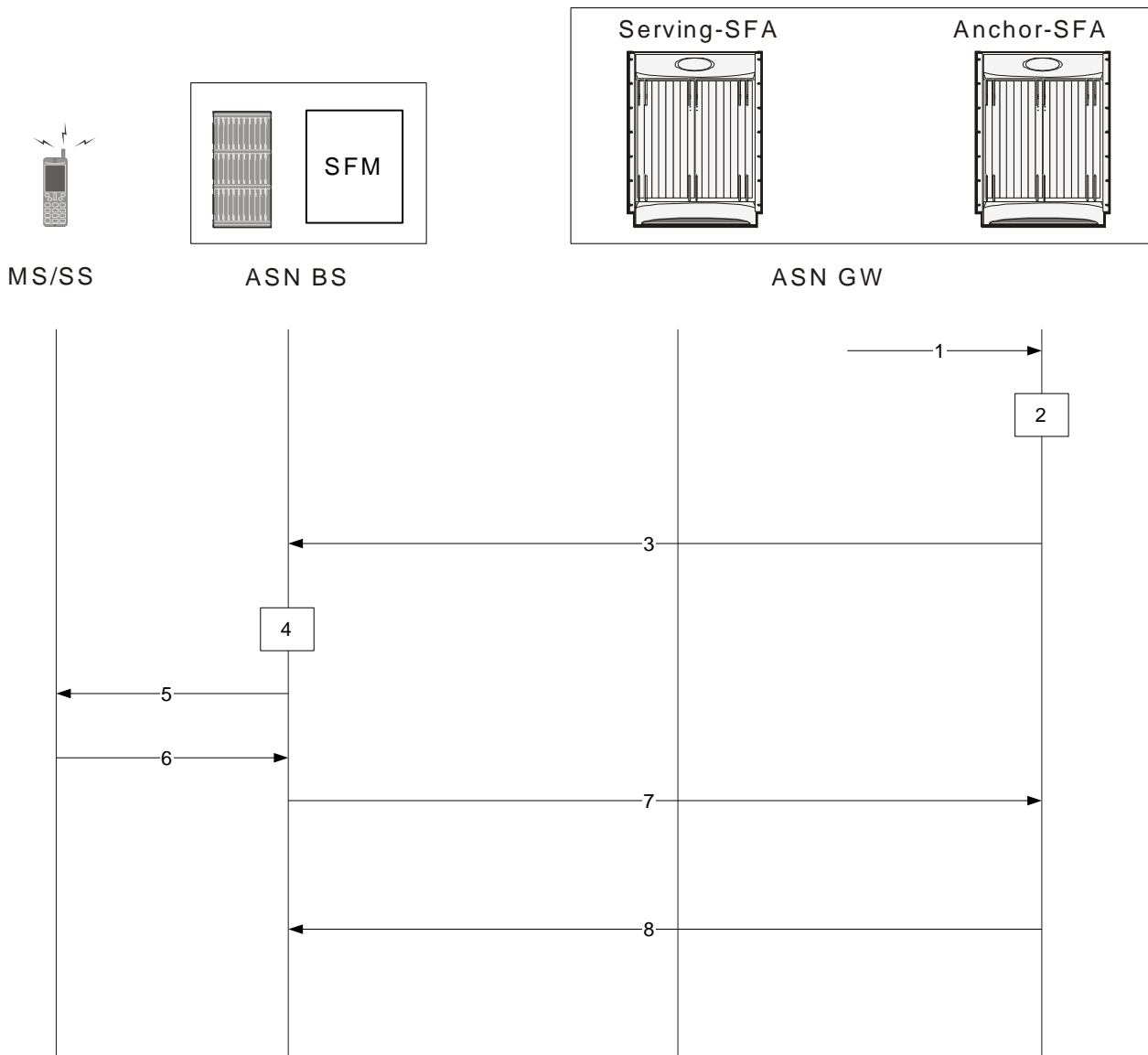
The QoS profile and associated policy rules are downloaded to the Anchor SFA through AAA-Client after user authentication and network entry.

QoS Message Flow

This section service flow creation and deletion is illustrated with updating of the SFA location.

Pre-provisioned Service Flow

This procedure is initiated by the anchor service flow authorization (SFA) after the completion of MS registration. The following figure shows the call flow procedure used by the anchor SFA to apply the QoS profile and associated policies. These are downloaded from AAA server to identify the pre-provisioned service flows that need to be created, admitted, and activated. The following table describes each step of the call flow.

Figure 46. SFA Triggered Pre-provisioned Service Flow Creation Call Flow**Table 34. SFA Triggered Pre-provisioned Service Flow Creation Call Flow Description**

Step	Description
1	Initial network entry is completed and the anchor SFA receives the QoS profile from the AAA.
2	Received QoS and associated profiles are applied to the subscriber.
3	Anchor-SFA sends Data Path Registration Request, including service flow information, to the Serving-SFA.
3	Serving-SFA sends Data Path Registration Request with service flow and data path information to the Service Flow Management module in ASN base station.
4	ASN base station applies the admission control parameters on the basis of subscriber profile.

Step	Description
5	The SFM (in the base station) verifies the availability of radio resources and decides the action for the request on the basis of QoS Info parameters. In case of acceptance, a Dynamic-Service-Accept Request (DSA-Request) or Dynamic-Service-Change Request (DSC-Request) is sent to the MS.
6	On the basis of request acceptance parameters, the MS accepts or rejects the DSA/DSC request and sends the DSA/DSC response message to SFM in ASN BS.
7	Upon successful response from the MS, the SFM sends a Path Registration Response message to the Serving-SFA to confirm the resource and path reservation. The message contains the granted QoS parameter set for service flow and data path information.
9	On receipt of successful response from the SFM, the Serving-SFA sends a Data Path Registration Response message to the Anchor-SFA to confirm the resource reservation. The response message contains the QoS-Info parameters containing granted QoS values.
8	Serving-SFA sends a Path Registration ACK or Path Modification ACK to the SFM.
11	On receipt of successful Data Path Registration Response message with the QoS-Info parameters containing granted QoS values from Serving-SFA, the Anchor-SFA sends back an Data Path Registration Acknowledgement message to the Serving-SFA. The context is kept until the MS performs network exit.

QoS and Service Flow Configuration

This section describes how to configure the multiple service flow and QoS-related parameters in ASN Gateway.

There are two types of provisioning for providing QoS and associated policies to the SFA.

- AAA Provided Configuration
- AAA Provided Service Profile Id only

AAA Provided Configuration

In this scenario, AAA provides all multiple service flow related QoS configuration during user authentication. AAA provides configuration for a list of service flows that include Packet Data Flow (PDF) identifier, Service Data flow (SDF) identifier, service classifier, and QoS descriptor identifier. AAA also provides the QoS Id to QoS parameter mapping. For the initial service flow, the SDF ID is set to 1.

Following is the list of parameters provided by AAA in this mode:

- Packet data flow identifier (PDF Id)
- Service data flow identifier (SDF Id)
- Uplink and Downlink service classifiers
- QoS descriptor

AAA Provided Service Profile Id

In this mode, AAA provides the Service Profile Id only, which is a pre-configured identifier in the ASN Gateway and contains following parameters:

- Packet data flow identifier (PDF Id)
- Service data flow identifier (SDF Id)
- Service profile Id

The ASN Gateway provides the facility for configuring local subsurface templates with server profile ID/packet data flow ID/service data flow ID for service flows. If the AAA server does not support these attributes, you can configure the local subscriber template to provide QoS to subscriber service.

Configuring the Traffic Class-Map Parameters

The following example configures the traffic the configuration of the ASN Gateway service for Service Profile:

```
configure
```



```

context <context_name>

  class-map name <class_map_name>

    match protocol udp

    match ip-tos <service_value> [ip-tos-mask <mask_value>

    match src-port-range <initial_port_num> [to <last_port_num>

    match dst-port-range <initial_port_num> [to <last_port_num>

    match src-ip-address <src_ip_address> [<subnet_mask>

    match dst-ip-address <dst_ip_address> [<subnet_mask>

  end

```

Configuring QoS Descriptor Table Parameters

The following configuration example modifies the ASN Gateway configuration for QoS Descriptor Table parameters in an ASN Gateway service:

```

configure

context <context_name>

  asn-qos-descriptor id <qos_id> [-noconfirm]


  service-class-name <svc_class_name>

  global-service-class-name <glb_svc_class_name>

  schedule-type {be | et-vr | rt-vr | nrt-vr | ugs}

end

```

 **Important:** For more information on how to configure schedule-type parameters for the QoS descriptor Id, refer to the Command Line Interface Reference.

Configuring the ASN Gateway Service Profile Parameters

The following example modifies the configuration of the ASN Gateway service for Service Profile:

```

configure

context <context_name>

```

```

asn-service-profile id <asn_profile_id> direction {bi-directional |
downlink | uplink} [-noconfirm]

    downlink-classifier class-map <class_map_name>

    downlink-qos-id <qos_table_id>

    uplink-classifier class-map <class_map_name>

    uplink-qos-id <qos_table_id>

end

```

Configuring the Service Flow and Policy Interaction

The following configuration binds dynamic policies to the service flows with the QoS descriptor Id and Service data flow Id.

configure

```

context <context_name>

    policy-map name <policy_name>

        type static | [dynamic {wimax {asn-qos-descriptor {any | id <qos_table_id>
} | asn-sdfid {any | id <sdf_id>} | asn-pdfid {any | id <pdf_id>}}}]

        qos encaps-header dscp-marking [<dscp_code> | copy-from-user-datagram

        qos user-datagram dscp-marking <dscp_code>

        access-control {allow | discard}

        qos traffic-police committed <bps> peak <bps> burst-size <bytes>
exceed-action {drop | lower-ip-precedence | allow} violate-action {drop | lower-
ip-precedence | allow}

    end

```

Applying QoS to Subscriber Template

The following example modifies the configuration for QoS and the Service Profile for a subscriber in the ASN Gateway service:

```

configure context <context_name> subscriber
<subscriber_name>          asn-pdfid <pdf_id> asn-service-profile-id
<svc_profile_id> asn-sdfid <sdf_id>          end

```

Configuring QoS for AAA-provided Service Profile Id

This section provides the configuration example to configure the QoS parameters to match AAA-provided service profile IDs.

These procedures assume that an ASN Gateway server is configured on your system and is ready to use for the ASN Gateway services described in this guide.

1. Configure the traffic classifier with Class-map to be applied to the service profile Id with the PDF Id in the destination context. Apply the example configuration in the *Configuring the Traffic Class-Map Parameters* section.
2. Set the QoS descriptor table identifier by applying the example configuration in the *Configuring QoS Descriptor Table Parameters* section.
3. Set service parameters by applying the example configuration in the *Configuring the ASN Gateway Service Profile Parameters* section.
4. Set service parameters by applying the example configuration in the *Configuring the Service Flow and Policy Interaction* section.
5. Configure the default AoR domain and session redirection by applying the example configuration in the *Applying QoS to Subscriber Template* section.
6. Save your configuration as per procedure described in Saving Your Configuration chapter.

Chapter 9

Service Configuration Procedures

Use this chapter in conjunction with the previous chapters to see examples for configuring the system to support Simple IP services, Mobile IP services, or both. This chapter provides procedures for configuring the elements that 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.

Procedures are provided for the following:

- [Creating Contexts](#)
- [Creating and Configuring Ethernet Interfaces and Ports](#)
- [Creating and Configuring FA Services](#)
- [Creating and Configuring HA Services](#)
- [Session Continuity Support](#)
- [Configuring DHCP-based IP Address Assignment](#)
- [Configuring the Destination Context Attribute](#)
- [Configuring IP Address Pools on the System](#)




Important: Make sure that at least one processing card is active prior to service configuration. Refer to the System Administration Guide for configuration instructions for processing cards.

Creating Contexts

To configure a specific function, such as source, destination, and/or AAA, use the same basic procedure.

This section provides instructions for creating contexts on the system. These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

 **Important:** It is recommended that if your system is using Ethernet 10/100 Line Cards, you configure at least one context per physical port to ensure adequate bandwidth for subscriber sessions.

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

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Create the new context by entering the following command:

```
context < context_name >
```

context_name is the name for the new context you are creating. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Optional. Configure a domain alias, creating a new AAA realm, for the context to apply AAA group. Refer to Configuring System-Level AAA Functionality for more information on domain aliases and AAA realms.

```
domain [*] < name > [default subscriber < subs_temp_name >
```

Keyword/Variable	Description
------------------	-------------

Keyword/Variable	Description
[*]name	The unique AAA realm to match in the domain portion of the subscriber name. Enter this variable as an alpha or alphanumeric string of 1 to 79 characters. If you enter a wildcard (*) as a prefix to the domain name and an exact match is not found for the domain portion of a subscribers username, subdomains of the domain name are matched. For example: if the domain portion of a subscribers username is abc.xyz.com and you use the domain command domain *xyz.com it matches. But if you do not use the wildcard (domain xyz.com) it does not match.
<i>subscriber-template-name</i>	The name of the of the realm-based default subscriber template that contains realm-specific AAA attributes. These attributes are used when a server returns the access-accept message for a user matching the domain alias (realm) without needed attribute values.

Step 4 If you created a realm-based subscriber template in *step 3* of this procedure, the following prompt appears:

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

Now you need to configure the default subscriber.



Important: Note that although you create a realm-based default subscriber template with the domain command, the actual default subscriber for this realm is not created. To complete this step, issue the subscriber name command from the context configuration mode where the AAA realm resides and then configure the required attributes in subscriber configuration mode.

Step 5 Exit the configuration mode by typing:

```
end
```

The following prompt appears:

```
[local] < host_name > #
```

Step 6 Repeat *step 1* through *step 5* to configure additional contexts.

Step 7 Verify that you created the contexts successfully by entering the following command:

```
show context all
```

The output is a two-column table that looks similar to the example below. In this example, it shows that two contexts were created: one called source and one called destination.

Context Name	Context ID	State
-----	-----	-----
local	1	Active

■ Creating Contexts

source	1	Active
destination	1	Active

The left column lists the contexts that are configured. The center column lists the corresponding context ID for each of the configured contexts. The third column lists the current state of the context.

Step 8 Save your configuration as described in Saving Your Configuration.

Step 9 Now that you have created the context, you can create interfaces and specific functionality within the context. Proceed to any of the other sections in this chapter for instructions on configuring specific services and options.

Creating and Configuring Ethernet Interfaces and Ports

To create and configure a Simple and/or Mobile IP data application interface (R4, R6, DHCP, R3, or CSN), you need to do the following:

- Name the interface
- Assign an IP address and subnet mask to the interface
- Assign a physical port for use by the interface
- Bind the port to the interface
- Optionally configure port switchover on L3 connectivity failure

This section provides the minimum instruction set for configuring interfaces and ports to allow the system to communicate on the network. Commands that configure additional interface or port properties are provided in the Ethernet Port Configuration mode and Ethernet Interface Configuration mode chapters of the Command Line Interface Reference.



Caution: To ensure that system line card and port-level redundancy mechanisms function properly, disable the Spanning Tree protocol on devices connected directly to any system port. Failure to turn off the Spanning Tree protocol may result in failures in the redundancy mechanisms or service outage.

This section provides instructions for creating and configuring Ethernet interfaces and ports. These instructions assume that you are at the root prompt for the Exec mode:

```
[local] < host_name > #
```

Step 1 Enter the configuration mode by typing:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config) #
```

Step 2 Enter context configuration mode typing:

```
context context_name
```

context_name is the name of the context in which to create and configure the interface. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the interface by typing the following command:

```
interface interface_name [loopback]
```

Keyword/Variable	Description
interface_name	The name for the interface. The name must be 1 to 79 alpha and/or numeric characters and is case sensitive.
loopback	Use this optional keyword to specify a loopback interface type. If you are using this interface for Interchassis Session Recovery you must specify loopback interface type after the interface_name.

The following prompt appears:

```
[<context_name>] < host_name > (config-if-eth)#
```

Step 4 Enter the following command to configure the IP address and subnet mask used by the interface:

```
ip address < address > subnetmask [secondary]
```

Keyword/Variable	Description
address	The IP address.
subnetmask	The subnet mask.
secondary	Use this optional keyword to assign multiple IP addresses to the interface. Issue the ip address command once without the secondary keyword to assign the primary address to the interface. Re-issue the command with the secondary keyword as many times as necessary to assign additional addresses to the interface.



Important: Assign multiple addresses to the interface if it is being configured to act as an ICC interface that provides a communications path between multiple services configured in the same context.

Step 5 Optional. Configure the interface so that the associated line card port switches over to the port on the redundant line card if connectivity to a specified IP address is lost. Enter the following command:

```
port-switch-on-L3-fail address ip_address [minimum-switchover-period  
switch_time] [interval int_time] [timeout time_out] [num-retry number]
```

Keyword/Variable	Description
ip_address	The IP address to monitor for connectivity. This must be an IPv4 address.

Keyword/Variable	Description
minimum-switchover-period <i>switch_time</i>	Default: 120 seconds After a switchover occurs, another switchover cannot occur until the amount of time specified has elapsed. Enter an integer for <i>switch_time</i> from 1 to 3600.
interval <i>int_time</i>	Default: 60 seconds This specifies how often, in seconds, monitoring packets are sent to the IP address being monitored. Enter an integer for <i>int_time</i> from 1 to 3600.
timeout <i>time_out</i>	Default: 3 seconds Specifies how long to wait without a reply before re-sending monitoring packets to the IP address being monitored. Enter an integer for <i>time_out</i> from 1 to 10.
num-retry <i>number</i>	Default: 5 This value specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover operation. Enter an integer for <i>number</i> from 1 to 100.

Step 6 Exit the Ethernet Interface Configuration mode by entering the following command:

```
exit
```

The following prompt appears:

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

Step 7 Exit the context configuration mode by typing:

```
exit
```

The following prompt appears:

```
[<context_name>] < host_name > (config) #
```

Step 8 Enter the following command to select the physical port that the interface is to use:

```
port ethernet slot#/port#
```

Variable	Description
<i>slot#</i>	The actual chassis slot in which the line card is installed. This can be any number from 17 to 23, or 26 to 39, or 42 to 48.
<i>port#</i>	The physical port on the line card designated for use. For the 10/100 Ethernet line cards, this value is from 1 to 8. For the QGLC, the value is 1 to 4. For the XGLC and Ethernet 1000 line cards, this value is 1.

The following prompt appears:

```
[<context_name>] < host_name > (config-port-<slot#/port#>)#
```

Step 9 Enter a description for the port if desired, by entering the following command:

```
description port_description
```

port_description is a name or character string used to identify this port. The description is case sensitive and must be from 1 to 79 alpha and/or numeric characters.



Step 10 Optional. If LC port redundancy was enabled at the card level, enter the following command to configure a port preference:

```
preferred slot slot#
```

slot# is the physical chassis slot where the LC is installed.

Step 11 Configure the port speed, if needed:

```
medium {auto | speed {10 | 100 | 1000} duplex {full | half}}
```

Keyword/Variable	Description
auto	Configures the system to auto detect the port speed. This is the default setting.
speed	<p>Specifies the port speed for the port. When manually configuring the port speed, you must ensure that the network server configuration supports the speed and duplex configuration. The possible rates are:</p> <ul style="list-style-type: none"> • 10 specifies 10 Mbps • 100 specifies 100 Mbps • 1000 specifies 1000 Mbps <hr/> <p> Important: If the port speed is manually configured, you must also configure the duplex mode.</p> <hr/>
duplex	<p>If the speed is manually configured, you must also use this parameter to configure the duplex mode. Either full or half duplex mode can be implemented.</p> <hr/> <p> Important: Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device negotiates to the manually configured speed of the second device but only communicates in half duplex mode.</p> <hr/>

Step 12 Enable the port by entering the following command:

```
no shutdown
```

Step 13 Bind the port to the interface. Binding associates the port and all of its settings to the interface. Enter the following command to bind the port to the interface:

```
bind interface interface_name context_name
```

Keyword/Variable	Description
<i>interface_name</i>	The name of the interface that was configured in <i>step 3</i> of this section.
<i>context_name</i>	The name of the context in which the interface was selected.

Step 14 Enter the following command to exit the Ethernet Port Configuration mode:

```
exit
```

The following prompt appears:

```
[<context_name>] < host_name > (config) #
```

Step 15 Configure a static route for the interface, if needed, by following these instructions:

Step a Enter the context configuration mode by typing the following command:

```
context context_name
```

context_name is the name of the context in which the interface was configured.

The following prompt appears:

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

Step b Enter the following command to configure the static route(s):

```
ip route network mask gw_address interface_name
```

Keyword/Variable	Description
<i>network</i>	The IP address of the target network or subnet.

Keyword/Variable	Description
<i>mask</i>	The subnet mask for network.
<i>gw_address</i>	The IP address of the default gateway or next-hop router.
<i>interface_name</i>	The name of the interface for which the static route is being configured.



Important: To configure a route to the gateway router, use 0.0.0.0 for the network and mask variables.

Repeat this step as needed. You can configure multiple static routes to the same destination to provide an alternative means of communication in case the preferred route fails.

Step c To exit the context configuration mode, enter the following command:

```
exit
```

The following prompt appears:

```
[<context_name>] <host_name> (config)#
```

Step 16 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local] < host_name > #
```

Step 17 Repeat *step 1* through *step 16* for every individual interface to be configured.

Step 18 To verify that your interface configuration settings are correct enter the following commands:

```
context context_nameshow ip interface
```

context_name represents the name of the context in which you created the interface. The output from these commands should look similar to that displayed below. In this example, an interface named mgmt1 was configured in the local context.

```
Intf Name: mgmt1
```

```
Intf Type: Broadcast
```

```
IP State: UP (Bound to 17/1 untagged, ifIndex 285278209)
```

```

IP Address: 192.168.100.3 Subnet Mask: 255.255.255.0

Bcast Address: 192.168.100.255 MTU: 1500

Resoln Type: ARP ARP timeout: 3600 secs

L3 monitor LC-port switchover: Disabled

Number of Secondary Addresses: 0

Total interface count: 1

```

Step 19 Verify that your port configuration settings are correct by entering the following command:

```
show configuration port slot#/port#
```

slot# is the chassis slot number of the line card on which the physical port resides. slot# can be any integer value from 17 to 39, and 42 to 48. port# is the number of the port.

This command produces an output similar to that displayed below, which shows the configuration of port 1 of the line card installed in chassis slot 17. In this example, the port is bound to an interface called rp1 configured in a context called source.

```

config
  port ethernet 17/1
  description LC17/1_RP1
  no shutdown
  bind interface rp1 source
  #exit
end

```

Step 20 To verify that you configured your static route(s) properly, by enter the following command:

```
show ip static-route
```

This command produces an output similar to that displayed in the following example, which shows a static route to a gateway with an IP address of 192.168.250.1:

Destination	Nexthop	Protocol	Prec	Cost	Interface
0.0.0.0/0	192.168.250.1	Static	0	0	SP101

Step 21 Save your configuration as described in Saving Your Configuration.

Creating and Configuring FA Services

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



Important: This section provides the minimum instruction set for configuring an FA service so the system can process data sessions. Commands for configuring additional FA service properties are provided in the Command Line Interface Reference. Additionally, when you configure mobile IP, take into account the MIP timing considerations discussed in *Appendix 1, R_MIP Timer Considerations*.

This section provides instructions for configuring FA services. These instructions assume that you are at the root prompt for the Exec mode:

```
[local] < host_name > #
```

Step 1 Enter the configuration mode by typing:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

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

```
context context_name
```

context_name is the name of the system context designated for FA service configuration. The name must from 1 to 79 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Enter the following command to create the FA service:

```
fa-service fa_service_name
```

fa_service_name is the name designated for the FA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:


```
[<context_name>] < host_name > (config-fa-service) #
```

Step 4 Configure the local User Datagram Protocol (UDP) port for the Pi interfaces' IP socket by entering:

```
ip local-port port#
```

port# is the UDP port number and can be any integer value from 1 to 65535. The default value is 434.

Step 5 Configure the security parameter index (SPI) between the FA service and the HA by entering the following command:

```
fa-ha-spi remote-address ha_ip_address spi-number number {encrypted  
secret enc_secret | secret secret} [description < string > ]
```

Keyword/Variable	Description
remote address	Specifies the IP address of the HA (<i>ha_ip_address</i>). Express <i>ha_ip_address</i> as an IP address or an IP address and mask in dotted decimal notation (###.###.###.### or ###.###.###/###).
spi number	Specifies the SPI (<i>number</i>) which indicates a security context between the FA and the HA in accordance with RFC 2002. Configure <i>number</i> to any integer from 256 to 4294967295.
encrypted secret	Specifies the encrypted shared key (<i>enc_secret</i>) between the FA and the HA services. The system uses the encrypted keyword when it saves configuration scripts. The system displays the encrypted keyword in the configuration file to indicate that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.
secret	Specifies the shared key (<i>secret</i>) between the FA and the HA services. <i>secret</i> is from 1 to 127 alpha and/or numeric characters and is case sensitive.
description <i>string</i>	This is a description for the SPI. <i>string</i> is an alpha and/or numeric string of 1 through 31 characters.



Important: You can configure a maximum of 2048 FA-HA SPIs for a single FA service. Specify how the system should handle the MN-HA authentication extension in the RRP by entering the following command:

```
authentication mn-ha {allow-noauth | always}
```

Keyword/Variable	Description
allow-noauth	Allows a reply that does not contain the authentication extension.
always	A reply should always contain the authentication extension to be accepted.

Step 6 Enter the following to specify how the system handles authentication for mobile node re-registrations:

```
authentication mn-aaa {always | ignore-after-handoff | init-reg | init-
reg-except-handoff | renew-and-dereg-noauth | renew-reg-noauth}
[optimize-retries]
```

Keyword/Variable	Description
always	Specifies that the FA service performs authentication each time a mobile node re-registers.
ignore-after-handoff	MN-AAA authentication is not done at the FA, for a handoff ASN Gateway.
init-reg	MN-AAA and MN-FAC extensions are required only in initialization RRQ.
init-reg-except-handoff	MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-ASN Gateway handoff.
renew-and-dereg-noauth	Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.
renew-reg-noauth	Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration is handled normally.
optimize-retries	Optimizes the number of Authentication retries sent to the AAA server. When an authentication request is pending for a MIP call at the ASN Gateway, if a retry RRQ is received from the mobile node, the ASN Gateway discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the ASN Gateway forwards the most recent RRQ to the HA. If the authentication fails, the ASN Gateway replies to the MN using the most recent RRQ.

Step 7 Specify to suppress the AAA distributed Mobile IP key coming from AAA server by entering the following command:

```
authentication aaa-distributed-mip-keys override
```

Step 8 To enable the proxy MIP to allow PMIP calls, enter:

```
proxy-mip allow
```

Step 9 Specify the FA agent advertisement lifetime. The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. Configure the FA agent advertisement lifetime with the following command:

```
advertise adv-lifetime time
```

Configure time in seconds with any integer from 1 to 65535. The default is 9000.

Step 10 Specify the number of unanswered agent advertisements that the FA service allows during call setup before it rejects the session:


```
advertise num-adv-sent number
```

For number enter an integer from 1 to 65535. The default is 3.

- Step 11** Specify the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. Enter the following command for the registration lifetime:

```
advertise reg-lifetime reg_time
```


Configure reg_time in seconds with any integer from 1 to 65534. The default is 600.

 **Important:** To configure an infinite registration lifetime, use the **no advertise reg-lifetime** command.

- Step 12** Specify the number of simultaneous Mobile IP sessions that are to be supported for a single subscriber:

```
multiple-reg number
```

Configure number with integer from 1 to 3. The default is 1.

 **Important:** The system supports multiple mobile IP sessions per subscriber only if the subscriber's mobile node has a static IP address. The system allows a single mobile IP session only for mobile nodes that receive a dynamically assigned home IP address.

- Step 13** Specify the maximum amount of time that the FA service waits for a Registration Rely message from the HA:

```
reg-timeout time
```

Configure time in seconds with any integer from 1 to 65535. The default value is 7.

- Step 14** Optional. Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:


```
revocation negotiate-i-bit
```

By default, the system does not send an I-bit in a revocation message.

- Step 15** Bind the service to an interface and specify the maximum number of subscribers that can access this service. Binding an interface to the FA service causes the interface to take on the characteristics of a Pi interface. Enter the following command:

```
bind address address max-subscribers max#
```

Keyword/Variable	Description
address	Specifies the IP address (<i>address</i>) of the interface that is to serve as a IP interface.

Keyword/Variable	Description
<i>max#</i>	Specifies the maximum number of subscribers that can access this service on this interface. Specify any integer from 0 to 500,000. The default is 500,000.
	 Important: The maximum number of subscribers supported is dependent on the session capacity license installed and the number of active processing cards installed in the system. A fully loaded system with 13 active processing cards can support 500,000 total subscribers. For additional information on session capacity licenses, refer System Administration Guide and <i>System Capacities</i> in this guide.



Important: The hardware configuration and installed features installed affect the maximum number of supported subscriber sessions.

Step 16 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local] < host_name > #
```

Step 17 Repeat *step 1* through *step 16* as needed to create and bind additional FA services to any other interfaces.

Step 18 Verify that your FA services were created and configured properly by entering the following command:

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


Keyword/Variable	Description
name	Specifies to display a specific FA service with the name <i>service_name</i> .
all	Specifies to display all configured FA services.

The output is a concise listing of FA service parameter settings for a configured FA service called fa1.

Step 19 Save your configuration as described in Saving Your Configuration.

Creating and Configuring HA Services

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

 **Important:** This section provides the minimum instruction set for configuring an HA service that allows the system to process data sessions. Refer to the Command Line Interface Reference to configure additional HA service properties. Additionally, when you configure mobile IP, take into account the MIP timing considerations discussed in *Appendix 1, R_MIP Timer Considerations*.

This section provides instructions for configuring HA services. These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

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

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode by typing:

```
context context_name
```

The context_name is name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Enter the following command to create the HA service:

```
ha-service ha_service_name
```

The ha_service_name is the name designated for the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-ha-service)#
```

Step 4 Configure the local User Datagram Protocol (UDP) port for the Pi interfaces' IP socket:

```
ip local-port port#
```

The port# is the UDP port number and is any integer from 1 to 65535. The default is 434.

Step 5 Configure the security parameter index (SPI) between the HA service and the FA by entering the following command:

```
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}]
```

Keyword/Variable	Description
remote-address	Specifies the IP address of the FA (<i>fa_ip_address</i>). Express <i>fa_ip_address</i> as an IP address or an IP address and mask in dotted decimal notation (###.###.###.### or ###.###.###/###). The system supports unlimited peer FA addresses per HA. See the <i>Service Rules</i> section of the <i>Engineering Rules</i> appendix in this guide for more information.
spi-number	Specifies the SPI (<i>number</i>) which indicates a security context between the FA and the HA in accordance with RFC 2002. Configure <i>number</i> as an integer from 256 to 4294967295.
encrypted secret	Specifies the encrypted shared key (<i>enc_secret</i>) between the HA and the FA services. The system uses the encrypted keyword only when it saves configuration scripts. The system displays the encrypted keyword in the configuration file to indicate that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.
secret	Specifies the shared key (<i>secret</i>) between the HA and the FA services. <i>secret</i> must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
description <i>string</i>	This is a description for the SPI. Define <i>string</i> as an alpha and or numeric string up to 31 characters.
hash-algorithm	Specifies the hash algorithm to use protect the SPI. The following algorithm are supported: <ul style="list-style-type: none"> • hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis. • md5: Configures the hash-algorithm to implement MD5 per RFC 1321. • rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.



Important: Configure a maximum of 2048 FA-HA security parameter indexes (SPIs) for each HA service. To configure the SPI between the HA service and the mobile node, enter the following command:

```
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]
```

Keyword/Variable	Description
spi-number	Specifies the SPI (<i>number</i>) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. Configure <i>number</i> to be an integer from 256 to 4294967295.
description <i>string</i>	This is a description for the SPI. <i>string</i> must be an alpha and/or numeric string of up to 31 characters.
encrypted secret	Specifies the encrypted shared key (<i>enc_secret</i>) between the HA service and the mobile node. The system uses the encrypted keyword only when it saves configuration scripts. The system displays the encrypted keyword in the configuration file to indicate that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.
secret	Specifies the shared key (<i>secret</i>) between the HA service and the mobile node. <i>secret</i> must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
hmac-md5	Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis. This is enabled by default.
md5	Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5	Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.
permit-any-hash-algorithm	Uses all other hash-algorithms to verify the MN-HA authenticator using after a failure with the configured hash-algorithm. The successful algorithm is logged to aid in troubleshooting and is used to create the MN-HA authenticator in the Registration Reply message.
replay-protection	Specifies the replay-protection scheme to implement by the HA service for this SPI.
nonce	Configures replay protection to implement using nonces per RFC 2002.
timestamp	Configures replay protection to implement using timestamps per RFC 2002.
<i>tolerance</i>	Specifies the allowable difference (<i>tolerance</i>) in timestamps that is acceptable. If the difference is exceeded, then the session is rejected. Configure <i>tolerance</i> in seconds with an integer from 1 to 65535.

Step 6 Specify how the system should handle the MN-HA authentication extension in the RRQ by entering the following command:

```
authentication mn-ha {allow-noauth | always}
```

Keyword/Variable	Description
allow-noauth	Allows a reply that does not contain the authentication extension.
always	A reply always contains the authentication extension to accept.

Step 7 Configure the HA service authentication parameters by entering the following command:

```
authentication mn-aaa {allow-noauth | always | noauth | renew-reg-noauth}
```

Keyword/Variable	Description
allow-noauth	Specifies that the HA service does not require authentication for every mobile node re-registration. However, if the mn-aaa extension is received, the HA service authenticates it.
always	Specifies that the HA service performs authentication each time a mobile node re-registers. Enabled by default.
noauth	Specifies that the HA service does not look for mn-aaa extension and does not authenticate it.
renew-reg-noauth	Specifies that the HA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration is handled normally.

- Step 8** Specify the longest registration lifetime that the HA service allows in any Registration Request message from the mobile node. Configure the registration lifetime by entering:

```
reg-lifetime time
```

Enter an integer from 1 to 65534 for time in seconds. The default value is 600.



Important: To configure an infinite registration lifetime, use the no reg-lifetime command.

- Step 9** Specify the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address:

```
simultaneous-bindings number
```

Configure number as an integer from 1 to 5. The default value is 3.

- Step 10** Optional. Configure the HA service for controlling the negotiation and sending of the I-bit in revocation messages by following command:


```
revocation negotiate-i-bit
```


By default, the system does not send I-bit in a relocation message.

- Step 11** Enter the following command to bind the service to the Pi or R3 interface and to specify the maximum number of subscribers that can access this service:

```
bind address address max-subscribers max#
```

Keyword/Variable	Description
address	Specifies the IP address (<i>address</i>) of the interface configured as the Pi interface.

Keyword/Variable	Description
<i>max#</i>	Specifies the maximum number of subscribers that can access this service on this interface. Specify an integer from 0 to 500,000. The default is 500,000.
	 Important: The maximum number of subscribers supported depends on the installed session capacity license and the number of active processing cards in the system. A fully-loaded system with 13 active processing cards supports 500,000 subscribers. For more information, refer to the System Administration Guide and <i>System Capacities</i> .

 **Important:** The hardware configuration and installed features affect the maximum number of supported subscriber sessions.

- Step 12** Optional. Change the maximum amount of time, in seconds, allowed to set up a session. The default is 60 seconds. To change this value use the following command:

```
setup-timeout < seconds >
```

Where seconds is an integer from 1 through 1000000.

- Step 13** Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local] < host_name > #
```

- Step 14** Repeat *step 1* through *step 13* as needed to create and bind additional HA services to any other interfaces.

- Step 15** Enter the following command to verify that your HA services were created and configured properly:

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

Keyword/Variable	Description
name	Specifies to display a specific HA service with the name <i>service_name</i> .
all	Specifies to display the configuration of all HA services.

The output is a concise listing of HA service parameter settings for a configured HA service called ha.

- Step 16** Save your configuration as described in Saving Your Configuration.

Session Continuity Support

This section describes how to enable the mobility for WiMAX and other access technology subscribers. 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.

The 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 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. This includes 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 the compute authenticator in RRP.

The authentication algorithm for MN-HA and FA-HA AE is HMAC-MD5. If a renew/dereg RRQ message is received, AAA authentication occurs only if the SPI value for the authentication extension in the RRQ changes. If the SPI returned by AAA is different from the requested one, the RRQ is rejected. Both MN-HA and FA-HA AE are expected in MIP RRQ for WiMAX calls.

Following is the description of how different requests for HA support are processed.

- Processing Access-Request: When the 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) are received. The MN-HA key is maintained for each subscriber session and the FA-HA key is computed based on HA-RK maintained per HA.

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

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

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

Apart from these processes, HA provides the 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 calls to get the MIP Keys.

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

Configuring Hybrid HA Service

This section provides the configuration procedure to configure the HA service for:

- WiMAX HA for WiMAX calls only
- Hybrid HA for WiMAX and 3GPP2 calls

With this support, an HA can work in a hybrid mode, meaning that an HA can handle a call from CDMA network, a call from WiMax network, and a hybrid call with an RRQ coming first from one network and then from another. This way, an operator can 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 an RRQ.

Configuring WiMAX HA for WiMAX Calls

This section provides instructions for configuring WiMAX HA services and enables the use of AAA-provided WiMAX MIP keys for authenticating MIP RRQ with mandatory keys. These instructions assume that you are at the root prompt for the Exec mode:

```
[local] < host_name > #
```

Step 1 Enter the configuration mode and enter:

```
configure
```

The following prompt appears:

```
[local] <host_name> (config)#
```

Step 2 Enter context configuration mode and enter:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the HA service by entering the following command:

```
ha-service ha_service_name
```

ha_service_name is the name designated for the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-ha-service) #
```

Step 4 Configure the HA service for WiMAX calls only by entering:

```
authentication aaa-distributed-mip-keys required
```

Step 5 Return to the Exec mode by entering:

```
end
```

Step 6 Save your configuration as described in Saving Your Configuration.

When this configuration is enabled, the system will support only WiMAX HA behavior for the particular HA-service. The system always expects WiMAX MIP keys from AAA and uses them 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.

Configuring WiMAX HA to Accept 3GPP2/Static MIP Key

This section provides instructions for configuring HA services to accept 3GPP2 calls and disable the use of AAA-provided WiMAX MIP keys for authenticating MIP RRQs. These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the HA service by entering the following command:

```
ha-service ha_service_name
```

`ha_service_name` is the name designated for the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-ha-service)#
```

Step 4 Configure the HA service for WiMAX calls only by entering:

```
authentication aaa-distributed-mip-keys disabled
```

Step 5 Return to the Exec mode by entering the following command:

```
end
```

Step 6 Save your configuration as described in Saving Your Configuration.

Hybrid HA for WiMAX and 3GPP2 Calls

This section describes how to configure HA services to accept WiMAX and 3GPP2 calls in the same service and to enable the use of AAA-provided WiMAX MIP keys for authenticating MIP RRQs with the fallback option to use 3GPP2/static keys. These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode by entering:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Enter the following command to create the HA service:

```
ha-service ha_service_name
```

`ha_service_name` is the name designated for the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-ha-service)#
```

Step 4 Enter the following command to configure the HA service for WiMAX and 3GPP2:

```
authentication aaa-distributed-mip-keys optional
```

Step 5 Enable 3GPP2-WiMAX interworking for session continuity with dual access device:

```
wimax-3gpp2 interworking
```

Step 6 Return to the Exec mode by entering the following command:

```
end
```

Step 7 Save your configuration as described in Saving Your Configuration.

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

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.

This capability provides the following benefits:

- Common billing and customer care
- Accessing home 3GPP2 service through Wimax network and vice versa
- Seamless session continuity with no perceived impact from a user's perspective

To provide this capability, the HA supports the seamless handoff from 3GPP2 to WiMAX, or WiMAX to 3GPP2.

This section describes how to configure session continuity.

Mobile Node Requirement

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

- The dual-mode MS must use PMIP to access the WiMAX network and use CMIP to access 3GPP2 network.
- The static NAI (the NAI that is pre-provisioned for access to 3GPP2) must be used in RRQs on both 3GPP2 and WiMAX networks.
- The dual-mode MS must 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 meet the following requirements to support 3GPP2-WiMax Interworking at HA:

- The H-AAA servers used by 3GPP2 and WiMax must be the same or have access to the same session state and subscriber profile.
- H-AAA server must assign and return the same HA address in response to 3GPP2 and WiMax network access requests.

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 must not include the MN-AAA AE in the RRQ.
- For 3GPP2 access, the FA must 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 the following functionality to support 3GPP2-WiMax Interworking at the 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, consider the following:

Generic Configuration:

- 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 the s-bit in the RRQ.

WiMAX FA Service Configuration

- MIP key from AAA must not be suppressed with the **authentication aaa-distributed-mip-keys override** command.
- Revocation must be enabled

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

```
[local] < host_name > #
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode by entering:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the FA service for WiMAX by entering the following:

```
fa-service fa_service_name
```

`fa_service_name` is the name designated for the FA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-fa-service)#
```

Step 4 To configure the FA service to disable the override of dynamic keys from AAA with static keys, entering the following command:

```
authentication aaa-distributed-mip-keys override
```

Step 5 Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:

```
revocation negotiate-i-bit
```

By default it will not send I-bit in revocation message.

Step 6 Return to the Exec mode by entering the following command:

```
end
```

Step 7 Save your configuration as described in Saving Your Configuration.

3GPP2 FA Service Configuration

- The FA must not be configured to remove the MN-FAC and MN-AAA extensions from RRQs, and the `mn-aaa-removal-indication` command MUST NOT be enabled
- Revocation must be enabled.

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

```
[local]host_name#
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode by entering:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the FA service for 3GPP2 by entering the following command:

```
fa-service fa_service_name
```

`fa_service_name` is the name designated for the FA service for 3GPP2 service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-fa-service)#
```

Step 4 To disable the removal of the MN-FAC and MN-AAA extensions from RRQs at FA service, enter:

```
default mn-aaa-removal-indication
```

Step 5 To configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages, enter:

```
revocation negotiate-i-bit
```

By default it will not send I-bit in revocation message.

Step 6 Return to the Exec mode by entering the following command:

```
end
```

Step 7 Save your configuration as described in Saving Your Configuration.

Common HA Service Configuration

- WiMAX-3GPP2 interworking must be enabled. Use the `wimax-3gpp2 interworking` command.
- The authentication `aaa-distributed-mip-keys` must be set to `required`.
- The authentication `mn-aaa` command must be set to `allow-noauth`.
- Revocation must be enabled.

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

```
[local] < host_name > #
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode by entering:

```
context context_name
```

`context_name` is the name of the system context designated for HA service configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create the HA service by entering the following command:

```
ha-service ha_service_name
```

ha_service_name is the name designated for the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

```
[<context_name>] < host_name > (config-ha-service) #
```

Step 4 To configure the HA service to process MIP keys coming from the AAA, enter:

```
authentication aaa-distributed-mip-keys required
```

Step 5 To enable 3GPP2-WiMAX interworking for session continuity with dual-access devices, enter:

```
wimax-3gpp2 interworking
```

Step 6 To configure the HA service to allow the message without authentication extensions between MN and AAA, enter:

```
authentication mn-aaa allow-noauth
```

Step 7 Configure the HA service for controlling the negotiation and sending of the I-bit in revocation messages by entering:

```
revocation negotiate-i-bit
```

By default it will not send I-bit in revocation message.

Step 8 Return to the Exec mode by entering the following command:

```
end
```

Step 9 Save your configuration as described in Saving Your Configuration.

Configuring DHCP-based IP Address Assignment

You can configure the system to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for subscriber sessions. Use one of the following two methods:

- **DHCP proxy mode:** Upon boot-up, the system communicates with a DHCP server to reserve a configurable number of IP addresses. The reserved addresses are stored in cache memory for assignment to subscriber sessions as required.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

- **DHCP relay mode:** The system proxies, or relays, DHCP requests from mobile stations to a DHCP server. The IP addresses assigned by the server are then assigned to the subscriber sessions by the system.

Regardless of the DHCP method, there are parameters you must configure that specify the DHCP servers to communicate with and how the IP address are handled. Configure these parameters as part of a DHCP service.

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

```
[local] host_name#
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] host_name(config)#
```

Step 2 Enter context configuration mode:

```
context context_name
```

`context_name` is the name of the system destination context designated for DHCP functionality configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.



Important: To ensure proper operation, configure DHCP functionality within a destination context.

The following prompt appears:

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

Step 3 Enter the DHCP service configuration mode by entering:

```
dhcp-service service_name
```

service_name is the name of the DHCP service containing the functionality configuration. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Step 4 Configure the DHCP servers within the context by entering the following command:

```
dhcp server < ip_address > [priority <priority > ]
```

Keyword/Variable	Description
ip address	Specifies the IP address of the DHCP server.
priority	Specifies the priority of the server when multiple servers are configured. Configure <i>priority</i> to be an integer from 1 to 1000. 1 is the highest priority. The default is 1.

Configure multiple DHCP servers by entering this command for each server. You can configure up to a maximum of 20 DHCP servers.

Step 5 Configure the minimum and maximum allowable lease times that are accepted in responses from DHCP servers by entering the following command:

```
lease-duration min min_time max max_time
```

Keyword/Variable	Description
min	Specifies the minimum acceptable lease time. Configure <i>min_time</i> in seconds as an integer from 600 to 3600. The default is 600 seconds.
max	Specifies the maximum acceptable lease time. Configure <i>max_time</i> in seconds as an integer from 10800 to 4294967295. The default is 86400 seconds.

Step 6 Bind the DHCP service to an IP interface in the same context by entering the following command:

```
bind < ip_address >
```

ip_address specifies the IP address of an interface in the current context through which communication with the DHCP server occurs. Enter *ip_address* in dotted decimal notation.

When this command is executed, the DHCP service is started. The request is sent for addresses from the DHCP server.

Step 7 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local]host_name#
```

Step 8 Repeat *step 1* through *step 4* to configure additional DHCP servers.

Step 9 Verify that your DHCP servers were configured properly:

```
show dhcp servers {all | name < svc_name > }
```

Keyword/Variable	Description
all	Displays information for all configured DHCP services.
name	Displays information for a specific DHCP service. <i>svc_name</i> is the name of the service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

Step 10 Save your configuration as described in Saving Your Configuration.

Configuring the Destination Context Attribute

Once a user is authenticated, an AAA attribute is returned in the access-accept message that contains the name of the destination context where the subscriber originates. For RADIUS-based subscribers, this is the SN-VPN-Name attribute, or SN1-VPN-Name attribute in some RADIUS dictionaries.

The system supports subscriber profiles configured locally within a context through subscriber templates or on a RADIUS server. Configure subscribers on the system within the contexts in which they were created. Refer to the System Operation and Configuration chapter of this document for a discussion of the role of subscriber default, which is automatically configured for each context, and realm-based subscriber templates, which serve as a default subscriber template for users whose domain portion of their username matches a domain alias within a context. These special subscriber templates provide a set of default attributes that you can use to populate missing values for an authenticated RADIUS-based subscriber. The parameter that contains this attribute value is called the ip context-name.

The System Operation and Configuration chapter also explains that you must manually configure these attributes for both the subscriber default template and any created realm-based subscriber template.

One of the rules you must configure is a parameter that allows subscriber data traffic to be routed between source and destination contexts. This section provides instructions for configuring that rule. Refer to the Command Line Interface Reference for information pertaining to other subscriber profile parameters.

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

```
[local] < host_name > #
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config) #
```

Step 2 Enter the context configuration mode:

```
context context_name
```

context_name is the name of the system source context designated for Default subscriber configuration. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Enter the subscriber configuration mode for the Default subscriber by entering the following command:

```
subscriber name default
```

The following prompt appears:

```
[<context_name>] < host_name > (config-subscriber)#
```

Step 4 Configure a name for the destination context by entering:

```
ip context-name destination_context_name
```

`destination_context_name` is the name of the destination context configured on the system containing the interfaces through which session traffic is routed.



Important: The `ip context-name` parameter in the subscriber profiles configured on the system corresponds to the `SN-VPN-NAME` and `SN1-VPN-NAME RADIUS` attributes.

Step 5 Return to the Exec mode by entering the following command:

```
end
```

The following prompt appears:

```
[local] < host_name > #
```

Step 6 Repeat *step 1* through *step 5* to configure the default subscriber in any other configured source contexts.

Step 7 To verify that your settings for the subscriber named `default` are correct, enter:

```
show subscribers configuration username default
```

This command's output displays the configured subscriber parameters.


Step 8 Save your configuration as described in *Saving Your Configuration*.

Configuring IP Address Pools on the System

One of the steps in establishing a subscriber session between the mobile and the ASN Gateway service running on the system is that upon successful authentication, the subscriber's mobile node is assigned an IP address. The IP address can be dynamically assigned from a pool that is configured on the system or on the AAA server. It also supports static or dynamic addressing through DHCP client-mode or DHCP relay-mode. The IP address may be an address that is statically configured in the user profile or even one that is requested by the subscriber.

IP addresses can be dynamically assigned from a single pool, a group of IP pools, or a group of IP pool groups. The addresses, IP pools, or IP pool groups are placed into a queue in each pool or pool group. An address is assigned from the head of the queue and when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm determines a probability for each pool based on the number of available addresses. A pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

 **Important:** Note that setting different priorities on each pool can cause addresses in some pools to be used more frequently.

This section provides instructions for configuring local IP address pools on the system. These instructions assume that you are at the root prompt for the Exec mode:

```
[local]system#
```

Step 1 Enter the configuration mode by entering:

```
configure
```

The following prompt appears:

```
[local] < host_name > (config)#
```

Step 2 Enter context configuration mode:

```
context context_name
```

`context_name` is the name of the destination context in which you want to configure the IP address pool. The name must be from 1 to 79 alpha and/or numeric characters and is case sensitive.

The following prompt appears:

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

Step 3 Create an IPv4 address pool by entering the following command.

```



ip pool name {ip_address subnet_mask | ip_addr_mask_combo | range
start_address end_address} [private [priority] | public [priority] |
static] [address-hold-timer seconds | alert-threshold [group-available |
pool-free | pool-hold | pool-release | pool-used] low_thresh [clear
high_thresh]] [group-name group_name] [nexthop-forwarding-address
ip_address [overlap vlandid vlan_id]] [nw-reachability server server_name]
[policy allow-static-allocation] [resource] [send-icmp-dest-unreachable]
[srp-activate] [suppress-switchover-arp] [unicast-gratuitous-arp-address
ip_address] [policy allow-static-allocation]

```



Important: Overlapping IP Pools: To configure IP pools whose addresses overlap, you must specify the nexthop-forwarding-address and overlap keywords. Each address in the pool requires approximately 60 bytes of memory. Therefore, in order to conserve available memory, you may need to limit the number of pools depending on the number of addresses to be configured and the number of processing cards installed.

Keyword/Variable	Description
<i>pool_name</i>	Specifies a name or description for the address pool. <i>pool_name</i> must be from 1 to 31 alpha and/or numeric characters and is case sensitive.
<i>ip_address</i>	Specifies the first IP address in the pool.
<i>subnet_mask</i>	Specifies the subnet mask for the pool which determines how many addresses are available to the pool.
<i>ip_addr_mask_combo</i>	Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. Specify <i>ip_addr_mask_combo</i> in the form IP Address/Mask Bits. Use the standard IPv4 format for the IP address.
range	Specifies the IP addresses for the IP pool as a range of addresses. <i>start_address</i> specifies the beginning of the range of addresses for the IP pool. <i>end_address</i> specifies the end of the range of addresses for the IP pool. Use the standard IPv4 format for the IP address range.
public	Specifies that the addresses contained in this pool can be assigned to any subscriber. <i>priority</i> represents the priority of the pool. Configure priority to be an integer from 0 to 10, 0 being the highest priority. The default is 0.
private	Specifies that addresses from this pool can only be assigned if RADIUS server asks to assign from this pool. Therefore, you must configure the name of this pool (<i>pool_name</i>) in the subscriber's RADIUS profile prior to its being assigned an address from it. <i>priority</i> represents the priority of the pool. Configure priority to be an integer from 0 to 10, 0 being the highest priority. The default is 0.

Keyword/Variable	Description
static	<p>Specifies that an IP address can only be assigned from this pool if a mobile node has a pre-assigned IP address and wants to establish a session. Therefore, when the MS requests the desired address, the subscriber's RADIUS profile dictates to assign it from this pool.</p> <hr/> <p> Important: If DHCP is used (either in client-mode or relay-mode), static address pools must be configured consisting of IP addresses identical to those that can be assigned by the DHCP server.</p> <hr/>
alert-threshold {group-available pool-free pool-hold pool-release pool-used} <i>low_thresh</i> [clear <i>high_thresh</i>]	<p>Default: All thresholds are disabled. Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds. group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group. pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool. pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold. pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state. pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool. <i>low_thresh</i>: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. Configure as an integer between 0 and 100. clear <i>high_thresh</i>: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. Configure as an integer between 0 and 100.</p> <hr/> <p> Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold. Refer to Thresholding Configuration Guide for additional information on configuring IP pool thresholding.</p> <hr/>
group-name <i>group_name</i>	<p>Assigns preconfigured one or more IP pools to the IP pool group <i>group_name</i>. <i>group_name</i> is case sensitive and must be a string of 1 to 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool.</p> <p>IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool's addresses are exhausted the pool with the next highest precedence is used.</p>
nexthop-forwarding-address <i>ip_address</i>	<p>A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address.</p>

Keyword/Variable	Description
overlap vlanid <i>vlan_id</i>	<p>When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN).</p> <p>For more information on configuring VLANs, refer to VLANs chapter for more information on configuring VLANs.</p> <p><i>vlan_id</i> is the identification number of a VLAN assigned to a physical port and can be configured to any integer value from 1 to 4095.</p> <p>NOTE: This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN, or as an ASN Gateway for Simple IP. This keyword can only be issued for pools of type private or static and must be associated with a different next hop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IP PDSN/ASN Gateway. For GGSNs, the total number of pools is limited by the number of VLANs defined; the maximum number per context is still 256.</p> <p>NOTE: Additional network considerations and configuration outside of the system may be required.</p>
nw-reachability server <i>server_name</i>	<p>Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.</p> <p><i>server_name</i>: The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.</p> <p>NOTE: Also see the following commands for more information: Refer to the policy nw-reachability-fail command to in the HA Service Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the nw-reachability server command in the Context Configuration Mode to configure network reachability servers. Refer to the nw-reachability-server command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.</p>
policy allow-static-allocation	Allow a dynamic pool to accept a static address allocation
resource	<p>Default: Disabled</p> <p>Define this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that exist in other resource pools. Do not use IP addresses from a resource pool for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs. Refer to the subscriber configuration mode l3-to-l2-tunnel address-policy command.</p>
send-icmp-dest-unreachable	<p>Default: Disabled</p> <p>When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool.</p>
srp-activate	Activates the IP pool for Interchassis Session Redundancy.
suppress-switchover-arp	<p>Default: Disabled</p> <p>Suppress corresponding gratuitous ARP generation when a line card switchover occurs.</p>
unicast-gratuitous-arp-address <i>ip_address</i>	<p>Default: Perform broadcast gratuitous ARP.</p> <p>Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required.</p>

Keyword/Variable	Description
policy allow-static-allocation	Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

Step 4 Repeat *step 3* to configure additional IPv4 pools within the context.

Step 5 Optional. Create an IPv6 address pool by entering the following command:

```
ipv6 pool name {6to4 local-endpoint ip_address [default-relay-router
router_address] | prefix ip_address/len [6to4-tunnel local-endpoint
ip_address | default-relay-router router_address]} [ private] [public]
[shared] [static] [group-name < name > ]
```



Important: Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, you may need to limit the number of pools, depending on the number of addresses to be configured and the number of processing cards installed.

Keyword/Variable	Description
<i>pool_name</i>	Specifies a name or description for the address pool. <i>pool_name</i> must be from 1 to 31 alpha and/or numeric characters and is case sensitive.
6to4 local-endpoint <i>IP address</i>	The IP address for the local end point that communicates between IPv4 and IPv6 networks.
6to4-tunnel local-endpoint <i>IP address</i>	The IP address for the static local endpoint that is reachable from the foreign tunnel endpoint that is used to route IPv6 packets.
default-relay-router	Passes 6to4 packets over the network. This router is set up for 6to4 and has a connection to another address space.
prefix <i>ip_address/len</i>	Specifies the prefix IP address for the pool. Enter <i>ip_address/len</i> in standard IPv6 colon notation.
public	Specifies that the addresses contained in this pool can be assigned to any subscriber. <i>precedence</i> represents the priority of the pool. Configure precedence to be an integer from 0 to 10, 0 being the highest priority. The default is 0.
private	Specifies that addresses from this pool can only be assigned if RADIUS server asks to assign from this pool. Therefore, configure the name of this pool (<i>pool_name</i>) in the subscriber's RADIUS profile prior to being assigned an address from it. <i>precedence</i> represents the priority of the pool. Configure to be an integer from 0 to 10, 0 being the highest priority. The default value is 0.

Keyword/Variable	Description
static	Specifies that an IP address can only be assigned from this pool if a mobile node has a pre-assigned IP address and wants to establish a session. Therefore, when the mobile station requests the address, the subscriber's RADIUS profile dictates that it is assigned from this pool. <div data-bbox="521 411 574 478" data-label="Image"></div> Important: If DHCP is used (either in client-mode or relay-mode), static address pools must be configured consisting of IP addresses identical to those that can be assigned by the DHCP server.
group-name <i>name</i>	Use to group IPv6 pools in to different groups. You may configured the subscribers/domain with the group-name instead of the prefix-pool names. <i>name</i> specifies the name of the group.

Step 6 Repeat *step 5* to configure additional IPv6 pools within the context.

Step 7 Return to the root prompt by entering the following command:

```
end
```

The following prompt appears:

```
[local]host_name#
```

Step 8 Restart this procedure to configure additional IP address pools in other contexts if needed.

Step 9 To verify that you configured your IP address pool properly, by entering the following commands:

```
context context_name show ip pool (for ipv4 address pools) show ipv6 pool
(for ipv6 address pools)
```

context_name represents the name of the context in which the pool was created. The output from this command should look similar to the sample shown below. In this example, the first IP pool, named ip_pool, was specified as a range of addresses and the second IP pool, named ip_pool1, was specified as an address and a mask. Both IP pools were configured in the mip_destination 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 254RG00 pool3 30.30.0.0 255.255.0.0
0 65534
SG00 pool2 20.20.0.0 255.255.0.0 10 65524
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

IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm determines a probability for each pool based on the number of available addresses. A pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

 **Important:** Note that setting different priorities on individual pools can cause addresses in some pools to be used more frequently.

Step 10 Save your configuration as described in the Saving Your Configuration chapter.

Chapter 10

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: gtp 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
```

■ Verifying the Configuration

```

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
<i>url</i>	<p>Specifies the path and name to which the configuration file is to be stored. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using one of the following formats:</p> <ul style="list-style-type: none"> • <code>{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> • <code>file://{ /flash /pcmcia1 /pcmcia2 } [/dir] /file_name</code> • <code>tftp://{ ipaddress host_name [:port#] } [/directory] /file_name</code> • <code>ftp://{ username [:pwd] @ } { ipaddress host_name } [:port#] [/directory] /file_name</code> • <code>sftp://{ username [:pwd] @ } { ipaddress host_name } [:port#] [/directory] /file_name</code> <p>/flash corresponds to the CompactFlash on the SPC/SMC. /pcmcia1 corresponds to PCMCIA slot 1. /pcmcia2 corresponds to PCMCIA slot 2. <i>ipaddress</i> is the IP address of the network server. <i>host_name</i> is the network server's <i>hostname</i>. <i>port#</i> is the network server's logical port number. Defaults are:</p> <ul style="list-style-type: none"> • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data <p>Note: <i>host_name</i> can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid <i>nameserver</i>. <i>username</i> is the username required to gain access to the server if necessary. <i>password</i> is the password for the specified username if required. <i>/directory</i> specifies the directory where the file is located if one exists. <i>/file_name</i> specifies the name of the configuration file to be saved. Note: Configuration files should be named with a <i>.cfg</i> extension.</p>
-redundant	<p>Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the <i>url</i> variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available.</p> <p>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 <i>/pcmcia1</i> 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.</p> <p>Note: If saving the file to an external network (non-local) device, the system disregards this keyword.</p>

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 11

Monitoring the Service

This chapter provides information on how to monitor service status and performance with the **show** commands in the Command Line Interface (CLI). These command have many related keywords that provide useful information on all aspects of the system, from software configuration through call activity and status.

The selection of keywords described in this chapter provides 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 sending 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 Service Status and Performance


Use the commands in this section to monitor the status of tasks, managers, applications, and other software components in the system. Output descriptions for most of the commands are in the Command Line Interface Reference Show Command Output Descriptions Appendix.


Table 35. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Administrative Information	
Display Current Administrative User Access	
View a list of all administrative users currently logged on to the system	<code>show administrators</code>
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	<code>show administrators session id</code>
View information pertaining to local-user administrative accounts configured for the system	<code>show local-user verbose</code>
View statistics for local-user administrative accounts	<code>show local-user statistics verbose</code>
View information pertaining to your CLI session	<code>show cli</code>
Determining the System's Uptime	
View the system's uptime (time since last reboot)	<code>show system uptime</code>
View the Status of Configured NTP Servers	
View the status of the configured NTP servers	<code>show ntp status</code>
View the Status of System Alarms	
View the Status of System Alarms	
View the status of the system's outstanding alarms	<code>show alarm outstanding all</code>
View detailed information about all currently outstanding alarms	<code>show alarm outstanding all verbose</code>
View system alarm statistics	<code>show alarm statistics</code>
View Congestion-Control Statistics	
View Congestion-Control Statistics	<code>show congestion-control statistics {allmgr gtpcmgr hamgr l2tpmgr}</code>
View Remote Management Statistics	
Display SNMP Notification Statistics	
View SNMP notification statistics	<code>show snmp notifies</code>
Display SNMP Access Statistics	

To do this:	Enter this command:
View SNMP access statistics	<code>show snmp accesses</code>
Display SNMP Trap History	
View SNMP trap history	<code>show snmp trap history</code>
Display ORBEM Information	
View ORBEM client status	<code>show orbem client id</code>
View ORBEM session information	<code>show orbem session table</code>
View individual ORBEM sessions	<code>show orbem session id orbem</code>
View ORBEM status information	<code>show orbem status</code>
View Subscriber Information	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View remotely configured subscriber profile settings	<code>show subscribers aaa-configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View information for all ASN Gateway only subscriber sessions	<code>show subscribers asngw-only all</code>
View information for a specific subscriber	<code>show subscribers full username username</code>
View Subscriber Counters	
View counters for a specific subscriber	<code>show subscribers counters username subscriber_name</code>
View Recovered Session Information	
View session state information and session recovery status	<code>show subscriber debug-info { callid msid username }</code>
View Session Statistics and Information	
Display Historical Session Counter Information	
View all historical information for all sample intervals	<code>show session counters historical</code>
Display Session Duration Statistics	
View session duration statistics	<code>show session duration</code>
Display Session State Statistics	
View session state statistics	<code>show session progress</code>

To do this:	Enter this command:
Display Session Subsystem and Task Statistics	
View ASN Gateway Manager statistics	<code>show session subsystem facility asngwmgr all</code>
View AAA Manager statistics	<code>show session subsystem facility aaamgr all</code>
View FA Manager statistics	<code>show session subsystem facility famgr all</code>
View HA Manager statistics	<code>show session subsystem facility hamgr all</code>
View ASN PC Manager statistics	<code>show session subsystem facility asnpcmgr all</code>
View L2TP Manager statistics	<code>show session subsystem facility l2tpmgr all</code>
View Session Manager statistics	<code>show session subsystem facility sessmgr all</code>
View Session Recovery Status	
View session recovery status	<code>show session recovery status [verbose]</code>
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons</code>
View R4/R6 Interface Statistics	
Display a details of R4 Interface Counter Status	
View cumulative R4 interface counters for every subscriber session currently in progress	<code>show asngw-service statistics r4-only verbose</code>
Display details of R6 Interface Counter Status	
View cumulative R6 interface counters for every subscriber session currently in progress	<code>show asngw-service statistics r6-only verbose</code>
Display R4/R6 Interface Counters for a Specific Subscriber	
View R4/R6 interface counters for a specific subscriber	<code>show asngw-service session counters msid <i>msid_number</i></code>
View Mobile IP Foreign Agent Statistics	
Display Mobile IP FA Information for a Specific Subscriber	
View Mobile IP FA counters for a specific subscriber	<code>show mipfa full username <i>subscriber_name</i></code>
Display Mobile IP Statistics for FA Services	
View statistics for a specific FA service	<code>show mipfa statistics fa-service <i>service_name</i></code>
Display Mobile IP FA Counters	

To do this:	Enter this command:
View Mobile IP FA counters for individual subscriber sessions	show mipfa counters
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 <i>subscriber_name</i>
Display Mobile IP Statistics for HA Services	
View Mobile IP statistics for a specific HA service	show mipha statistics ha-service <i>service_name</i>
Display Mobile IP HA Counters	
View Mobile IP HA counters for individual subscriber sessions	show mipha counters
View DHCP Information and Counters	
Display DHCP Counter Information	
View DHCP counter information for a specific DHCP service	show dhcp dhcp-service <i>svc_name</i>
View DHCP counter information for a specific DHCP user	show dhcp counter user-address <i>address</i>
Display DHCP Server Statistics	
View the status of the DHCP servers.	show dhcp statistics
Display DHCP Status	
View the status of the DHCP servers.	show dhcp status
View AAA and RADIUS Counters	
Display Local AAA Counters	
View local AAA counters for the current context	show aaa local counters
Display RADIUS Server States	
 Important: These commands can display 10 state transition histories of RADIUS accounting and authentication servers (Active/Not responding/Down States). For a complete explanation of RADIUS server states, refer AAA Interface Administration and Reference.	
View RADIUS accounting server states	show radius accounting servers detail
View RADIUS authentication server states	show radius authentication servers detail

To do this:	Enter this command:
Display RADIUS Server Group Server States	
 Important: RADIUS Server Group functionality is a license-controlled feature. You must install a valid feature license prior to configuring a RADIUS group for AAA functionality. If you have not previously purchased this enhanced feature, contact your sales representative for more information. For a complete explanation of RADIUS server states, refer AAA Interface Administration and Reference.	
View RADIUS authentication server group server states for a specific group	<code>show radius authentication servers radius group <i>group_name</i> detail</code>
View RADIUS accounting server group server states for a specific group	<code>show radius accounting servers radius group <i>group_name</i> detail</code>
Display RADIUS Protocol Counters	
View cumulative RADIUS protocol counters	<code>show radius counters all</code>
View RADIUS protocol counter summary of RADIUS authentication and accounting	<code>show radius counters summary</code>

Clearing Statistics and Counters

You may have to periodically clear statistics and counters in order to gather new information. The system can clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Use the CLI **clear** command to clear statistics and counters. Refer to the Command Line Reference for detailed information.

Chapter 12

Troubleshooting the ASN Gateway Service

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during system operation.

The following topics are discussed:

- [Verifying Network Connectivity](#)
- [Using the System's Diagnostic Utilities](#)

Verifying Network Connectivity

The system supports several commands that you can use to verify and troubleshoot network connectivity. Note that you cannot test network connectivity until system interfaces and ports have been configured and bound.

Issue the commands specified in this section on a context-by-context basis. Contexts act like virtual private networks (VPNs) in that they operate independent of the others. Therefore, ports, interfaces, and routes configured in one context can not be tested from another without additional configuration.

To switch between contexts you must enter the following command at the root prompt for the Exec mode:

```
context context_name
```

context_name is the name of the context that you wish to switch to. The following prompt appears:

```
[context_name]host_name#
```

Using the Ping Command

Use the **ping** command to verify the system's ability to communicate with a remote node in the network by passing data packets and measuring the response. This command is useful in verifying network routing and whether a remote node responds at the IP layer. The command has the following syntax:

```
ping host_ip_address [count num_packets] [pattern packet_pattern] [size
octet_count] [src {src_host_name | src_host_ip_address}]
```

Keyword/Variable	Description
<i>host_ip_address</i>	Identifies the remote node which is the target of the ping command. <i>host_ip_address</i> specifies the remote node using the node's assigned IP address specified with standard IPv4.
count <i>num_packets</i>	Specifies the number of packets to send to the remote host for verification. <i>num_packets</i> must be within the range 1 through 10000. The default is 5.
pattern <i>packet_pattern</i>	Specifies a pattern to use to fill the internet control message protocol packets. Specify <i>packet_pattern</i> in hexadecimal format in the range 0x0000 through 0xFFFF. Begin <i>packet_pattern</i> with a 0x followed by up to 4 hexadecimal digits. The default is that each octet of the packet is encoded with the octet number of the packet.
size <i>octet_count</i>	Specifies the number of bytes each IP datagram. <i>octet_count</i> must be in the range 40 through 18432. The default is 56.

Keyword/Variable	Description
src { <i>src_host_name</i> <i>src_host_ip_address</i> }	Specifies an IP address to use in the packets as the source node. <i>src_host_name</i> : Specifies the source node using the node's logical host name which must be resolved via DNS lookup. <i>src_host_ip_address</i> : Specifies the source node using the node's assigned IP address specified using the standard IPv4. The default is the IP address of the interface through which the ping was issued.

The following figure displays a sample of a successful response to this command's output.

```

PING 192.168.250.1 (192.168.250.1): 56 data bytes

64 bytes from 192.168.250.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 192.168.250.1: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 192.168.250.1: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.250.1: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 192.168.250.1: icmp_seq=4 ttl=255 time=0.2 ms
--- 192.168.250.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms

```

If no response is received from the target, follow these troubleshooting procedures:

- Verify that you entered the correct IP address.
- Attempt to ping a different device on the same network. If the ping is successful it is likely that your system configuration is correct. Verify that the device you are attempting to ping is powered and functioning properly.
- Use the information in the System Administration Guide to verify that the port is operational.
- Verify that your configuration of the ports and interfaces within the context are correct. Refer to the information in *Service Configuration Procedures* of this reference.
- If your configuration is correct and you have access to the device that you're attempting to ping, ping the system from that device.
- If there is still no response, it is likely that the packets are getting discarded by a network device. Use the **traceroute** and **show ip static-route** commands discussed in this chapter to further troubleshoot the issue.

Using the Traceroute Command

The **traceroute** command collects information on the data's route to a specified host. Use this troubleshooting command to identify the source of significant packet delays or packet loss on the network. You can also use this command to identify bottle necks in the routing of data over the network.

The command has the following syntax:

```
traceroute {host_name | host_ip_address} [count packets] [df] [maxttl
max_ttl] [minttl min_ttl] [port port_number] [size octet_count] [src
{src_host_name | src_host_ip_address} ] [timeout seconds]
```

Keyword/Variable	Description
<i>host_name</i>	Identifies the remote node to trace the route to. <i>host_name</i> specifies the remote node using the node's logical host name to be resolved via DNS lookup.
<i>host_ip_address</i>	Identifies the remote node to trace the route to by the IP address. <i>host_ip_address</i> specifies the remote node using the node's assigned IP address specified using the standard IPv4.
count	Specifies the number of UDP probe packets to send. The default is 3.
df	Specifies to not fragment the packets for the tracing of the route. If a packet requires fragmenting it is dropped and the ICMP response "Unreachable, Needs Fragmentation" is received.
maxttl <i>max_ttl</i>	Specifies the maximum time to live (TTL), in seconds, for the route tracing packets. Specify <i>max_ttl</i> in the range of 1 through 255. It is an error if <i>max_ttl</i> is less than <i>min_ttl</i> whether <i>min_ttl</i> is specified or defaulted. The time to live is the number of hops through the network; it is not a measure of time. The default maximum TTL is 30 seconds.
minttl <i>min_ttl</i>	Specifies the minimum time to live, in seconds, for the route tracing packets. Specify <i>min_ttl</i> in the range of 1 through 255. It is an error if <i>min_ttl</i> is greater than <i>max_ttl</i> whether <i>max_ttl</i> is specified or defaulted. The time to live is the number of hops through the network; it is not a measure of time. The default minimum TTL is 1 second.
port <i>port_number</i>	Specifies a specific port to connect to where <i>port_number</i> is a value of 1 through 65535. The default port is 33434.
size	Specifies the number of bytes each packet. Specify <i>octet_count</i> as a value of 40 through 32768. The default is 40.
src { <i>src_host_name</i> <i>src_host_ip_address</i> }	Specifies an IP address to use in the packets as the source node. <i>src_host_name</i> : Specifies the remote node using the node's logical host name which must be resolved via DNS lookup. <i>src_host_ip_address</i> : Specifies the remote node using the node's assigned IP address specified with standard IPv4. The default is the IP address of the interface through which the ping was issued.
timeout <i>seconds</i>	Specifies the maximum time to wait for a response from each route tracing packet. <i>seconds</i> must be a value in the range 2 through 100. The default is 5.

The following displays a sample of this command's output.

```
traceroute to 192.168.250.1 (192.168.250.1), 30 hops max, 40 byte packets
1 192.168.250.1 (192.168.250.1) 0.446 ms 0.235 ms 0.178 ms
```

Viewing IP Routes

You can view route information to a specific node or for an entire context. Use this information to verify network connectivity and to ensure the efficiency of the network connection. The command has the following syntax:

```
show ip route [route_ip_address [route_gw_address]]
```

Keyword/Variable	Description
<i>route_ip_address</i>	Specifies the IP address of a network node for which route information is displayed.
<i>route_gw_address</i>	Specifies the IP address of the gateway router between the system and the network node for which route information is displayed. This is an optional keyword.

If you do not specify keywords, all IP routes within the context's routing table are displayed.

The following displays a sample of this command's output showing a context's routing table.

```
"*" indicates the Best or Used route.

Destination Nexthop Protocol Prec Cost Interface
*0.0.0.0/0 10.0.4.1 static 0 0 SPIO1
*10.0.4.0/24 0.0.0.0 kernel 0 0 SPIO1
*10.0.4.0/32 0.0.0.0 kernel 0 0 SPIO1
*10.0.4.3/32 0.0.0.0 kernel 0 0 SPIO1
*10.0.4.255/32 0.0.0.0 kernel 0 0 SPIO1
```

Viewing the Address Resolution Protocol Table

You can view Address Resolution Protocol (ARP) table information to a specific node or for an entire context. Use this information to verify that when the system sends an ARP packet, it receives valid responses from other network nodes. The command has the following syntax:

```
show ip arp [arp_ip_address]
```

arp_ip_address specifies a specific network node for which to display ARP information. If you do not specify this keyword, all entries within the context's ARP table are displayed.



Important: When the VPN Manager restarts, it removes all interfaces from the kernel. The kernel removes all ARP entries. When this occurs, the NPU still holds all of the ARP entries so that there is no traffic disruption. From a user's point of view, **show ip arp** is broken since this command gathers information from the kernel and not the NPU.

The following displays a sample of this command's output showing a context's ARP table.

```
Flags codes:

C - Completed, M - Permanent, P - Published, ! - Not answered

T - has requested trailers

Address Link Type Link Address Flags Mask Interface

10.0.4.240 ether 00:05:47:02:20:20 C SPI01

10.0.4.7 ether 00:05:47:02:03:36 C SPI01

10.0.4.1 ether 00:01:30:F2:7F:00 C SPI01
```

Using the DHCP Test Command

Use this command to test the system's ability to communicate with a Dynamic Host Control Protocol (DHCP) server. Perform testing on a per-DHCP service basis for a specific server or all servers the DHCP service is configured to communicate with. This functionality is useful for troubleshooting or monitoring.

Once executed, the test attempts to obtain an IP address from the DHCP server(s) and immediately release it.



Important: Execute this command from within the context in which at least one GGSN service is configured.

The command has the following syntax:

```
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

Keyword/Variable	Description
dhcp-service <i>svc_name</i>	The name of the DHCP service. For <i>svc_name</i> , use from 1 to 63 alpha and/or numeric characters. Case sensitive.
all	Tests DHCP functionality for all servers.
server <i>ip_address</i>	Tests DHCP functionality for the server.

The following displays a sample of this command's output showing a successful DHCP test for a DHCP service called DHCP-Gi to a server with an IP address of 192.168.16.2. The IP address provided during the test was 192.168.16.144.

```
DHCP test status for service <DHCP-Gi>:

Server address: 192.168.16.2 Status: Tested
```



```
Lease address: 192.168.16.144 Lease Duration: 600 secs.
```

Using the System's Diagnostic Utilities

You can use the system's protocol monitor and test utilities to troubleshoot or verify configurations. The information generated by these utilities can in many cases either identify the root cause of a software or network configuration issue or, at the very least, greatly reduce the number of possibilities.

This section contains information and instructions for using these utilities.

Using the Monitor Utility

For troubleshooting purposes, the system provides a powerful protocol monitoring utility. Use this tool to display protocol information for a particular subscriber session or for every session being processed.



Caution: Use the monitor tool for troubleshooting only. The monitor tool is intrusive in that it may cause session processing delays and/or data loss.

Using the Protocol Monitor

The system's protocol monitor displays information for every session that is currently being processed. Depending on the number of protocols you are monitoring and the number of sessions in progress, a significant amount of data is generated. It is highly recommended that you enable logging on your terminal client to capture all the generated information.

Follow the instructions in this section to invoke and configure the protocol monitoring tool.

Step 1 Invoke the protocol monitor by entering the following command:

```
monitor protocol
```

The following output is displayed.

```
MONITOR GLOBAL PROTOCOLS:
```

```
11 - SNMP 21 - L2TP (Admin only)
12 - RADIUS Authentication (Admin only) 22 - L2TPMGR (Admin only)
13 - RADIUS Accounting (Admin only) 23 - L2TP Data (Admin only)
```

```

14 - A11 (R-P Interface) (Admin only) 24 - GTPC (Admin only)
15 - Mobile IPv4 (Admin only) 25 - GTPCMGR (Admin only)
16 - A11MGR (Admin only) 26 - GTPU (Admin only)
17 - PPP (Admin only) 27 - GTPP (Admin only)
18 - A10 (Admin only) 28 - DHCP (Admin only)
19 - User L3 (Admin only) 29 - GCDR (Admin only)
31 - RADIUS COA (Admin only)
32 - MIP Tunnel (Admin only)
33 - L3 Tunnel (Admin only)
34 - CSS Data (Admin only) 35 - CSS Signaling (Admin only)
36 - EC Diameter (Admin only)
37 - SIP (IMS) (Admin only)
38 - IPSec IKE Only (Admin only)
39 - IPSec Data Header (Admin only)
41 - IPSG RADIUS Signal (Admin only)
42 - ROHC (Admin only)
43 - WiMAX R6 (Admin only)
44 - WiMAX Data (Admin only)
45 - SRP (Admin only)
46 - BCMCS SERV AUTH (Admin only)
98 - GSS GCDR (Admin only) 99 - Geog Red (Admin only)

(B)egin Protocol Decoding, (Q)uit, <ESC> Prev Menu

```

- Step 2** At the Select: prompt, choose the protocol that you wish to monitor by entering menu number associated with the protocol: 11 through 19 and 21 through 28. A greater-than sign (>) appears next to the protocol you selected.
- Step 3** Repeat *step 2* as needed to choose multiple protocols.
- Step 4** Press B to begin the protocol monitor. If you selected any protocol other than 11 (SNMP), the following message is displayed:

```

WARNING!!! You have selected options that can DISRUPT USER SERVICE

Existing CALLS MAY BE DROPPED and/or new CALLS MAY FAIL!!!

```

(Under heavy call load, some debugging output may not be displayed)
 Proceed? - Select (Y)es or (N)o

Step 5 Enter Y to proceed with the monitor or N to go back to the previous menu.

```
C - Control Events (ON )
D - Data Events (ON )
E - EventID Info (ON )
I - Inbound Events (ON )
O - Outbound Events (ON )
S - Sender Info (OFF)
T - Timestamps (ON )
X - PDU Hexdump (OFF)
A - PDU Hex/Ascii (OFF)
+/- Verbosity Level ( 1)
L - Limit Context (OFF)
M - Match Newcalls (ON )
R - RADIUS Dict (no-override)G - GTPP Dict (no-override)
Q)uit, <ENTER> Display Options, <ESC> Prev Menu, <SPACE> Pause
```

Step 6 Configure the amount of information that is displayed by the monitor. To enable or disable options, enter the menu letter associated with that option. To increase or decrease the verbosity, use the plus (+) or minus (-) keys.
 The current state, ON (enabled) or OFF (disabled), is shown to the right of each option.

Step 7 Press the Enter key to refresh the screen and begin monitoring.
 The following displays a sample of the monitor protocol output with verbosity level 2.

```
*** Verbosity Level ( 2) ***
INBOUND>>>> 04:39:58:808 Eventid:47000(3)
GTPC Rx PDU, from 192.168.35.3:2123 to 192.168.35.1:2123 (190)
TEID: 0x00000000, Message type: GTP_CREATE_PDP_CONTEXT_REQ_MSG (0x10)
INFORMATION ELEMENTS FOLLOW:
IMSI: 40427000000001
```

ROUTING AREA IDENTITY (RAI) FOLLOWS:

MCC: 333

MNC: 444

LAC:0

RAC:0

ROUTING AREA IDENTITY (RAI) ENDS:

Recovery: 0x01 (1)

Selection Mode: 0x1 (MS provided APN, subscription not verified(Sent by MS))

Tunnel ID Data I: 0x00000400

Tunnel ID Control I: 0x00000400 NSAPI: 0x05 (5)

Charging Characteristics: 0x0800 (Normal)

End User Address: Organisation=IETF, PDP Type=IPv4, Address=10.0.0.1

Access Point Name: cisco.com

PROTOCOL CONFIG. OPTIONS FOLLOW:

Protocol id: 0xC021 (LCP)

Protocol length: 0x0E (14)

Protocol contents: 0103000E05063D38509B0304C023

Protocol id: 0xC021 (LCP)

Protocol length: 0x0E (14)

Protocol contents: 0203000E05063D38509B0304C023

Protocol id: 0xC023 (PAP)

Protocol length: 0x12 (18)

Protocol contents: 01040012086E626E73757365720461626364

PROTOCOL CONFIG. OPTIONS END.

GSN Address I: 0xC0A82303 (192.168.35.3)

GSN Address II: 0xC0A82303 (192.168.35.3)

MSISDN: 9876543210

QOS Profile: 0x0122720D7396404886074048

```
USER LOCATION INFORMATION: 111-22-33333-44444

IMEI (SV) : 8888888866666622

INFORMATION ELEMENTS END.
```

The monitor remains active until disabled. To quit the protocol monitor and return to the prompt, press q.

Using the Protocol Monitor for a Specific Subscriber

You can use the system's protocol monitor to display information for a specific subscriber session currently being processed. Depending on the number of protocols you are monitoring and the number of sessions in progress, a significant amount of data is generated. It is highly recommended that you enable logging on your terminal client in order to capture all of the generated information.

Follow the instructions in this section to invoke and configure the protocol monitoring tool for a specific subscriber session.

- To invoke the session-specific protocol monitor enter the following command:

```
monitor subscriber
```

The following screen is displayed:

```
MONITOR SUBSCRIBER:

1) By MSID/IMSI/MSISDN
2) By Username
3) By Callid
4) By IP Address
5) By IPv6 Address
6) Next-Call
Q) Quit

<ESC> Return to Previous Menu Select:
```

Menu Selection	Description
1) By MSID/IMSI	Specifies that the monitor is executed for a subscriber with a specific mobile station identification (MSID) number or International Mobile Subscriber Identity (IMSI) number. When prompted, enter up to a 15 digit MSID or IMSI number.
2) By Username	Specifies that the monitor is executed for a subscriber with a specific username. When prompted, enter the specific username to monitor. The username must be a string of 1 to 127 alpha and/or numeric characters.

Menu Selection	Description
3) By Callid	Specifies that the monitor is executed for a subscriber with a specific call identification number (callid). When prompted, enter the specific call identification number to monitor. The callid must be an 8-byte Hexadecimal number.
4) By IP Address	Specifies that the monitor is executed for a subscriber with a specific IPv4 address. When prompted, enter the specific IPv4 address that you wish to monitor.
5) By IPv6 Address	Specifies that the monitor is executed for a subscriber with a specific IPv6 address. When prompted, enter the specific IPv6 address that you wish to monitor.
6) Next-Call	Monitor the next call made to the system across all active services.

- Enter 1 through 5 from the menu to specify the method to use to select the subscriber to monitor.
- Enter the information for the selected menu item.

If no session matching the specified criteria was being processed when the monitor was invoked, the following output is displayed:

```

NO MATCHING CALL - waiting for a matching call to connect...

C - Control Events (ON ) 11 - PPP (ON ) 21 - L2TP (ON )
D - Data Events (ON ) 12 - A11 (ON ) 22 - L2TPMGR (OFF)
E - EventID Info (ON ) 13 - RADIUS Auth (ON ) 23 - L2TP Data (OFF)
I - Inbound Events (ON ) 14 - RADIUS Acct (ON ) 24 - GTPC (ON )
O - Outbound Events (ON ) 15 - Mobile IPv4 (ON ) 25 - GTPCMGR (OFF)
S - Sender Info (OFF) 16 - A11MGR (OFF) 26 - GTPU (OFF)
T - Timestamps (ON ) 17 - SESSMGR (ON ) 27 - GTPP (ON )
X - PDU Hexdump (OFF) 18 - A10 (OFF) 28 - DHCP (ON )
A - PDU Hex/Ascii (OFF) 19 - User L3 (OFF) 29 - GCDR (ON )
+/- Verbosity Level ( 1) 31 - Radius COA (ON )
L - Limit Context (OFF) 32 - MIP Tunnel (ON )
M - Match Newcalls (ON ) 33 - L3 Tunnel (OFF)
R - RADIUS Dict: (no-override) 34 - CSS Data (OFF)
G - GTPP Dict: (no-override) 35 - CSS Signal (OFF)
Y - Multi-Call Trace (OFF) 36 - EC Diameter (ON )
37 - SIP (IMS) (OFF)

```

41 - IPSG RADIUS (OFF)

(Q)uit, <ESC> Prev Menu, <SPACE> Pause, <ENTER> Re-Display Options

- Configure the amount of information that is to be displayed by the monitor. To enable or disable options, enter the menu letter associated with that option. To increase or decrease the verbosity, use the plus (+) or minus (-) keys.

The current state, ON (enabled) or OFF (disabled), is shown to the right of each option.



Important: Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the “Next-Call” option. It allows you monitor up to 11 primary PDP contexts for a single subscriber.

- Repeat *step 4* as needed to enable or disable options.
- Choose the protocols that you wish to monitor by entering the menu number associated with the protocol: 11 through 19 or 21 through 23.

The current state, ON (enabled) or OFF (disabled), is shown to the right of each protocol.

- Repeat *step 6* as needed to enable or disable multiple protocols.
- Press the Enter key to update the menu screen

The following displays a portion of a sample of the monitor's output for a subscriber named user2@aaa. The default protocols were monitored.

```
-----
--
Incoming Call:-----
-----

MSID: 0000012345 Callid: 002dc6c2
Username: user2@aaa SessionType: unknown
Status: Active Service Name: xxx1
Src Context: source Dest Context:
-----
--

<<<<OUTBOUND 10:02:35:415 Eventid:25001(0)

PPP Tx PDU (9)

PAP 9: Auth-Ack(1), Msg=

<<<<OUTBOUND 10:02:35:416 Eventid:25001(0)

PPP Tx PDU (14)

IPCP 14: Conf-Req(1), IP-Addr=192.168.250.70
```



```

<<<<OUTBOUND 10:02:35:416 Eventid:25001(0)

PPP Tx PDU (27)

CCP 27: Conf-Req(1), MPPC, Stac-LZS, Deflate, MVRCA

INBOUND>>>>> 10:02:35:517 Eventid:25000(0)

PPP Rx PDU (30)

IPCP 30: Conf-Req(1), IP-Comp VJ-Comp, IP-Addr=0.0.0.0, Pri-DNS=0.0.0.0,
Sec-DNS=0.0.0.0

<<<<OUTBOUND 10:02:35:517 Eventid:25001(0)

PPP Tx PDU (26)

IPCP 26: Conf-Rej(1), IP-Comp VJ-Comp, Pri-DNS=0.0.0.0, Sec-DNS=0.0.0.0

INBOUND>>>>> 10:02:35:517 Eventid:25000(0)

PPP Rx PDU (12)

IPCP 12: Conf-Ack(1), IP-Addr=192.168.250.70

INBOUND>>>>> 10:02:35:518 Eventid:25000(0)

PPP Rx PDU (31)

LCP 31: Prot-Rej(1), Rejected-Protocol=CCP (0x80fd)

INBOUND>>>>> 10:02:35:518 Eventid:25000(0)

PPP Rx PDU (12)

IPCP 12: Conf-Req(2), IP-Addr=0.0.0.0

<<<<OUTBOUND 10:02:35:518 Eventid:25001(0)

PPP Tx PDU (14)

IPCP 14: Conf-Nak(2), IP-Addr=192.168.250.87

INBOUND>>>>> 10:02:35:519 Eventid:25000(0)

PPP Rx PDU (12)

IPCP 12: Conf-Req(3), IP-Addr=192.168.250.87

```


The monitor remains active until disabled. To quit the protocol monitor and return to the prompt, press q.

Using the RADIUS Testing Tools

You can use CLI commands to test the network connectivity and configuration of RADIUS authentication and accounting servers. This functionality is useful for determining the accuracy of the system's RADIUS configuration and the configuration of the subscriber profile on the RADIUS server, and for troubleshooting the server's response time.

Testing a RADIUS Authentication Server

When you test a RADIUS authentication server, the tool generates an authentication request message for a specific username.

 **Important:** The username must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool enter the following command:

```
radius test authentication { all | radius group group_name | server
server_name port server_port } user_name password
```

Keyword/Variable	Description
all	Specifies to test all configured RADIUS authentication servers.
radius group group_name	Specifies the configured RADIUS authentication servers in a RADIUS server group named group_name for server group functionality.
server_name	Specifies the IP address of a specific RADIUS authentication server to test.
server_port	Specifies the to test TCP port the system uses to communicate with the RADIUS authentication server.
user_name	Specifies a username that is supplied to the RADIUS server for authentication.
password	Specifies the password associated with the username that is supplied to the RADIUS server for authentication.

The following displays a sample of this command's output for a successful response when testing a RADIUS authentication server with an IP address of 192.168.250.150 on port 1812.


```
Authentication from authentication server 192.168.250.150, port 1812

Authentication Success: Access-Accept received

Round-trip time for response was 8.8 ms
```

Testing a RADIUS Accounting Server

Use the following command to test a RADIUS accounting server. The tool generates an accounting start/stop pair for a specific username.

 **Important:** The username must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, enter the following command:

```
radius test accounting { all | radius group group_name | server  
server_name port server_port } user_name
```

Keyword/Variable	Description
all	Specifies that all configured RADIUS accounting servers should be tested.
radius group <i>group_name</i>	Specifies the configured RADIUS authentication servers in a RADIUS server group named <i>group_name</i> for server group functionality.
<i>server_name</i>	Specifies the IP address of a specific RADIUS accounting server to test.
<i>server_port</i>	Specifies the TCP port over that the system should use when communicating with the RADIUS accounting server to test.
<i>user_name</i>	Specifies a username that is supplied to the RADIUS server for accounting.

The following displays a sample of this command's output for a successful response. A RADIUS accounting server with an IP address of 192.168.1.102 on port 1813 was tested.

```
RADIUS Start to accounting server 192.168.1.102, port 1813  
  
Accounting Success: response received  
  
Round-trip time for response was 554.6 ms  
  
RADIUS Stop to accounting server 192.168.1.102, port 1813  
  
Accounting Success: response received  
  
Round-trip time for response was 85.5 ms
```


Chapter 13

ASN Paging Controller and Location Registry Overview

The ASN Paging Controller and Location Registry (PC/LR) provides the paging and location update to WiMAX subscriber in IEEE 802.16 Mobile WiMAX radio access networks. This service can be used as a standalone product or in combination with ASN Gateway as co-located services on same chassis.

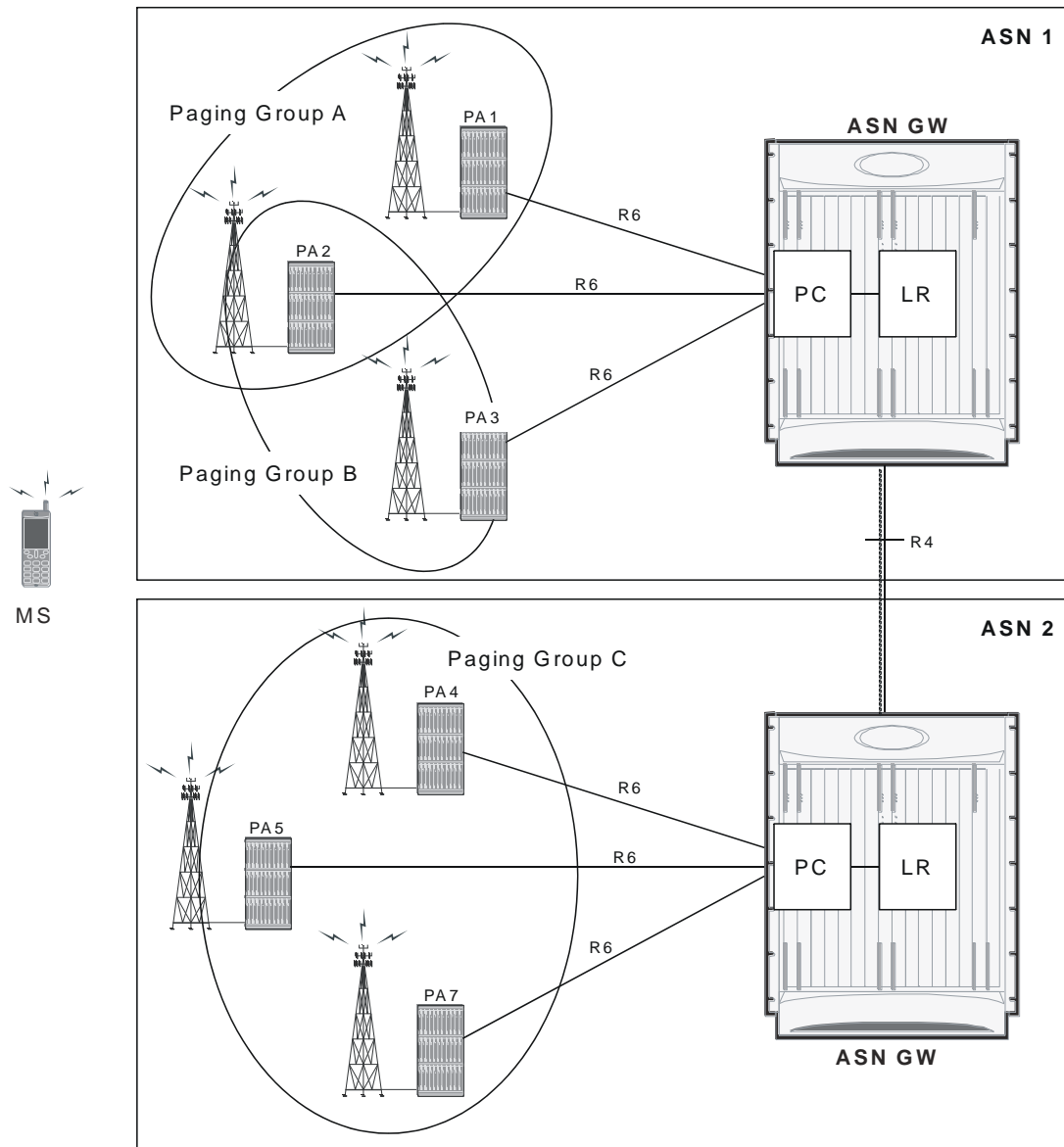
Introduction

ASN Paging Controller and Location Registry (PC/LR) supports connection management and mobility across cell sites and inter-service provider network boundaries by processing subscriber control and bearer data traffic.

Each ASN Gateway can concentrate traffic from many radio base stations. This reduces the required number of devices under management and minimizes connection set-up latency by decreasing the number of call hand-offs in the network.

Paging and Idle Mode Operation maintains a track and alert for MSs when they are in idle mode to save battery power. Paging is executed to alert MSs when there is an incoming message. Figure 8 illustrates the paging operation and paging and idle mode elements in the WiMAX network system.

Figure 47. ASN Paging Controller and Location Registry in WiMAX Networks



In WiMAX networks, a mobile station is tracked when it is in idle mode. The information is stored to a location register (LR). The tracking area is larger than the cell size because a paging group (PG) comprises multiple cells. When a mobile station moves across paging groups, its location is updated via R6 and/or R4. The paging controller (PG) in ASN-GW retrieves the location from the LR and alerts the paging agent in (PA) in the base station to signal to the mobile station.

Location information for idle mode subscribers is maintained in a location register central database that is co-located on an anchor paging controller. Idle mode can be initiated by the mobile device or the network. The paging controller retains subscriber session context information in addition to supervising paging activities. It also represents an authentication liaison between the user device and the AAA server. As the subscriber roams across cell sites, it is associated with a group of base stations known as a paging group. Location updates to the LR database are conveyed over R6 and R4 messages between the relay paging controller serving ASN and the A-PC/LR. When a remote host

attempts to reach an idle mode subscriber device, the anchor paging controller alerts the paging group members when it receives downlink traffic by requesting the paging agent in the base station to signal the idle mode subscriber.

Description of PC/LR Support

The PC/LR runs as a stand-alone function in a separate chassis or as an integrated service on same chassis as the Anchor Authenticator (A-PC)/Anchor Datapath (A-DP) ASN Gateway. The idle mode LR database uses distributed software architecture and provides an LR manager task that partitions smaller database volumes across separately running session manager tasks in the system. The implementation is based on a topologically unaware paging scheme in which the A-PC does not have global awareness of all member base stations in a paging group. The A-PC uses a single-step paging operation where paging notifications are sent to the last-reported serving paging controller or directly attached base station.

Idle mode operation is very important in order for any cellular system to keep the mobile device reachable when it is inactive. It enables mobility in addition to conserving battery life. Idle mode paging also eliminates the requirements of independent VLRs/HLRs, when it is supported as an integrated function in the ASN Gateway system.

Licenses

The ASN PC/LR service is a separate product from the ASN Gateway. You must purchase the WiMAX Paging Controller/Location Register product license separately to enable this service.

Paging and Location Update Procedures

This section provides an overview of the ASN Gateway's paging and location update procedures.

The system provides following components for the paging controller, paging group and location registry functionality.

Paging Controller (PC)

The paging controller is a functional entity that administers the activity of idle mode mobile stations in the network. It is identified by PC ID, which maps to the address of a functional entity in a WiMAX network. In this implementation, the PC is co-located with ASN Gateway. There are two types of PCs:

- **Anchor PC:** For each idle mode MS, there is a single anchor PC that contains the updated location information of the MS.
- **Relay PC:** There are one or more other PCs in the network, called relay PCs, that participate in relaying paging and location management messages between the paging agent and the anchor PC.

Paging Agent (PA)

The paging agent is a functional entity, implemented in an ASN base station, that handles the interaction between PC- and paging-related functionality.

Paging Group (PG)

A paging group is a logical entity comprising one or more paging agents. A paging group resides entirely within a NAP boundary. Paging groups are managed by the network management system and provisioned per the access network operator's provisioning requirements.

Location Register (LR)

A location register is a distributed database, with each instance corresponding to an anchor PC. Location registers contain information about idle mode MSs. The information for each MS includes:

- MS paging information: Information about each MS that has registered in the past in the network but is currently in idle mode
- Current paging group ID (PGID)
- PAGING_CYCLE
- PAGING_OFFSET
- Last reported BSID
- Last reported relay PCID
- MS service flow Information comprising
 - Idle mode retention information for each MS in idle mode
 - Information about the service flows associated with the MS

An instance of a location register is associated with every anchor PC.

Paging Controller and Location Update functionality supports following operation and procedures in ASN Gateway:

[Location Update Procedure](#)

[Location Update with Paging Controller Relocation](#)

[Paging Operation](#)

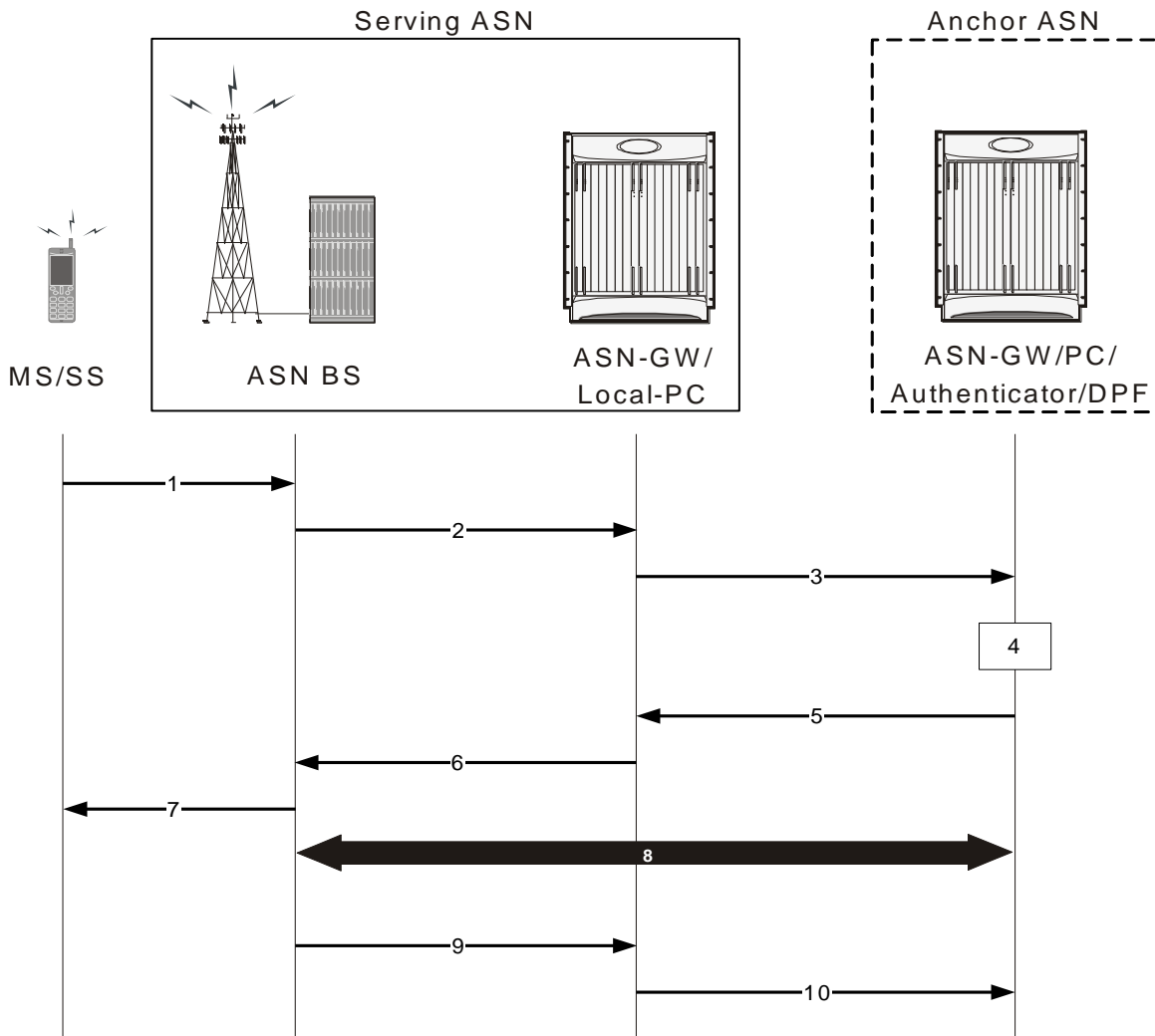
[MS Initiated Idle Mode Entry](#)

[MS Initiated Idle Mode Exit](#)

Location Update Procedure

This section describes the secure location update procedure for a WiMAX MS.

The following figure and table provides a high-level view of the steps involved in a secure location update.

Figure 48. Location Update Flow**Table 36. Location Update Procedure Flow Description**

Step	Description
1	The MS initiates a secure Location Update procedure by sending a RNG-REQ message to Serving ASN BS, which includes the Ranging Purpose Indication TLV set to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor ASN Gateway acting as the Anchor PC function for the MS, and the HMAC/CMAC tuple.
2	The serving ASN BS sends an R6 LU_Req message to the serving ASN Gateway and starts timer TR6_LU_Req. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving ASN BS proposes an update to these parameters.
3	The Serving ASN Gateway (associated with the local Paging Controller) sends an R4 LU_Req message to the Anchor PC (associated with Anchor ASN Gateway) and starts timer TR6_LU_Req. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the Serving ASN Gateway proposes an update to these parameters. Note: This message may be relayed by several intermittent ASNs before reaching the Anchor PC (Anchor ASN Gateway).

Step	Description
4	If the Anchor PC retains context information for the MS including its Authenticator ID, the Anchor PC initiates a Context Request procedure with the Anchor Authenticator/ASN Gateway. If the Anchor Authenticator/ASN Gateway has valid key material for the MS, it returns AK context for the MS to the Anchor PC.
5	Upon successful retrieval of the AK context, the Anchor PC sends an R4 LU_Rsp message back to the Serving ASN Gateway and starts timer TR4_LU_Conf. The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Anchor PC ID TLVs, and Location Update Status TLV set to Accept. Upon receipt of the R4 LU_Rsp message, Serving ASN Gateway stops timer TR4_LU_Req.
6	Upon receipt of the R4 LU_Rsp message, the Serving ASN Gateway stops timer TR4_LU_Req, sends an R6 LU_Rsp message to the Serving ASN BS, and starts timer TR6_LU_Conf. The message includes the Location Update Status TLV set to Accept, AK Context TLVs, as well as the assigned Paging Information TLV if they were included in the corresponding R4 message.
7	Based on the AK and AK context received from the Anchor PC, the Serving BS (associated with Local PC/Relay PC in Serving ASN Gateway) successfully authenticates the RNG_REQ message received from the MS and sends a RNG_RSP message with HMAC/CMAC and Successful LU_Rsp indication to the MS.
8	The Serving ASN BS initiates an R6 CMAC Key Count Update procedure with the ASN Gateway. The Serving ASN Gateway initiates an R4 CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key Count.
9	The Serving ASN BS sends an R6 LU_Cnf message to the serving ASN Gateway with Location Update TLV indicating success. Upon receipt of the message, the serving ASN Gateway stops timer TR6_LU_Conf.
10	The Serving ASN Gateway sends an R4 LU_Cnf message with a successful LU indication to the Anchor PC and stops timer TR6_LU_Req. Upon receipt of the message, the Anchor PC updates the LR with MS Idle Mode information and stops timer TR4_LU_Conf.

Location Update with Paging Controller Relocation

This section describes the secure location update with PC relocation procedure for a WiMAX MS.

The following figure and table provides a high-level view of the steps involved in a secure location update with PC relocation.

Table 37. Location Update with PC Relocation - Procedure Flow

Step	Description
1	The MS initiates a secure Location Update procedure by sending a RNG-REQ message to the Serving ASN BS, which includes the Ranging Purpose Indication TLV set to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor ASN Gateway acting as the Anchor PC function for the MS, and the HMAC/CMAC tuple.
2	The serving BS sends an R6 LU_Req message to the serving ASN Gateway and starts timer TR6_LU_Req. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS proposes an update to these parameters.
3	The Serving ASN Gateway (associated with the serving BS and local PC) sends an R4 LU_Req message to the Anchor PC ASN associated and starts timer TR4_LU_Req. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the Serving ASN proposes an update to these parameters. Note that this message may be relayed by several intermittent ASNs before reaching the current Anchor PC ASN. The Serving ASN or any intermittent ASN along the path may request PC relocation.

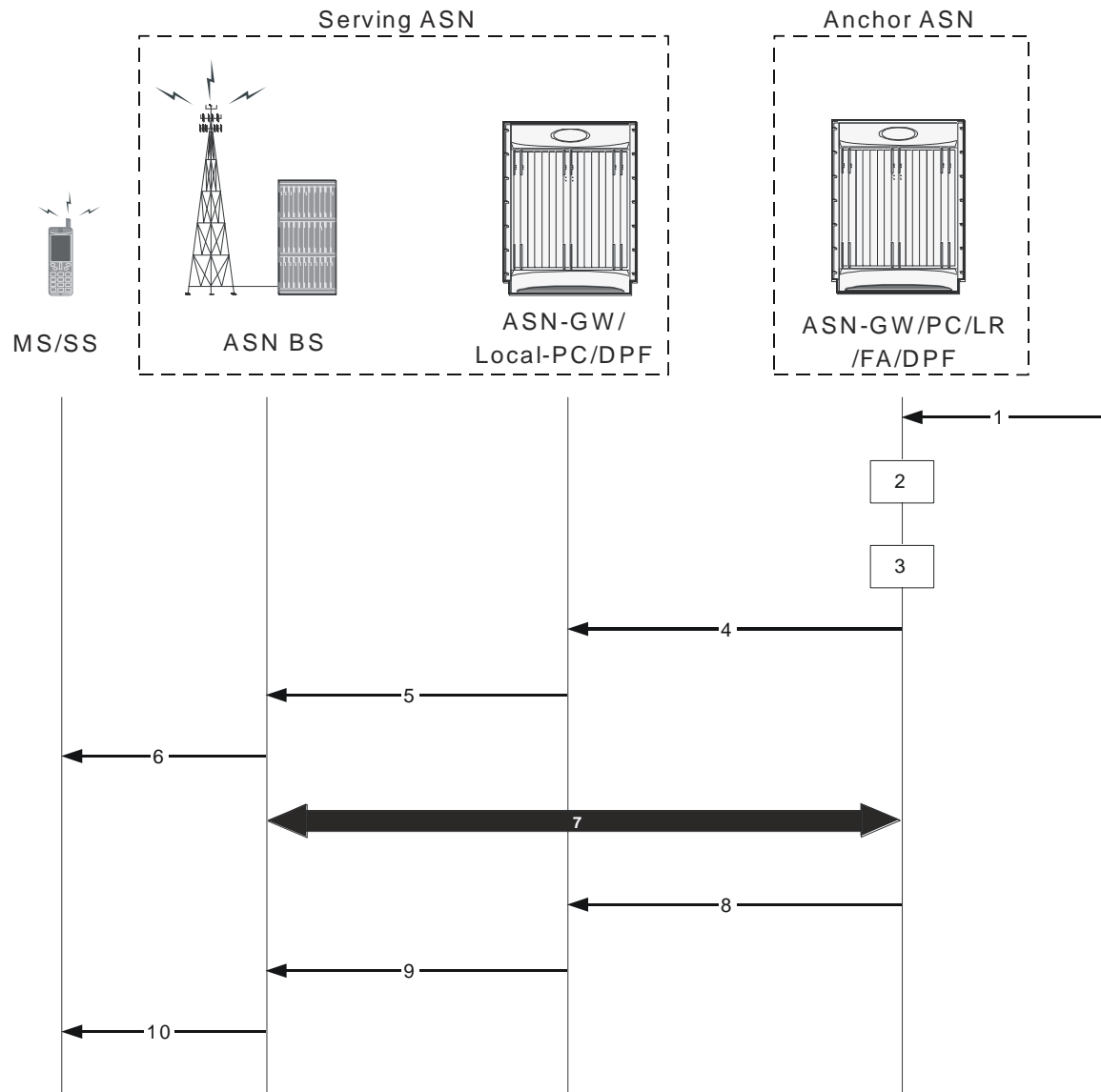
Step	Description
4	Upon receipt of the R4 LU_Req message, a relay PC ASN adds the Anchor PC Relocation Destination TLV to initiate PC relocation to. The message is forwarded to the Anchor PC ASN. New Anchor PC ASN starts timer TR4_LU_Request.
5	Refer to section 4.13 for the call flow. If the current Anchor PC ASN retains context information for the MS, including its Authenticator ID, the current Anchor PC ASN initiates a Context Request procedure with the Anchor Authenticator ASN. If the Anchor Authenticator ASN has valid key material for the MS, it returns AK context for the MS to the Anchor PC ASN.
6	The current Anchor PC ASN sends an R4 LU_Rsp message back to the new Anchor PC ASN and starts timer TR4_LU_Conf. The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Anchor PC ID TLVs, and Location Update Status TLV set to Accept. The Anchor PC Relocation Request Response TLV is set to Accept to indicate that the Current Anchor PC ASN accepted the PC_Relocation_Req and the Anchor PC ID TLV is set to the identifier of New Anchor PC ASN ID which was received in the Anchor PC Relocation Destination TLV in the R4 LU_Req message. The R4 LU_Rsp message also includes MS Info TLV containing MS context for transfer to the new Anchor PC ASN. If the new Anchor PC ASN does not request PC Relocation, the current Anchor PC MAY still request to perform the procedure by including the PC Relocation Indication TLV. If the new Anchor PC does not accept the relocation, it reports a failure in step 17.
7	Upon receipt of the R4 LU_Rsp message from current Anchor PC ASN, new Anchor PC ASN stops timer TR4_LU_Req, stores the MS context received from current Anchor PC ASN, updates the Paging Information (Paging Group ID, Paging Cycle, Paging Offset), forwards the R4 LU_Rsp message on to the Serving ASN, and starts timer TR4_LU_Conf.
8	Upon receipt of the R4 LU_Rsp message, the Serving ASN-GW stops timer TR4_LU_Req, sends an R6 LU_Rsp message to the S-BS, and starts timer TR6_LU_Conf. The message includes the Location Update Status TLV set to Accept, MS Info, AK Context, Anchor PC ID, and old Anchor PC ID TLV. The message may include the paging Information TLV if they were included in the corresponding R4 message.
9	Based on the AK and AK context received from the current Anchor PC, the Serving BS (associated with Local PC/Relay PC) successfully authenticates the RNG_REQ message received from the MS. The serving BS sends a RNG_RSP message with HMAC/CMAC and Successful Location Update Response indication to the MS.
10	The Serving BS sends an R6 LU_Cnf message to the serving ASN-GW with Location Update TLV indicating success. Upon receipt of the message, the serving ASN-GW stops timer TR6_LU_Conf.
11	The Serving ASN sends an R4 LU_Cnf message with a successful LU indication to new Anchor PC ASN (as indicated by the Anchor PC ID received from the BS) and stops timer TR6_LU_Req. Alternatively, the Relay PC ASN forwards LU_Cnf to the ASN associated with new Anchor PC with the result indication reassigned by Relay PC. Upon receipt of the message, new Anchor PC ASN stops timer TR4_LU_Conf.
12	Upon receipt of the LU_Cnf message, the new Anchor PC ASN sends an R4 PC_Relocation_Ind to the Anchor DP/FA ASN, and starts timer TR4_PC_Reloc_Upd_ADP.
13	The Anchor DP/FA ASN updates the Anchor PC for the MS with the new Anchor PC ASN ID and responds with an R4 PC_Relocation_Ack message confirming the Anchor PC update. Upon receipt of the message, the new Anchor PC ASN stops timer TR4_PC_Reloc_Upd_ADP. The new Anchor PC ASN hosts the Anchor PC function and becomes the new current Anchor PC ASN for the MS. The Anchor PC is de-allocated from the old current Anchor PC ASN.
14	Simultaneous with sending PC_Relocation_Ind to Anchor DP/FA, the new Anchor PC sends an R4 PC Relocation Indication to Anchor Authenticator ASN to inform the change of the Anchor PC, and starts timer TR4-PC_Reloc_Upd_AA.
15	The Anchor Authenticator ASN updates the Anchor PC for the MS with the New Anchor PC ASN ID and responds with an R4 PC_Relocation_Ack message confirming the Anchor PC update. Upon receipt of the message, the New Anchor PC ASN stops timer TR4-PC_Reloc_Upd_AA. At this point, New Anchor PC ASN hosts the Anchor PC function and becomes the new Current Anchor PC ASN for the MS. The Anchor PC is de-allocated from the old Current Anchor PC ASN.

Step	Description
16	The new Anchor PC ASN sends an R4 LU_Cnf message with a successful LU indication to the current Anchor PC ASN and stops timer TR4_LU_Conf. The old current Anchor PC ASN clears its LR context for the MS.
17	This step is optional. If Anchor PC ASN receives CMAC Key Count TLV update in LU_Cnf message, it should perform an R4 CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key Count. Refer to section 4.13 for the call flow.

Paging Operation

This section describes the paging operation for a WiMAX MS.

The following figure and table provides a high-level view of the steps involved in the paging operation call flow of an MS.

Figure 49. Paging Operation Procedure Flow**Table 38. Paging Operation Procedure Flow Description**

Step	Description
1	Data from HA arrives through the tunnel at the FA and its associated DPF. The Anchor DPF buffers the data.
2	Anchor Data Path Function (DPF) sends an R4 Initiate_Paging_Req message to Anchor PC/LR to request paging. Optionally the R4 Initiate_Paging_Req message contains the QoS parameters of the flow for which the data arrived at the Anchor DPF. This helps set priority treatment of the Paging operation based on the QoS parameters and flow types. The Anchor DPF may have policies for triggering paging based on the QoS parameters for the data received. The Anchor DP Function starts timer TInit_Page_Req. Note: When MS is in Idle Mode, if data not belonging to any saved Service Flow (SF) of the MS arrives, the decision to initiate paging or not is on the basis of operator's setting.

Step	Description
3	Anchor PC/LR retrieves the information related to the MS and sends an R4 Initiate_Paging_Rsp to Anchor Data Path function. This message indicates whether the MS context as contained in the PC/LR is correct and the requested paging action is authorized. Exclusion of the Response Code TLV indicates intent to page the MS. Upon receipt of this message the Anchor DP Function starts timer TInit_Page_Req if running.
4	If paging action is authorized, Anchor PC retrieves the MS paging information and constructs Paging_Announce message. The Anchor PC issues one or more Paging_Announce messages based on its knowledge of the Paging Region topology as shown in sections XXXXX. The Anchor PC starts a timer TR4_Paging_Announce when it sends out the first Paging_Announce message and waits for the paging response. The Anchor PC sets a paging re-transmission counter <i>N</i> . If the Anchor PC does not receive a paging response, it retransmits the Paging_Announce message prior to the expiration of the timer TR4_Paging_Announce. If the Anchor PC is topologically aware of the defined Paging Group (PG), including the last BS from which the MS performed location update, the Anchor PC directly issues Paging_Announce messages to all or some subset of the Paging Group members. The members consist of BSs and/or relay PCs in the region. If the Anchor PC is topologically unaware of the Paging region or the BSs defined in the Paging group, the Paging_Announce messages are sent to the known Relay PC(s). The Relay PC(s) forwards the announce message to one or more BSs in the Paging region.
5	The ASN Gateway that contains the local/relay PC function for the MS initiates the paging operation and sends the R6 Paging_Announce message to the BS(s) associated with the Paging Group ID (PGID) received in R4 Paging_Announce. The ASN Gateway performs single- or multi-step paging based on whether the BS ID TLV or the L-BSID TLV is present. Associated with each R4 Paging_Announce message, the ASN Gateway starts timer TR6_Paging_Announce.
6	Once the Paging Agent (PA) at the BS receives the Paging_Announce message with the requested action set to Start, it extracts the relevant paging parameters for the MS (Paging Cycle, Paging Offset). It then initiates the paging action requested by sending out MOB-PAG_ADV message over the airlink as per the indicated paging cycle and the paging offset. The optional SF Flow info in the message helps the BS implement a paging priority scheme for faster call setup when bandwidth is constrained or for resource allocation. The PA continues to page the MS for the duration specified by the Paging Announce Timer TLV, until the appropriate response is received from the MS, or a stop page indication is received from the Local PC.
7	Upon being successfully paged the MS performs a Idle Mode Exit or a Location Update procedure. If any Paging Agent (PA) receives a successful reply from the paged MS, the Paging Agent notifies the Local PC by sending a R6 LU_Req message in the case of Network Initiated location update or R6 IM_Exit_State_Change_Req message in the case of data delivery to MS in idle mode. Upon receipt of a such a message the Local PC stops timer TR6_Paging_Announce if running, and sends the appropriate R4 LU_Req or R4 IM_Exit_State_Change_Req message to the Anchor PC. Upon receipt of such a message, the Anchor PC stops timer TR4_Paging_Announce, if running. The Anchor PC also initiate stop paging procedures as described at step 8 and onward.
8	Upon receipt of a response from the MS as mentioned at step 7, and Anchor PC wants to initiate stop paging procedure, the Anchor PC sends a R4 Paging_Announce message to all BSs in the PG. The R4 Paging_Announce message has the Paging Start/Stop TLV set to 0.
9	The Local PC sends a R6 Paging_Announce message to the BSs. The R6 Paging_Announce message has the Paging Start/Stop TLV set to 0.
10	Upon receipt of the R6 Paging_Announce message with Paging Start/Stop = 0, the BS terminate/cease a MOB_PAG-ADV messages over the air.

MS Initiated Idle Mode Entry

This section describes the MS-initiated idle mode entry procedure for a WiMAX subscriber.

The following figure and table provides a high-level view of the steps involved in MS-initiated idle mode entry call flow of an SS/MS.

Figure 50. MS Initiated Idle Mode Entry Procedure Flow

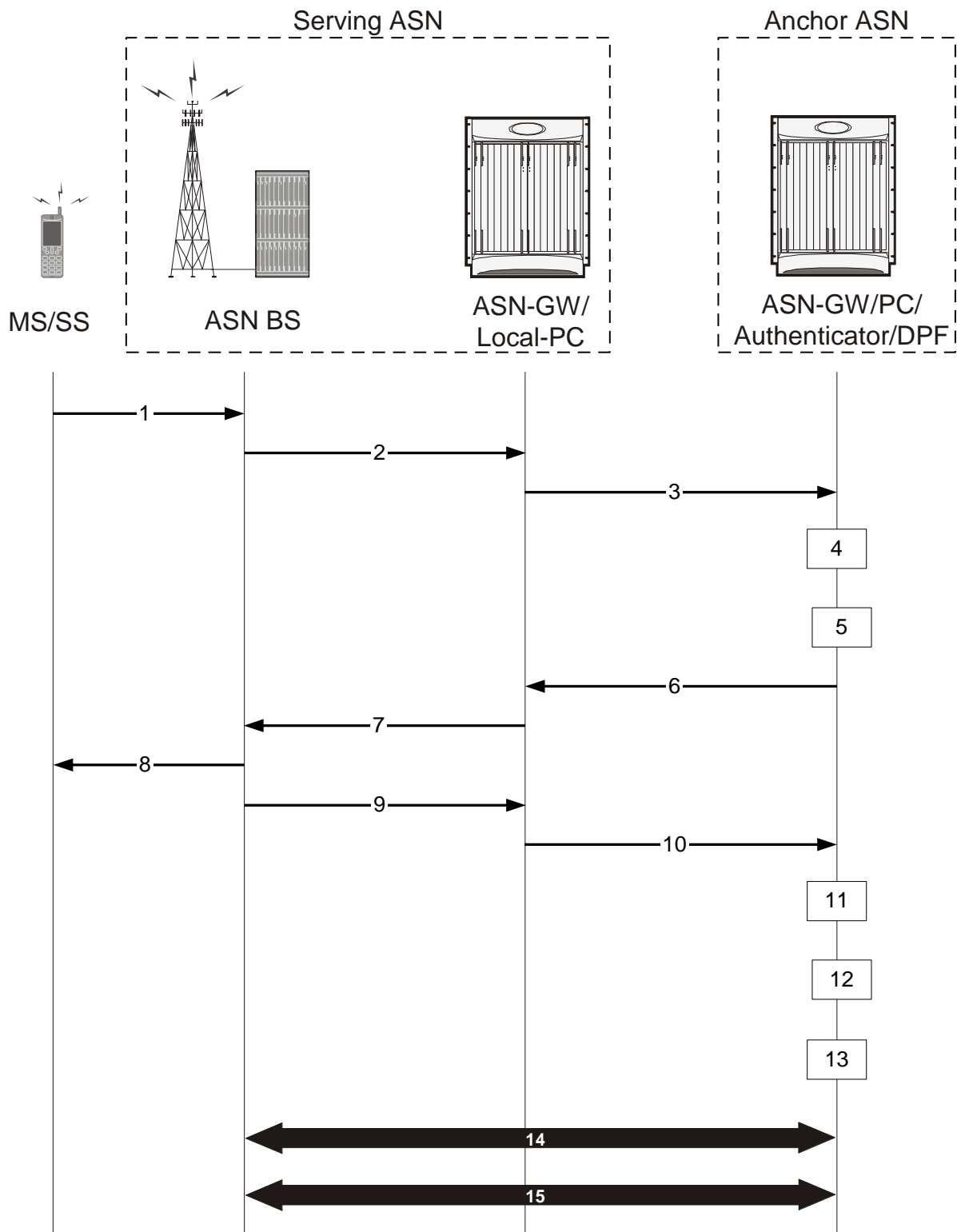


Table 39. MS Initiated Idle Mode Entry Procedure Flow Description

Step	Description
1	MS decides to enter Idle Mode and sends DREG_REQ formatted as described in IEEE 802.16e. The De-Registration Request code is set to 0x01 indicating that the MS intends to enter Idle Mode.
2	Based on the MS's request, the serving ASN BS (Paging Agent) in Serving ASN sends an R6 IM_Entry_State_Change_Req message to its ASN Gateway. Timer TR4_IM_Entry_Req is started to monitor R6 IM_Entry_State_Change_Rsp at the serving ASN BS(PA).
3	The local Relay PC in Serving ASN Gateway chooses an Anchor PC for the MS and sends inter-ASN R4 IM_Entry_State_Change_Req message to the Anchor ASN associated with the chosen Anchor PC. Timer TR4_IM_Entry_Req_ASN is started to monitor the R4 IM_Entry_State_Change_Rsp.
4	The Anchor PC/LR, sends R4 IM_Entry_State_Change_Req to Anchor Authenticator to verify whether MS is allowed to go in to Idle mode. Timer TR4_IM_Entry_Req_APC is started at this time to monitor the R4 IM_Entry_State_Change_Rsp from the Anchor Authenticator. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN Gateway.
5	Anchor Authenticator checks if the MS is allowed to enter Idle Mode and saves necessary information if allowed, then sends back R4 IM_Entry_State_Change_Rsp to Anchor PC/LR including MSID, IDLE mode authorization indication. If Anchor Authenticator rejects the Idle mode entry request, the Idle Mode Authorization TLV contains the rejection code. When R4 IM_Entry_State_Change_Rsp for MS entering Idle Mode is send successfully, Anchor Authenticator stores Anchor PC ID for this MS. Upon reception of this message at Anchor PC, TR4_IM_Entry_Req_APC is stopped. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN Gateway.
6	According to the reported information in R4 IM_Entry_State_Change_Rsp, based on the content of Idle mode authorization indication IE, Anchor PC updates the LR with current MS location information (PGID) and other parameters, and sends back R4 IM_Entry_State_Change_Rsp message to the Serving ASN Gateway. When this message is received at serving ASN Gateway timer TR4_IM_Entry_Req_ASN is stopped.
7	Serving ASN Gateway forwards the R6 IM_Entry_State_Change_Rsp to serving BS (PA) including IDLE Mode authorization indication and accepted Paging parameters. Upon reception of this message at the BS, timer TR6_IM_Entry_Req is stopped.
8	Serving ASN BS sends DREG_CMD to the MS. The DREG_CMD conveys "PC ID" field pointing to Anchor PC for the MS and allocated Idle mode parameters.
9	After sending the DREG_CMD to the MS, the serving ASN BS(PA) acknowledges the successful delivery of DREG_CMD to the local Relay PC in serving ASN Gateway by sending R6 IM_Entry_State_Change_Ack.
10, 11	The local Relay PC in serving ASN Gateway forwards the successful entry of MS in to Idle mode to the Anchor PC in Anchor ASN Gateway by sending R4 IM_Entry_State_Change_Ack. Upon reception of this message at Anchor PC, timer TR4_IM_Entry_Rsp is stopped.
12	Anchor ASN Gateway associated with Anchor PC/LR updates the information of MS into LR database and sends Anchor PC Indication message to Anchor DPF/FA to reflect the success of MS entering Idle Mode. Timer TR4_APC_Ind is started at this time when Anchor PC Indication is send, to monitor the response.
13	The Anchor DPF/FA finally updates the information of MS including the Anchor PC ID of this MS and acknowledges to the Anchor PC/LR by Anchor PC Ack message. When Anchor PC Ack is received at Anchor ASN Gateway timer TR4_APC_Ind is stopped.
14	After the expiration of the Management Resource Holding Timer (an 802.16e parameter), serving BS initiates the related R6 data Path Dereg procedure by sending R6 Path_Dereg_Req to the Anchor ASN Gateway.

Step	Description
15	Serving ASN Gateway completes the data path de-registration from its side and send R4 Path_Dereg_Ack to Anchor DPF/FA. Upon reception of this message Anchor ASN Gateway stops timer TPath_Dereg_Rsp_ADPF and serving BS(PA) updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN Gateway as per the CMAC Key count update procedure. The Anchor Authenticator acknowledges the CMAC update for the MS. Optionally this procedure may be invoked anytime after step 11.

MS Initiated Idle Mode Exit

This section describes the MS-initiated idle mode exit procedure for a WiMAX subscriber.

The following figure and table provides a high-level view of the steps involved in MS- initiated idle mode exit call flow of an SS/MS.

Figure 51. MS Initiated Idle Mode Exit Procedure Flow

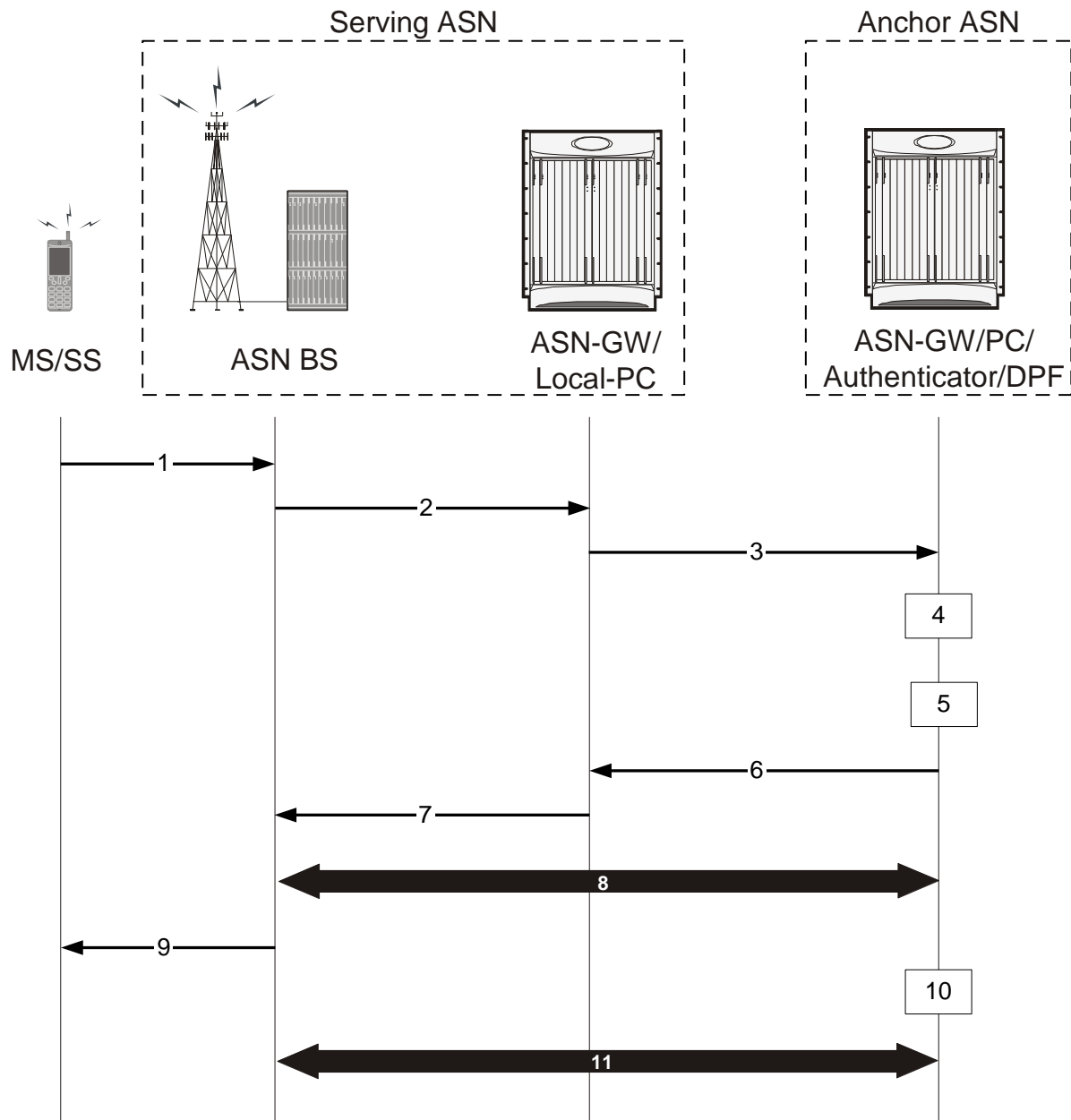


Table 40. MS Initiated Idle Mode Exit Procedure Flow Description

Step	Description
1	MS initiates exit procedure from IDLE mode and sends RNG_REQ to serving ASN BS. The Ranging Purpose Indication TLV is set to one and PC ID TLV is included, thus indicating that the MS intends to Re-Entry from Idle Mode.

Step	Description
2	The ASN BS receives the RNG_REQ message from MS indicating Idle mode exit and sends R6 IM_Exit_State_Change_Req to the Relay PC in the ASN Gateway, indicating that the MS wants to become active. Timer TR6_IM_Exit_Ctx_Req is started at this point by the BS to monitor the response for this message.
3	The Relay PC in the Serving ASN Gateway receives the R6 IM_Exit_State_Change_Req from the BS indicating Idle mode exit and sends R4 IM_Exit_State_Change_Req to the Anchor PC/LR in Anchor ASN Gateway, indicating that the MS wants to become active. Timer TR4_IM_Exit_Ctx_Req is started at this point by the Anchor ASN Gateway to monitor the response for this message. In the event that the relay PC is the anchor PC, this step is not required.
4	On receiving the R4 IM_Exit_State_Change_Req, the Anchor PC/LR proceeds to request the security context from the Anchor Authenticator in Anchor ASN Gateway using the R4 IM_Exit_State_Change_Req. Timer TR4_IMexit_ctx_req_PC is started at this point by the Anchor PC to monitor the response for this message. This step is optional if the Anchor Authenticator and Anchor PC/LR are co-located in the same ASN Gateway.
5	Anchor Authenticator responds with the security context back to the Anchor PC/LR with R4 IM_Exit_State_Change_Rsp message. Once the Anchor PC receives this message, Timer TIM_Exit_Ctx_Req_PC is stopped. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN Gateway.
6	Anchor PC/LR, sends R4 IM_Exit_State_Change_Rsp to the Relay PC. Once the relay PC receives this message, Timer TR4_IM_Exit_Ctx_Req is stopped. R4 IM_Exit_State_Change_Rsp contains the stored information for the MS at the Anchor PC.
7	Serving ASN Gateway retrieves the MS context from Anchor PC ASN and forwards the MS context to the serving BS on the R6 interface. Once the BS receives this message, Timer TR6_IM_Exit_Ctx_Req is stopped. The AK fetched from the authenticator is used to verify the RNG-REQ.
8	After successful authentication, the BS starts data path establishment across the serving BS, Serving ASN Gateway, Relay PC, Anchor PC, Authenticator, and DPF.
9	Serving BS uses MS service and operational information indicated by IDLE Mode Retain Info obtained by Step 7 to construct HO Process Optimization TLV settings in the RNG-RSP based on local policy; then sends RNG_RSP message to the MS formatted according to IEEE 802.16e specification. This message delivers all the required information to resume service in accordance with Idle Mode Retain Information.
10	When R4 Path_Reg_Ack is received at Anchor DPF, the Data Path function associated with FA sends a Delete_MS_Entry_Req message to PC/LR in order to delete the Idle mode entry associated with the MS. If MS is exiting Idle mode due to a network initiated Idle mode exit, the PC/LR will cease all Paging Announce operations.
11	The serving BS updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN Gateway. The Anchor Authenticator acknowledges the CMAC update for the MS.


Supported Platforms and Software

ASN PC-LR is available for all chassis running StarOS Release 8.0 or later.

Chapter 14

ASN PC/LR Service Configuration

This chapter provides configuration information for the ASN Paging Controller and Location Registry service.

 **Important:** Refer to the Command Line Interface Reference for information about commands in this chapter. Not all commands are available on all platforms.

Since each wireless network is unique, the system is designed with a variety of parameters for various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Refer to the Command Line Interface Reference for optional configuration commands specific to the WiMAX product.

This chapter includes the following:

- [Configuring the ASN PC_LR Services](#)
- [Configuring Bulk Statistics Schema](#)
- [Save the Configuration](#)
- [Managing Your Configuration](#)
- [Gathering ASN PC_LR Statistics](#)

Configuring the ASN PC/LR Services

This section provides basic configuration examples to create and configure a paging controller and location registry (ASN PC/LR) service in single chassis.

Overview

- Configure initial configuration parameters by applying the example configuration in the *Initial Configuration* section.
- Optional. Configure the ASN Gateway service within the newly created ASN Gateway service by applying the example configuration in the *ASN Gateway Configuration* chapter.
- Create ASN PC and LR service within the context by applying the example configuration in the *Creating the PC and LR Service* section.
- Configure the timeout duration for idle mode and paging announcements in newly created ASN PC and LR services by applying the example configuration in the *Configuring the PC and LR Service* section.
- Optional. Configure log system activity by applying the example configuration in the *ASN PC/LR Logging Configuration* section of this chapter.
- If they are not configured in ASN Gateway service, add basic subscribers to the system by applying the example configuration in the *Subscriber Configuration* section.
- Save the configuration by applying the example configuration in the *Save the Configuration* section of this chapter.

Initial Configuration

- Step 1** Specify the role of the processing cards in the chassis. The following example activates two processing cards, placing one in active mode and labeling the other as redundant:

```
configure
  card slot_number
    redundancy card-mode
  exit
  card slot_number
    mode active psc      end
```

- Step 2** Set local system management parameters.

The following example sets the default subscriber and RADIUS group in the local context:

```
configure
  context local      interface interface_name
    ip address ip_address ip_mask
    exit
  server ftpd
    exit
  server telnetd
    exit
  subscriber default
    exit
  aaa group default
    exit
    administrator name encrypted password password ftp
    ip route ip_addr ip_mask next_hop_addr local_context_interface
    _name
  exit
  port ethernet slot#/port#
  no shutdown
  bind interface local_context_interface_name local
  exit
end
```

Step 3 Create the context where the service will reside.

The following example creates the VPN context and interface and binds the VPN interface to a configured Ethernet port.

```
configure
  context context_name -noconfirm
    interface interface_name
```

```

        ip address address

        exit

    subscriber default

        exit

    ip route 0.0.0.0 0.0.0.0 next_hop_address vpn_interface_name

    exit

    port ethernet slot_number/port_number

        no shutdown

        bind interface vpn_interface_name vpn_context_name

    end

```

Step 4 Create the service within the newly created context.

The following configuration example creates the ASN PC/LR service:

```

configure

    context context_name

        asnpc-service service_name -noconfirm

    end

```

Creating the PC and LR Service

The following example creates the ASN PC and LR service with identifier and bind this service to an IP address for idle mode entry and location update for WiMAX subscriber:

```

configure

    context context_name

        asnpc-service asn_pc_lr_svc_name

        asnpc-id mac_address

        bind-address ip_address max-subscribers sessions]

        ip local-port port_num

    end

```

Configuring the PC and LR Service

The following example configures the timeout ASN PC and LR service behavior for idle mode entry and location update:

```
configure
  context context_name
    asnpc-service asn_pc_lr_svc_name
      idle-mode timeout duration
      max-retransmission retry
      paging-announce timeout duration
      retransmission-timeout duration
    end
```

Subscriber Configuration

The following example configures local subscribers for ASN Gateway and ASN PC/LR service:

```
configure
  context context_name
    subscriber name user_name
      password password
    exit
  subscriber name user_name
    password password
  exit
  subscriber name user_name
    password password
  exit
end
```

ASN PC/LR Logging Configuration

The following example configures logging for the ASN PC/LR services:

```
logging active
logging filter active facility vpn level debug
logging filter active facility sessctrl level debug
logging filter active facility sessmgr level debug
logging filter active facility asnpcmgr level debug
logging filter active facility wimax-r6 level debug
```

Configuring Bulk Statistics Schema

The following example enables the bulk statistics schema for the Personal Stateful Firewall service on a chassis:

```
configure
    bulktats mode
        context schema schema_name format format_string
    end
```



Important: To configure the various parameters for the Bulk Statistics collection, refer to the “Configuring and Maintaining Bulk Statistics” chapter in System Administration Guide prior to configuring these commands.


For more information on *format_string* variable, refer to the “Bulk Statistics Configuration Mode Commands” chapter in Command Line Interface Reference.

Save the Configuration

To save changes made to the system configuration for this service, refer to the “Saving Your Configuration” chapter in this guide.

Managing Your Configuration

This section explains how to display and review the configurations after you save them in a .cfg file. Refer to the “Saving Your Configuration” chapter of this guide. This section also describes how to retrieve errors and warnings within an active configuration for a service.

 **Important:** All commands listed here are under Exec mode. Not all commands are available on all platforms.

Output descriptions for most of the commands are described in the Command Line Interface Reference.

Table 41. System Status and ASN Gateway Service Monitoring Commands

To do this:	Enter this command:
View Administrative Information	
Display Current Administrative User Access	
View a list of all administrative users currently logged on to the system	<code>show administrators</code>
View the context in which the administrative user is working, the IP address from which the administrative user is accessing the CLI, and a system generated ID number	<code>show administrators session id</code>
View information pertaining to local-user administrative accounts configured for the system	<code>show local-user verbose</code>
View statistics for local-user administrative accounts	<code>show local-user statistics verbose</code>
View information pertaining to your CLI session	<code>show cli</code>
Determining the System's Uptime	
View the system's uptime (time since last reboot)	<code>show system uptime</code>
View the Status of Configured NTP Servers	
View the status of the configured NTP servers	<code>show ntp status</code>
View the Status of System Alarms	
View the status of the system's outstanding alarms	<code>show alarm outstanding all</code>
View detailed information about all currently outstanding alarms	<code>show alarm outstanding all verbose</code>
View system alarm statistics	<code>show alarm statistics</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>

To do this:	Enter this command:
View information for a specific subscriber	<code>show subscribers full username</code>
View the ASN PC/LR Related Information	
Display System Configuration	
View the configuration of a context	<code>show configuration context <i>name</i></code>
View configuration errors for ASN PC/LR service	<code>show configuration errors section asnpc-service [verbose] [{grep <i>grep_options</i> more}]</code>
Display ASN PC session	
View all active ASN PC subscriber session	<code>show asnpc-service session full all</code>
View all ASN PC session counters	<code>show asnpc-service session counters all</code>
View ASN PC statistics	<code>show asnpc-service session statistics verbose</code>

Gathering ASN PC/LR Statistics

Use the commands listed below to gather statistics for ASN PC/LR services.


 **Important:** All commands listed here are under Exec mode. For more information on these commands, refer to the “Executive Mode Commands” chapter in the Command Line Interface Reference.

Table 42. Gathering Statistics

Statistics Wanted	Action to Perform	Information to Look For
Active ASN PC/LR service session related statistics on a chassis.	At the Exec Mode prompt, enter the following command: show asngw-service session full	The output of this command displays the statistics about the ASN PC/LR service session in a system/service.
Detailed disconnect reasons for an ASN PC/LR session.	At the Exec Mode prompt, enter the following command: show session disconnect-reasons	The output of this command displays the disconnect reasons ASN PC/LR service session in a system/service.
Detailed statistics of ASN PC/LR services.	At the Exec Mode prompt, enter the following command: show asngw-service statistics	The output of this command displays the detailed statistics ASN PC/LR service in a system/service.

Appendix A

Engineering Rules

This section provides engineering rules and guidelines to consider before you configure the system for your network deployment.

Interface and Port Rules

The rules discussed in this section pertain to the Ethernet 10/100 and Ethernet 1000 Line Cards and the type of interfaces they facilitate, regardless of the application.

R6 Interface Rules

The following engineering rules apply to the R6 interface:

- An R6 interface is created once the IP address of a logical interface is bound to an ASN Gateway service.
- Configure the logical interface(s) that will facilitate the R6 interface(s) within an ingress context.
- Configure ASN Gateway services within an ingress context.
- Bind at least one ASN Gateway service to each interface. However, you can bind multiple ASN Gateway services to a single interface if secondary addresses are assigned to the interface.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the R6 interface can be limited.

Connectivity Service Network (CSN) Interface Rules

The following engineering rules apply to the interface to the connectivity service network (CSN):

- Configure the logical interfaces that will be used to facilitate the CSN interface within the egress context. The default is to use a single interface within the egress context to facilitate the CSN interface.
- You can configure multiple interfaces in the egress context by using static routes or dynamic routing protocols.
- You can optionally configure next-hop gateways.

FA to HA R3 Interface Rules

For Mobile IP support, you can configure the system to perform the role of an FA, an HA, or both. This section describes the engineering rules for the R3 interface when you use the system as an FA.

The following engineering rules apply to the R3 interface between the FA and HA:

- An R3 interface is created once the IP address of a logical interface is bound to an FA service.
- Configure the logical interface(s) that will be used to facilitate the R3 interface(s) within the egress context.

- Configure FA services within the egress context.
- Configure each FA service with the Security Parameter Index (SPI) of the HA it will be communicating with over the R3 interface. The SPI configuration is applicable if the use of static keys is forced.
- You can configure multiple SPIs within the FA service to allow communications with multiple HAs over the R3 interface. The SPI configuration is applicable if the use of static keys is forced. It is best to define SPIs with a net mask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the R3 interface can be limited.

HA to FA R3 Interface Rules

The following engineering rules apply to the R3 interface between the HA and FA. For Mobile IP support, you can configure the system to perform the role of a FA, an HA or both. This section describes the engineering rules for the R3 interface when using the system as an HA.

- An R3 interface is created once the IP address of a logical interface is bound to an HA service.
- Configure the logical interface(s) that will be used to facilitate the R3 interface(s) within an ingress context.
- Configure HA services within an ingress context.
- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the R3 interface.
- You can configure multiple SPIs within the HA service to allow communications with multiple FAs over the R3 interface. The SPI configuration is applicable if the use of static keys is forced. Define SPIs with a net mask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Configure Each HA service with a Security Parameter Index (SPI) that it will share with mobile nodes. The SPI configuration is applicable if the use of static keys is forced.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the R3 interface can be limited in order to allow higher bandwidth per subscriber.

Subscriber Rules

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

- You can configure a maximum of 2,048 local subscribers per context.
- Configure default subscriber templates on a per-ASN Gateway or FA service basis.

Service Rules

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

- You can configure a maximum of 256 services (regardless of type) per system.



Caution: Large numbers of services greatly increase the complexity of management and may affect overall system performance. It is recommended that you configure a large number of services only if your application absolutely requires it. Please contact your local service representative for more information.

- Up to 2,048 MN-HA and 2048 FA-HA SPIs are supported for a single HA service.
- Up to 2,048 FA-HA SPIs are 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.
- Up to 10,000 LAC addresses can be configured per LNS service.
- It is not good practice to have service names identical to those configured in different contexts on the same system. Services with the same name can lead to confusion because of the difficulty in troubleshooting problems and understanding the output of show commands.

DHCP Service Engineering Rules

You can configure up to 20 DHCP servers per DHCP service.

Appendix B

MIP Timer Considerations

This appendix provides considerations for lifetime, idle, and absolute timer settings that you should understand when setting up a system in a Mobile IP environment. This section focuses on the call flow of the Mobile IP setup and provides an explanation of the timer values you must apply to make the system function most efficiently.

Call Flow Summary

The following steps describe the call flow in relation to the timers that affect a MIP call initiated from the mobile node.

- Step 1** The call arrives at the system and R6 is processed successfully.
- Step 2** PPP negotiation is started. At this point, since authentication is not performed, the system does not know the username or password. As a result, 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.
- Step 3** The system determines which FA service to use for the mobile IP session.
- Step 4** The system still does not know the username and password at this point, so it looks at the default subscriber profile. If the idle or absolute timeouts are configured, the system compares the settings for the idle and absolute timeout to the setting for the advertised registration lifetime in the FA-service.

Use the following CLI command sequences to set absolute and idle timeout for the default subscriber:

```
[local]host_name# config
[local] <host_name> (config)# context < context_name>
[ < context_name > ]< host_name > (config-ctx)# subscriber default
[ < context_name > ]< host_name > (config-subscriber)# timeout idle <
value >
[ < context_name > ] < host_name > (config-subscriber)# timeout absolute
< value >
```

In the above commands, the *context_name* variable represents the name of the source context on the system. The *value* variable is measured in seconds. Configure this value to be between 0 and 4294967295. Enter a value of 0 to disable the timer.

Use the following CLI command sequence to set FA agent reg-lifetime in the FA service:

```
[local] < host_name > # config
[local] < host_name > (config)# context context_name
[ < context_name > ]< host_name > (config-ctx)# fa-service <
fa_service_name >
[ < context_name > ] < host_name > (config-fa-service)# advertise reg-
lifetime < value >
```

In the above command, the *value* variable is measured in seconds. Configure this value to be between 1 and 65534.

- Step 5** The system prepares the Agent advertisement. To select the value of the registration lifetime, the system compares the configured agent registration lifetime in the FA service to the idle and absolute timeouts configured in the default subscriber profile in the source context. If the lifetime is lower, this value is used in the agent advertisement. If the idle timeout or absolute timeout is lower, the system sends the registration lifetime as 5 seconds less than the configured idle or absolute timeout. Note that if no idle or absolute timeout is configured, it defaults to off and the registration lifetime is sent.
- Step 6** After the system sends the agent advertisement, the mobile sends a registration request. The requested lifetime in the mobile request should be the lower of the values in its configured lifetime and the lifetime sent in the Agent advertisement.
- Step 7** When the FA receives the MIP RRQ, it authenticates the user. If the AAA returns a value for the subscriber idle timeout that is less than the lifetime in the MIP RRQ, the system sends a lifetime too long error code (Code: 0x45, Requested Lifetime Too Long). The system sends back a lifetime value equal to the configured subscriber idle timeout.
- Step 8** Assuming that the mobile can handle this error code, it adjusts the lifetime value to that sent by the system and send a new RRQ.
- Step 9** 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.

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

```
[local] < host_name > # config[local] < host_name > (config)# context <
host_name > [ha] < host_name > (config-ctx)# ha-service < ha_service_name
> [ha] < host_name > (config-ha-service)# reg-lifetime < value >
```

In the above command, the *value* variable is measured in seconds. Configure it to be a value between 1 and 65534.

Timer Values and Recommendations

The following table shows values that would be populated in the Mobile IP call flow under a number of different configured scenarios.

Table 43. Sample Mobile IP 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-Absolute	300	300	300	300	300	300	300
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:

- 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 subscriber, 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.
- The FA-service advertise reg-lifetime parameter should be configured to a value less than the source context default subscriber timeout idle parameter.

Failure to follow these recommendations could result in lifetime too long failures when the FA processes the subscriber profile 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 a per-domain (context) basis. However, you can have a domain-wide lifetime timer 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, 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.

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

```
[local] < host_name > # config

[local] < host_name > (config)# context < aaa_context_name >

[ < aaa_context_name > ] < host_name > (config-ctx)# subscriber default

[ < aaa_context_name > ] < host_name > (config-subscriber)# ip context-
name < abc >

[ < aaa_context_name > ] < host_name > (config-subscriber)# exit

[ < aaa_context_name > ] < host_name > (config-ctx)# subscriber name <
ptt.bigco.com >

[ < aaa_context_name > ] < host_name > (config-subscriber)# timeout idle
< 3605 >

[ < aaa_context_name > ] < host_name > (config-subscriber)# ip context-
name < abc >

[ < aaa_context_name > ] < host_name > (config-subscriber)# exit

[ < aaa_context_name > ] < host_name > (config-ctx)# subscriber name <
bigco.com >

[ < aaa_context_name > ] < host_name > (config-subscriber)# timeout idle
< 7205 >

[ < aaa_context_name > ] < host_name > (config-subscriber)# ip context-
name < abc >

[ < aaa_context_name > ] < host_name > (config-subscriber)# exit
```

```

[aaa_context_name]host_name(config-ctx)# domain ptt.bigco.com default
subscriber ptt.bigco.com

[aaa_context_name]host_name(config-ctx)# domain bigco.com default
subscriber bigco.com

[ < aaa_context_name > ] < host_name > (config-ctx)# end

[local] < host_name > # config

[local] < host_name > (config)# context < ha_context_name >

[ < ha_context_name > ] < host_name > (config-ctx)# subscriber default

[ < ha_context_name > ] < host_name > (config-subscriber)# exit

[ < ha_context_name > ] < host_name > (config-ctx)# ha-service ha

[ < ha_context_name > ] < host_name > (config-ha-service)# idle-timeout-
mode normal

[ < ha_context_name > ] < host_name > (config-ha-service)# reg-lifetime <
7200 >

[ < ha_context_name > ] < host_name > (config-ha-service)# exit

[ < ha_context_name > ] < host_name > (config-ctx)# end

[local] < host_name > # config

[local] < host_name > (config)# context < fa_context_name >

[ < fa_context_name > ] < host_name > (config-ctx)# fa-service < fa >

[ < fa_context_name > ] < host_name > (config-fa-service)# advertise reg-
lifetime < 7200 >

[ < fa_context_name > ] < host_name > (config-fa-service)# exit

```

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 one hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of two 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. This is because the configured value is less than the registration lifetime value configured for the Agent Advertisement. Five 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. This is 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 data and upon inter-ASN Gateway 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.

Appendix C

Supported Registration Reply Codes

Each of the three sections that follow describe the registration reply codes supported by the system for the ASN Gateway, FA, and HA services.

FA Service Reply Codes

The following registration reply codes are supported by the system's FA 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
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000

Table 44. Supported FA Service Registration Reply Codes

Reply Code (Hex / Base 10)	Description	Notes
40H / 64	Registration Denied - reason unspecified	Sent when internal errors are encountered when processing the Request packet.
41H / 65	Registration Denied - administratively prohibited	Sent when a newcall policy is set to reject calls or the subscriber is not permitted to use Mobile IP FA services.
42H / 66	Registration Denied - insufficient resources	Sent when no memory or session managers are available to process the session.
43H / 67	Registration Denied - mobile node failed authentication	Sent when the mobile node failed authentication.
44H / 68	Registration Denied - home agent failed authentication	Sent when an HA attempted to communicate with the FA service using an incorrect security parameter index (SPI).
45H / 69	Registration Denied - requested lifetime too long	Sent when the mobile node requests a registration lifetime longer than the maximum supported by the FA.
46H / 70	Registration Denied - poorly formed request	Sent when the registration request is poorly formed, such as missing an Authentication extension.
47H / 71	Registration Denied - poorly formed reply	Sent when the registration reply is poorly formed, such as missing an Authentication extension.
48H / 72	Registration Denied - requested encapsulation unavailable	Sent when requested encapsulation type is unavailable (GRE or minimal IP encapsulation).
4AH / 74	Registration Denied - reverse tunneling unavailable	Sent when reverse tunneling is requested by the mobile node but it is not enabled on the system.
4BH / 75	Registration Denied - reverse tunneling mandatory	Sent when reverse tunneling is enabled on the system but is not supported by the mobile node.
4CH / 76	Registration Denied - reverse tunneling mobile node too distant	Sent when IP TTL is not set to 255 in Reg Request with T bit set

Reply Code (Hex / Base 10)	Description	Notes
4DH / 77	Registration Denied - invalid care-of address	Sent when D bit is set in the Registration Request.
4EH / 78	Registration Denied - registration timeout	Sent when FA reg-timeout is exceeded.
4FH / 79	Registration Denied - reverse tunneling delivery style unavailable	Sent if the Encapsulating Delivery Style Extension sent by the mobile is not supported by the FA service.
50H / 80	Registration Denied - home network unreachable (ICMP error received)	Sent when the FA service can not contact the home network due to an Internet Control Message Protocol (ICMP) error.
51H / 81	Registration Denied - home agent host unreachable (ICMP error received)	Sent when the FA service can not contact the HA host due to an Internet Control Message Protocol (ICMP) error.
52H / 82	Registration Denied - home agent port unreachable (ICMP error received)	Sent when the FA service can not contact the HA port due to an Internet Control Message Protocol (ICMP) error.
58H / 88	Registration Denied - home agent unreachable (other ICMP error received)	Sent when the FA service can not contact the HA due to an Internet Control Message Protocol (ICMP) error.
60H / 96	Registration Denied - missing home address	Sent when the FA service could not determine the IP address of the mobile node.
61H / 97	Registration Denied - missing NAI	Sent when the FA service could not determine the subscriber's network access identifier.
62H / 98	Registration Denied - missing home agent	Sent when the FA service could not determine the IP address of the mobile node's home agent.
68H / 104	Registration Denied - unknown challenge	Sent if the FA cannot validate the Mobile IP mobile-to-foreign agent advertisement challenge extension provided in the Registration Request.
69H / 105	Registration Denied - missing challenge	Sent if the mobile node's Registration Request does not include a mobile-to-foreign agent advertisement challenge extension.
6AH / 106	Registration Denied - stale challenge	Sent when the mobile node has sent a Registration Request with a challenge value that was already used before.

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 45. 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.

Appendix D

Sample Configuration

This appendix contains sample configuration files for the ASN Gateway operating as an ASN Gateway for WiMAX subscribers with Proxy Mobile IP support, and ASN Paging Controller and Location Registry. Commented lines are labeled with the number symbol (#). Variables are identified with italics (*variable*).

ASN Gateway Configuration in Single Context (Simple IP)

This section provides the sample configuration to configure ASN Gateway service in a single context with Simple IP authentication.

```
config
  context local
    interface 24/1 broadcast
    ip address 10.1.15.82 255.255.255.0
    #exit
  subscriber default
  exit
  aaa group default
  #exit
  #exit
  context asngw_ingress_ctx
    interface 17/1
      ip address ip_address/mask
      ip address ip_address/mask secondary
      policy allow-static-allocation
    #exit
  subscriber default
  exit
  subscriber name wimax_subs1
    password password
    exit
  aaa group default
    radius attribute nas-ip-address address ip_address/mask
  radius server ip_address key secret_key port port_num
  radius accounting server ip_address key secret_key port port_num
```



```
#exit

asnwgw-service asn_svc_name authentication single-eap

bind address ip_address

#exit

    dhcp-service dhcp

bind address 172.20.1.9

    end
```

FA and HA Configuration with Mobile IP

```
config
  context local
    interface 24/1 broadcast
    ip address 10.1.15.82 255.255.255.0
  #exit
  subscriber default
  exit
  aaa group default
  #exit
#exit

  context asngw_ingress_ctx
  interface 17/1
    ip address ip_address/mask
    ip address ip_address/mask secondary
  #exit
  subscriber default
  exit
  subscriber name wimax_subs1
    password password
  ip context-name csn_egress_ctx
  exit
  aaa group default
    radius attribute nas-ip-address address ip_address/mask
    radius server ip_address key secret_key port port_num
    radius accounting server ip_address key secret_key port port_num
  #exit
```

```
fa-service fa
    fa-ha-spi remote-address ip_address spi-number spi secret key
    authentication mn-ha allow-noauth
    authentication aaa-distributed-mip-keys override
    proxy-mip allow
    bind address ip_address
#exit
asn-gw-service asn_svc_name
    authentication single-eap
    mobile-ip foreign-agent context mobileIP
    bind address ip_address
#exit
dhcp-service dhcp
    bind address asn_svc_name
end
config
    context csn_egress_ctx
        ip pool ip_pool_name ip_address/mask public 0
        ip pool ip_pool_name ip_address/mask static
        interface 18/1
            ip address ip_address/mask
        #exit
    interface 20/1
        ip address 192.168.1.10 255.255.255.0
    #exit
    subscriber default
    #exit
    ha-service ha
        mn-ha-spi spi-number spi encrypted secret key
```

```
fa-ha-spi remote-address ip_address spi-number spi secret key
authentication mn-aaa allow-noauth
authentication mn-ha allow-noauth
bind address ip_address
end
```


ASN Gateway Service QoS Configuration

This section provides the sample configuration to configure QoS for WiMAX subscriber in an ASN Gateway service.

```
config

context <csn_egress_ctx>

    class-map name classmap_name match-all
        match protocol protocol_name
    #exit

    class-map name classmap_name match-all
        match protocol protocol_name
        match ip-tos 255 ip-tos-mask 255
        match src-port-range port_start_range to port_end_range
        match dst-port-range port_start_range to port_end_range
        match dst-ip-address ip_address/mask
        match src-ip-address ip_address/mask
    class-map name classmap_name match-all
        match protocol protocol_name
    #exit

asn-service-profile id asn_prof_id direction bi-directional -no
    uplink-qos-id 1
    uplink-classifier class-map all-ipip
    downlink-qos-id 1
    downlink-classifier class-map all-ipip
#exit

asn-service-profile id asn_prof_id direction bi-directional -no
    uplink-qos-id 1
    uplink-classifier class-map all-tcp
    uplink-classifier class-map all-udp
```

```
downlink-qos-id 1

downlink-classifier class-map all-tcp

downlink-classifier class-map all-udp

#exit

asn-qos-descriptor id 1 -no

    global-service-class-name ABCDEF

    service-class-name StarentService

    schedule-type rt-vr min-reserved-traffic-rate 1 max-latency 2 unsolicited-
polling-interval 3 traffic-priority 6 max-sustained-traffic-rate 4 max-traffic-
burst 5

#exit

context aaa

subscriber default

    asn-pdfid 21 asn-service-profile-id 100 asn-sdfid 5

    asn-pdfid 22 asn-service-profile-id 101 asn-sdfid 6

end
```


ASN Gateway and ASN PC/LR Configuration

This section provides the sample configuration to configure ASN PC/LR and ASN Gateway service in a single chassis.

```
config
  context <context_name>
    asngw-service <asngw_svc_name>
      bind address <ip_address>
      authentication single-eap
      idle-mode timeout <timeout_dur>
      peer-asngw address <ip_address>
    exit
  asnpc-service <asnpc_svc_name>
    bind address <ip_address>
    paging-group id <paging_grp_id>
      paging-params cycle <cycle> offset <offset> interval <frames>
      paging-node id <MAC_address> address <ip_address>
      paging-node id <MAC_address> address <ip_address>
    exit
  exit
  subscriber default
    ip context-name <dest_context_name>
  end
config
  context <dest_context_name>
    dhcp-service <asnpc_svc_name> -n
      bind address <ip_address>
      dhcp server <ip_address>
    end
```

