



# **Cisco ASR 5000 Series Packet Data Interworking Function 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-22963-01

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](http://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 Packet Data Interworking Function Administration Guide

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

# CONTENTS

---

<b>About this Guide .....</b>	<b>vii</b>
Conventions Used.....	viii
Contacting Customer Support .....	x
<b>Packet Data Interworking Function Overview .....</b>	<b>11</b>
Product Description .....	12
Product Specifications .....	13
Operating System Requirements .....	13
Platforms .....	13
Hardware Requirements .....	13
Licenses .....	14
Interfaces .....	15
Sample Deployments .....	17
Mobile Station using Mobile IP with PDIF/FA .....	17
Overview .....	17
Mobile IP / Native Simple IP Call Minimum Requirements .....	18
Mobile IP Session Setup over IPSec .....	18
Simple IP and Simple IP Fallback .....	21
Simple IP Fallback Minimum Requirements .....	24
Features and Functionality - Base Software .....	25
PSC2 Support .....	25
Duplicate Session Detection .....	26
Unsupported Critical Payload Handling .....	26
Registration Revocation .....	27
CHILD SA Rekey Support .....	27
Denial of Service (DoS) Protection: .....	27
Cookie Challenge Statistics .....	28
MAC Address Validation .....	29
RADIUS Accounting .....	29
Special RADIUS Attribute Handling .....	30
Mobile IP and Proxy Mobile IP Attributes .....	31
IPv6 Support .....	31
IPv6 Neighbor Discovery .....	31
IPv6 Static Routing .....	32
Port-Switch-On-L3-Fail for IPv6 .....	32
IKEv2 Keep-Alive (Dead Peer Detection (DPD)) .....	32
Congestion Control and Overload Disconnect .....	32
SCTP (Stream Control Transmission Protocol) Support .....	33
X.509 Digital Trusted Certificate Support .....	33
Custom DNS Handling .....	33
Features and Functionality - Licensed Enhanced Feature Support .....	35
PDIF Service .....	35
Multiple PDIF Services .....	36
Lawful Intercept .....	37
Diameter Authentication Failure Handling .....	37
Online Upgrade .....	38
The Active-Standby Upgrade Model .....	38

Operation Over a Common IPv4 Network .....	40
Operation Over a Common IPv6 Network .....	41
Other Devices .....	42
Session Recovery Support .....	43
IPSec/IKEv2 .....	44
Simple IP Fallback .....	44
Simple IP .....	45
Proxy Mobile IP .....	45
Multiple Authentication in a Proxy Mobile IP Network .....	45
AAA Group Selection .....	46
RADIUS Authentication .....	46
First-Phase Authentication .....	47
Second-Phase Authentication .....	47
Termination .....	48
Session Recovery .....	48
Intelligent Packet Monitoring System (IPMS) .....	49
Multiple Traffic Selectors .....	49
Selective Diameter Profile Update Request Control .....	50
Supported Standards and RFCs .....	51
3GPP2 References .....	51
IETF References .....	51
Object Management Group (OMG) Standards .....	52
<b>Configuration .....</b>	<b>53</b>
Configure the PDIF for Mobile IP or Proxy Mobile IP .....	54
Initial Configuration .....	54
Modify the Local Context .....	54
Create the PDIF Context .....	55
PDIF Configuration .....	56
Create the PDIF Service .....	57
Create the EAP Profile .....	57
Create the IKEv2 and IPSec transform sets .....	58
Create the Crypto Template .....	58
Establish the Initial IKEv2 SA Tunnel Inner Address (TIA) .....	58
Establish the IPSec Child SAs for MIP Sessions .....	59
Configuring the Default Subscriber .....	59
Configuring the IMS-SH Service .....	59
Configuring the Diameter Endpoint .....	60
Configuring AAA Interfaces and AAA Groups .....	60
Configuring the FA Service .....	61
Configuring the HA Service .....	62
Binding the Interfaces to Physical Ports .....	63
Configuring IPSec Traffic Classes and Traffic Selectors .....	65
Creating Access Control Lists to Define IPSec Traffic Classes and Traffic Selectors .....	65
Defining Traffic Classes .....	65
Defining Traffic Selectors .....	66
Verifying the ACL Configuration .....	67
<b>Maintenance .....</b>	<b>69</b>
Configuring an Online Upgrade .....	70
Prerequisites .....	70
Software Upgrade Process .....	71
Software Upgrade Process .....	71
Configuring and Binding an SRP Context .....	72
Creating Interfaces and the SRP Virtual MAC Address .....	74
Upgrading the Primary Chassis .....	75
Completing the Upgrade .....	75

<b>Troubleshooting.....</b>	<b>77</b>
Troubleshooting the PDIF .....	78
System Monitoring Tools .....	78
Generating Statistics .....	78
Clearing Statistics and Counters .....	81
Network Connectivity Testing .....	81
Session Termination Attributes .....	81
Call Failure Scenarios .....	83
MS Power-Down or Failure .....	83
The MS Temporarily Roams Away From the WiFi Access Point .....	84
MS Proxy-MIP Registration Failure .....	84
MS Proxy-MIP Registration Renew Failure .....	84
MS MIP Registration Failure .....	84
WiFi or Access Network Failure .....	84
Total PDIF Failure .....	85
Partial or Transient PDIF Failure .....	85
HA Failure .....	86
General Error Cases for Mobile-IP Networks .....	86
General Error Cases for Proxy Mobile IP Networks .....	87
IPMS Errors .....	87
IPMS Disconnect Reasons .....	88
Show IPMS All Command .....	88
<b>Verifying and Saving Your Configuration .....</b>	<b>91</b>
Verifying the Configuration .....	92
Feature Configuration .....	92
Service Configuration .....	93
Context Configuration .....	94
System Configuration .....	94
Finding Configuration Errors .....	94
Saving the Configuration .....	96
Saving the Configuration on the Chassis .....	97
<b>Sample Configuration .....</b>	<b>99</b>
Sample Mobile IP Configuration .....	100
<b>Engineering Rules .....</b>	<b>107</b>
IKEv2/IPSec Restrictions .....	108
X.509 Certificate (CERT) Restrictions .....	110
IPv6 Restrictions .....	111
ICMPv6 Restrictions .....	112
SCTP Restrictions .....	113







# 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 <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: Login:
Text represented as <b>commands</b>	This typeface represents commands that you enter, for example: <b>show ip access-list</b> This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a <b>command variable</b>	This typeface represents a variable that is part of a command, for example: <b>show card slot_number</b> 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
{ <b>keyword</b> 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
[ <b>keyword</b> 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>{ <b>nonce</b>   <b>timestamp</b> }</pre> <p>OR</p> <pre>[ <b>count</b> <i>number_of_packets</i>   <b>size</b> <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

## Packet Data Interworking Function Overview

---

This chapter discusses the features and functions of Packet Data Interworking Function (PDIF) software. It includes the following topics:

- [Product Description](#)
- [Product Specifications](#)
- [Interfaces](#)
- [Sample Deployments](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - Licensed Enhanced Feature Support](#)
- [Supported Standards and RFCs](#)

## Product Description

The goal of the Fixed Mobile Convergence (FMC) application is to enhance the in-building cellular coverage for FMC subscribers, to reduce the cost of the infrastructure required to carry these calls, and to provide secure access to the carrier's network from a non-secure network. Designed for use exclusively on the Cisco® ASR 5000 Chassis, the Packet Data Interworking Function (PDIF) is a network function based on the 3GPP2 X.S0028-200 standard defining cdma2000 Packet Data Services over an 802.11 WLAN.

A PDIF allows mobile devices to access the Internet over an all-IP WLAN using IKEv2 as the signaling interface. The IKEv2 control path exists between the mobile station (MS) (a dual-mode handset (DMH)) and the PDIF establishing an IPSec tunnel. PDIF also acts as a security gateway protecting CDMA network resources and data (see the Interfaces section). The PDIF is tightly integrated with a collocated Foreign Agent (FA) service, and the PDIF is known throughout this manual as PDIF/FA.

For handsets that do not support mobile IP, PDIF supports proxy mobile IP. If the MS is not suitable for proxy mobile IP registration, it may still be allowed to establish a simple IP session, in which case the traffic is directly routed to the Internet or corporate network from the PDIF. This behavior is controlled through the **proxy-mip-required** configuration in the domain, local default subscriber, or the corresponding Diameter AVP or RADIUS Access Accept. If this is not present, establishing a simple IP session is permitted. Proxy-MIP is documented in the System Enhanced Features Configuration Guide. Although not required for Proxy-MIP, this manual documents Proxy-MIP with a custom-designed feature called multiple authentication (Multi-Auth). Instead of the more usual subscriber authentication, Multi-Auth requires both the device and the subscriber be authenticated using EAP/AKA authentication for the first stage (the device authentication) and GTC/MD5 for the second stage (the subscriber authentication). For this installation, neither GTC nor MD5 is supported, which means authentication is done using PAP/CHAP instead.

When the subscriber is mobile, the MS operates as a normal mobile phone, sending voice and data over the CDMA network. When the FMC subscriber returns home, or encounters a WiFi hotspot, the MS detects the presence of the WiFi network, and automatically establishes an IPSec session with the PDIF/FA. When the secure connection has been established and mobile IP registration procedures successfully finished, the PDIF/FA works with other network elements to provide the MS with access to packet data services.

From here, all voice and data communication is carried over the IPSec tunnel and the PDIF/FA functions as a pass-through for the authentication and accounting information on a RADIUS and/or Diameter server. The MS continues operating over the IPSec tunnel until such time as it can no longer access the WiFi Access Point (AP). At this point, the MS switches back to the CDMA network for normal mobile operation.

# Product Specifications

The following information is located in this section:

- [Operating System Requirements](#)
- [Platforms](#)
- [Hardware Requirements](#)
- [Licenses](#)

## Operating System Requirements

The PDIF operates on the ASR 5000 running StarOS Release 8.1 or later.

## Platforms

The PDIF operates on the ASR 5000.

## Hardware Requirements

- **System Management Cards (SMCs):** SMCs provide full system control and management of all cards within the ASR 5000. Up to two SMCs can be installed; one active, one redundant.
- **Packet Services Cards (PSCs/PSC2s):** PSCs provide high-speed, multi-threaded PDP context processing capability. Up to 14 PSCs can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs):** Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management. Up to 2 SPIOs can be installed: one active, one redundant.
- **Line Cards:** Installed directly behind the PSCs, these cards provide the physical interfaces from the PDIF to various elements in the network. Up to 26 line cards can be installed for a fully loaded system with 13 active PSCs: 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs do not require line cards. Ethernet 10/100 Fast Ethernet and/or Gigabit Ethernet 1000 and/or four-port Quad Gig-E line cards (QGLCs) all provide redundant IP connections.
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards/QGLCs and every PSC in the system for redundancy. Two RCCs can be installed to provide redundancy for line cards and PSCs.

Table 1. PDIF Chassis Hardware Configuration Options

Component	Minimum per Chassis	Minimum for Redundant Chassis Configuration	Maximum per Chassis
System Management Card (SMC)	1	2	2
Packet Services Card (PSC/PSC2)	1	2	14
Switch Processor I/O (SPIO) Card	1	2	2
Redundancy Crossbar Card (RCC)	0	2	2
Power Filter Unit (PFU)	2	2	2
Upper Fan Tray Assembly	1	1	1
Lower Fan Tray Assembly	1	1	1
Line Cards			
Fast Ethernet (10/100) Line Card (FELC)	1	2	28
Gigabit Ethernet Line Card (GELC)	1	2	28
Quad Gigabit Ethernet Line Card (QGLC)	1	2	28

For full descriptions, and for more information on installing, populating, and maintaining the ASR 5000 and its hardware, refer to the *Hardware Installation and Administration Guide*.

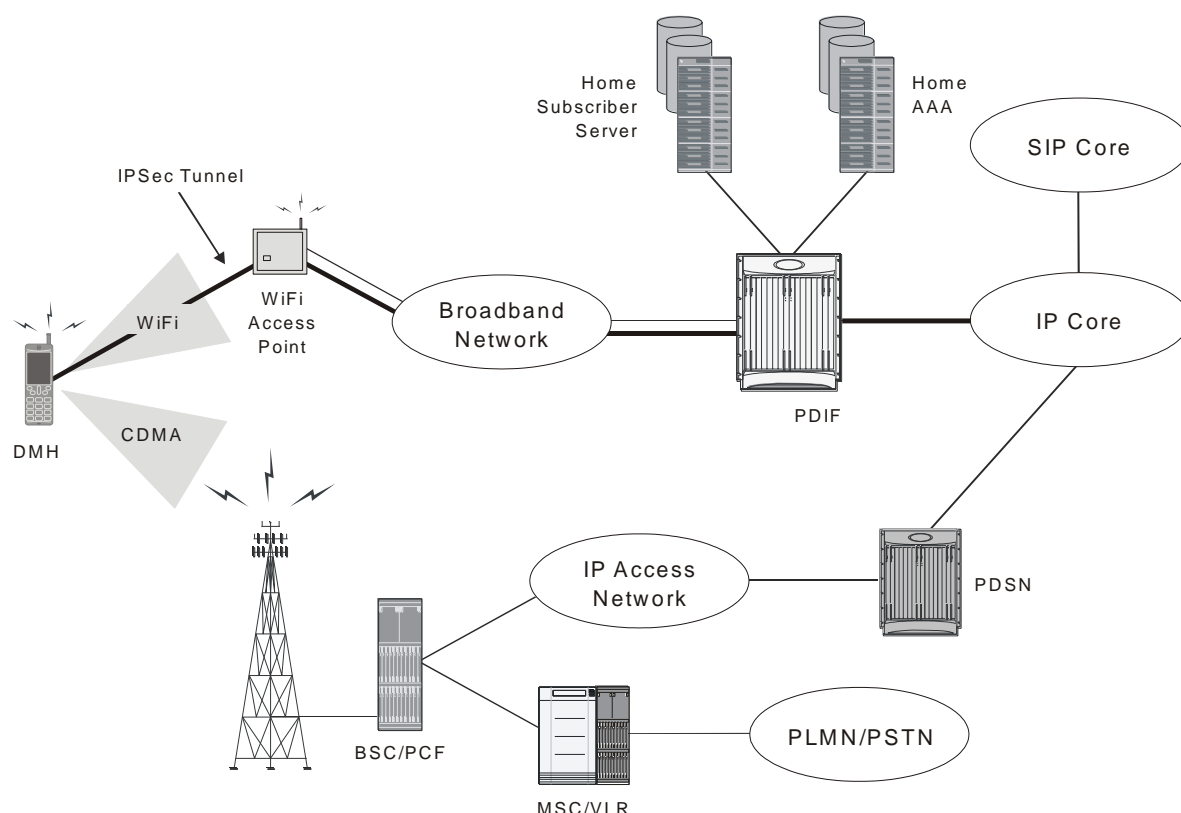
## Licenses

The PDIF is a licensed product with a session counting license, which can be purchased in 1,000 or 10,000 session increments. For information about PDIF licenses, contact your sales representative.

# Interfaces

The figure below shows how the PDIF/FA acts as a security gateway between the Internet and packet data services. All components are located in the home network.

**Figure 1. PDIF/FA Mobile IP Interfaces**



1. The IPsec virtual tunnel interface with the MS: The Mode keyword in the IPsec-transform-set configuration mode defaults to Tunnel. In Tunnel mode, the IP datagram is passed to IPsec, where a new IP header is created ahead of the AH and/or ESP IPsec headers. The original IP header is left intact.
2. The Diameter interface: In a mobile IP network, the IMS Sh interface is used for MAC address validation with the HSS as well as HSS subscriber profile updates. In a Proxy-MIP network using multiple authentication, the HSS server is used to authenticate the device during Stage 1 authentication using the EAP-AKA authentication method.
3. The RADIUS authentication and accounting interface: In a mobile IP network, this interface is used for subscriber authentication using the EAP-AKA authentication method. For subscriber accounting, the PDIF/FA sends start, stop and interim messages to the accounting server. When used in a Proxy-MIP network using multiple authentication, RADIUS is used with the AAA servers to authenticate the subscriber using the GTC/MD5 authentication methods.

4. The home agent interface: This interface is used for Proxy mobile IP and mobile IP subscribers. All mobile station packets are tunneled to the HA through this interface. This interface is not used for simple IP subscribers.
5. The simple IP interface: This interface provides internet access for simple IP users.



## Sample Deployments

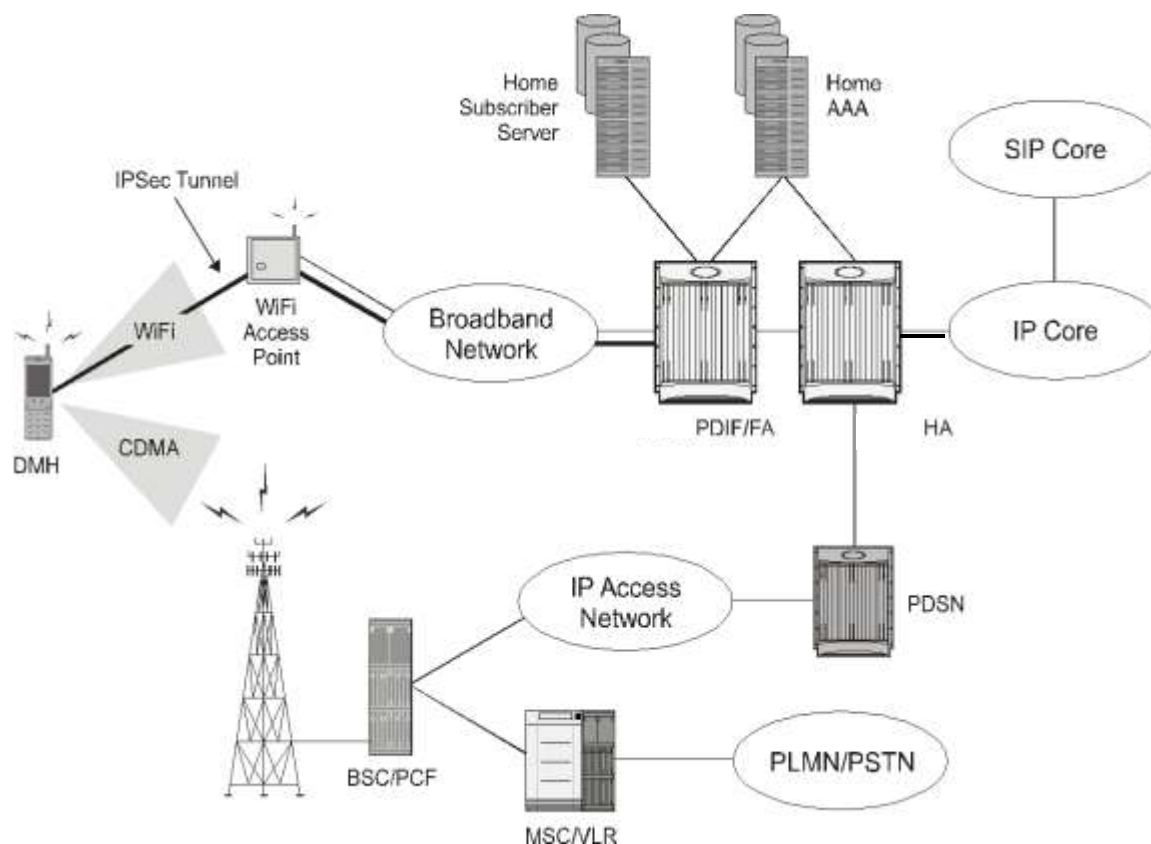
The following are some sample deployments using a PDIF/FA.

### Mobile Station using Mobile IP with PDIF/FA

#### Overview

As shown in the figure below, the PDIF/FA supports the Fixed Mobile Convergence (FMC) application, which employs a Dual Mode Handset (DMH) to provide a VoIP solution over an IP-based WiFi broadband network. The DMH can access the traditional CDMA voice and data networks over the Radio Access Network (RAN). Over the RAN, the DMH implements circuit-switched voice and standard mobile IP (MIP) data over EVDO Rev. A, using the services of a PDSN and an HA.

Figure 2. PDIF/FA Mobile IP Implementation



Alternately, the DMH can send both voice and data over WiFi when a local AP is available. When the DMH connects to the AP, it establishes an IPsec tunnel over the broadband access network. This tunnel terminates at the PDIF/FA.

The DMH initially gets an IP address, also known as a Tunnel Inner Address (TIA), from the PDIF/FA when the DMH establishes the first IPSec tunnel. The PDIF/FA assigns the TIA from its IP address pool. The DMH then starts mobile IP through this initial TIA-based IPSec tunnel.

When the DMH successfully sets up mobile IP, it receives the home address from the HA. The DMH then establishes a second IPSec tunnel using this HA. Once the DMH successfully establishes the second IPSec tunnel with the PDIF/FA, the PDIF/FA tears down the first TIA-based IPSec tunnel to free the TIA, which then returns to the IP address pool. If required, use the **no release-tia** command in config-subscriber mode to prevent the TIA from returning to the pool. The DMH sends packetized voice and data through the PDIF/FA to the HA through the second IPSec tunnel.

In this scenario, the PDIF/FA forwards all the packets between the DMH and the HA. From there, voice packets are delivered to the Session Initiation Protocol (SIP) infrastructure, while data is delivered to the Internet or other appropriate destinations.

## Mobile IP / Native Simple IP Call Minimum Requirements

The following provides the minimum requirements for each call type:

### Mobile IP Calls

The PDIF/FA assumes MIP tunnel establishment over IPSec tunnel as part of the PDIF call flow as soon as any one of the following three possible conditions is met:

1. The default subscriber profile has configured, or:
2. The Radius VSA SN1-PDIF-MIP-Required is returned by AAA during user authentication, or,
3. The MS requests the MIP session type by injecting the IKEv2 configuration attribute 3GPP2\_MIP4\_MODE.

### Native Simple IP Calls

The PDIF/FA assumes a native simple IP session over an IPSec tunnel if:

1. The MS (DMH) does not request 3GPP2\_MIP4\_MODE in IKEv2 exchange, and:
2. If a subscriber profile is defined, it does not have the pdif mobile-ip required parameter, and:
3. The AAA server does not return the VSA SN1-PDIF-MIP-Required during MS user authentication.

## Mobile IP Session Setup over IPSec

The following diagram and table describe the mobile IP session setup over IPSec.

Figure 3. Mobile IP Session Setup over IPSec

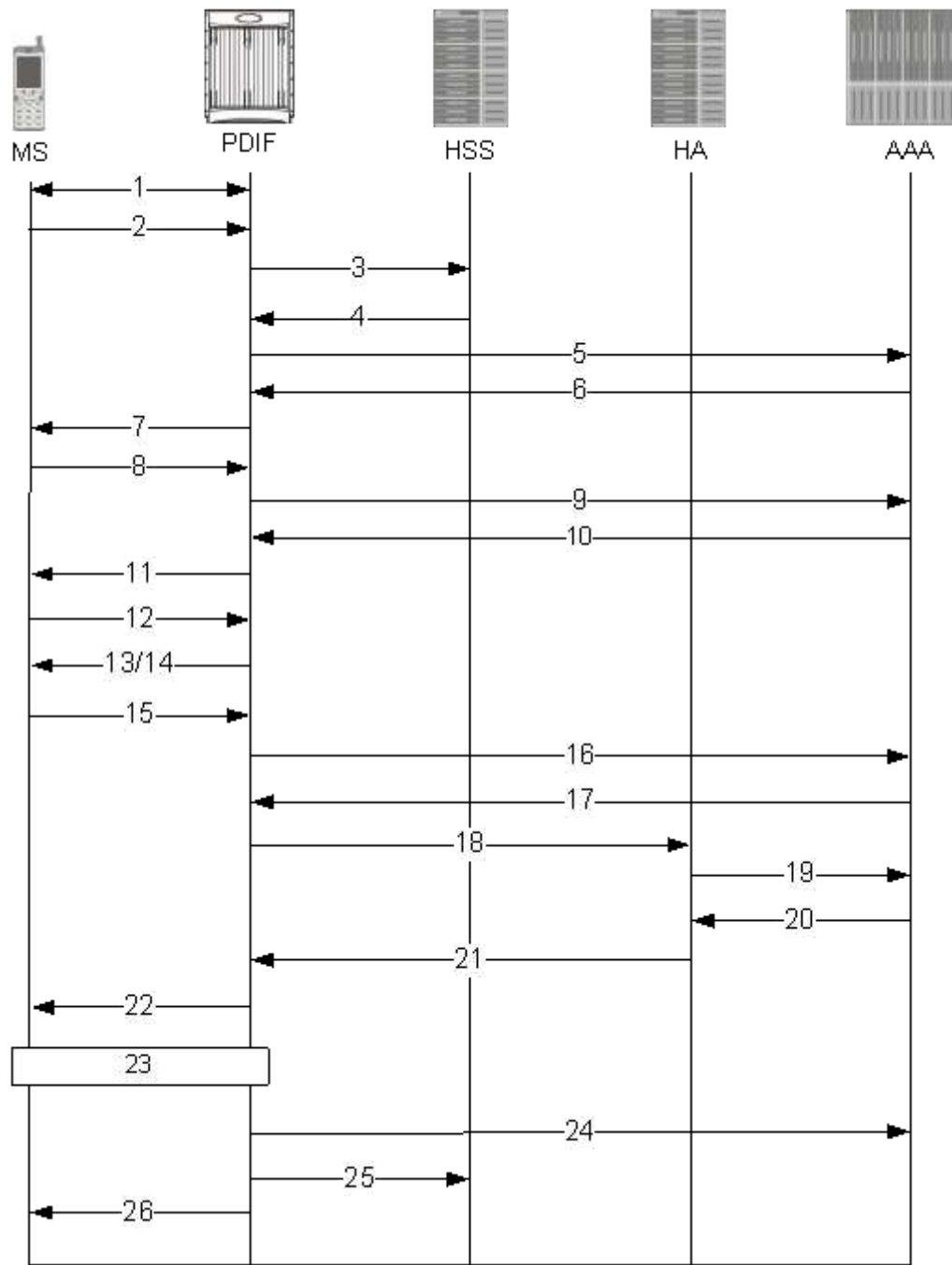


Table 2. Mobile IP over IPSec Call Flow Description

Step	Description
1	After the MS learns the IP address of the PDIF, the MS and the PDIF/FA exchange IKE_SA_INIT messages to negotiate an acceptable cryptographic suite.

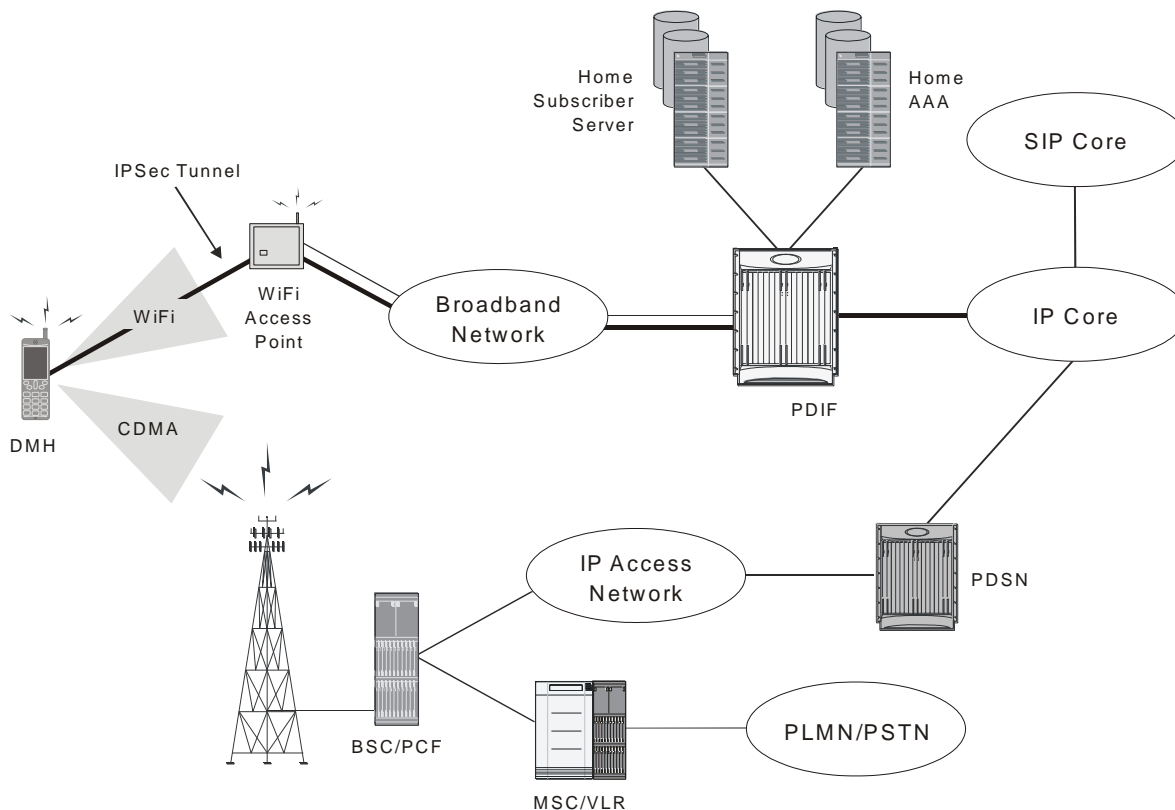
Step	Description
2	The MS initiates IKE_AUTH exchange messages with the PDIF/FA. The MS omits the AUTH parameter to the PDIF/FA, indicating that it wants to use EAP over IKEv2. The MS includes its identity in the IDi payload of the IKE_AUTH request. The IDi is set to be the same as the NAI and the NAI realm is chosen appropriately for M-NAI devices. The MS embeds the MAC address of the WiFi access point (AP) in the NAI and includes the IKEv2 configuration payload. Attributes included in the CFG_REQUEST are at least the INTERNAL_IP4_ADDRESS (with the length set to zero), the INTERNAL_IP4_DNS, and the 3GPP2_MIP_MODE.
3	When the PDIF/FA receives the IKE_AUTH request, it checks if MAC address authorization is enabled. If so, the PDIF/FA uses the ims-sh-service interface to the HSS and requests the list of authorized APs for this user via a User Data Request (UDR).
4	The HSS answers with the list of authorized WiFi APs for the user.
5	After checking that the AP MAC address in the realm portion of the NAI matches with one of the authorized MAC addresses received from the HSS, the PDIF/FA strips the AP MAC address from the realm portion of the NAI and sends the resulting NAI as an EAP response identity to the H-AAA using a RADIUS Access-Request message. This message includes at least the user-name set as the NAI being sent in the EAP response identity, the 3GPP2 correlation ID, the EAP-Message attribute, and the message-authenticator attribute.
6	The H-AAA verifies the identity and checks that WiFi service is allowed for the subscriber. The H-AAA generates a random value RAND and AUTN based on the shared DMU CHAP-key and a sequence number. The H-AAA sends the EAP-Request/AKA Challenge to the PDIF/FA via a RADIUS access-challenge. The EAP-Request/AKA Challenge contains the AT RAND, AT AUTN, and the AT_MAC attribute to protect the integrity of the EAP message.
7	The PDIF/FA sends an IKE_AUTH response to the MS with the EAP-Request/AKA-Challenge message received from the H-AAA.
8	The MS verifies the authentication parameters in the EAP-Request/AKA-Challenge message and if the verification is successful, it responds to the challenge with an IKE_AUTH Request message to the PDIF/FA. The main payload of this message is the EAP-Response/AKA-Challenge message.
9	The PDIF/FA forwards the EAP-Response/AKA-Challenge message to the H-AAA via a RADIUS access-request message (RRQ).
10	If authentication succeeds, the H-AAA sends a RADIUS access-accept message with the EAP-message attribute containing EAP Success. The H-AAA sends the EAP-Success and the MSK generated during the EAP-AKA authentication process to the PDIF/FA. The 64-byte MSK is split into two 32-byte parts, with the first 32 bytes sent in the MS-MPPE-REC-KEY and the second 32 bytes sent in the MS-MPEE-SEND-KEY. Both of these attributes (the values of which are encrypted) are needed to construct the 64-byte MSK at the PDIF/FA. If either are missing, the PDIF/FA rejects the session. In addition, the H-AAA sends other attributes equivalent to what it normally sends to the PDSN for a simple IP session. The attributes include at least the following: The Framed-Pool (if required) so that the PDIF/FA can assign a TIA from the right IP address pool, the Session-Timeout, and The Idle-Timeout.
11	The PDIF/FA forwards the EAP Success message to the MS in an IKE_AUTH Response message.
12	The MS calculates the MSK (RFC 4187) and uses it to generate the AUTH payload to authenticate the first IKE_SA_INIT message. The MS sends the AUTH payload in an IKE_AUTH Request message to the PDIF/FA.
13	The PDIF/FA uses the MSK to check the correctness of the AUTH payload received from the MS and calculates its own AUTH payload for the MS to verify [RFC 4306]. The PDIF/FA sends the AUTH payload to the MS together with the Configuration Payload (CP) containing security associations and the rest of the IKEv2 parameters in the IKE_AUTH Response message, and the IKEv2 negotiation terminates. The CP contains the TIA and IP address of the DNS servers that the device had requested earlier. Although the MS requested a DNS address by including only a single payload option for INTERNAL_IP4_DNS, the PDIF/FA may include both a primary DNS address and a secondary DNS address if one is available.

Step	Description
14	After a CHILD_SA is created using the TIA, if the PDIF/FA received 3GPP2_MIP_MODE during the IKEv2 negotiation, or if MIP_Required subscriber configuration is present in the subscriber profiles, the PDIF/FA sends agent advertisements to the MS.
15	The MS sends a MIP RRQ (including the NAI extension), an MN-AAA authentication extension, etc., to the FA. The HA IP address is set to 0 (zero) because the H-AAA assigns the HA. This is the usual NAI without the MAC address of the WiFi AP in the realm.
16	The PDIF/FA sends a RADIUS access-request to the H-AAA to authenticate the MS credential conveyed in the MN-AAA authentication extension and requests the assignment of an HA.
17	The H-AAA authenticates the MS successfully and sends the RADIUS access-accept message with the HA IP address.
18	The PDIF/FA forwards the RRQ to the HA.
19	The HA sends an access-request to the H-AAA to retrieve the MN-HA key in order to authenticate the MN-HA extension.
20	The HA receives the MN-HA key and authenticates the extension.
21	The HA assigns the IP address (HoA) for the MS and sends the RRP back to the PDIF/FA.
22	The PDIF/FA sends the HoA IP address to the MS.
23	After the MS obtains the HoA in the RRP, the MS sends the CREATE_CHILD_SA message with the Traffic Selector payload for Initiator (TSi) set to the HoA. This IKEv2 exchange creates a new IPSec SA.
24	The PDIF/FA sends a RADIUS accounting start message to the H-AAA.
25	The PDIF/FA then updates the subscriber's HSS profile with the indication that the IPSec session is active and the appropriate IP address. In this case, since it is MIP, it is the HoA assigned by the HA. In the case of simple IP Fallback, it would be the TIA assigned by the PDIF/FA. The HSS profile is updated using the Profile Update-Request (PUR) command.
26	PDIF/FA sends Delete payload in the informational message to delete the old IPSec SA associated with the previously assigned TIA.

## Simple IP and Simple IP Fallback

For some simple IP deployments, the PDIF/FA authenticates the MS and provides an IP address for packet data services. In addition, the PDIF/FA supports Simple IP fallback if the MS abandons mobile IP operations due to not being able to successfully finish mobile IP registration after the first TIA-based IPSec tunnel is established. These scenarios are described below.

Figure 4. PDIF Simple IP Implementation



As described for mobile IP, during the initial IPsec tunnel establishment the MS gets a publicly routable TIA from a pool specified in the Framed Pool RADIUS attribute. When the IKEv2 negotiation finishes, an IPsec SA with a TIA is established as shown above.

Under normal situations, the MS successfully finishes mobile IP and establishes a new IPsec tunnel. However, if mobile IP fails, and simple IP fallback mode is enabled, the MS can revert to simple IP fallback mode and start using the TIA as the source IP address for all communication.



**IMPORTANT:** Simple IP fallback is disabled by default. Use the `pdif mobile-ip simple-ip-fallback` command in config-subscriber mode to enable simple IP fallback.

Under these circumstances, the PDIF/FA opens the IPsec tunnel to data traffic and forwards any packets from the MS to the Internet directly. Any received packets from the Internet will be forwarded to the MS. A summary of this process from the point the TIA is assigned is given below:

Figure 5. Simple IP Fallback Message Sequence

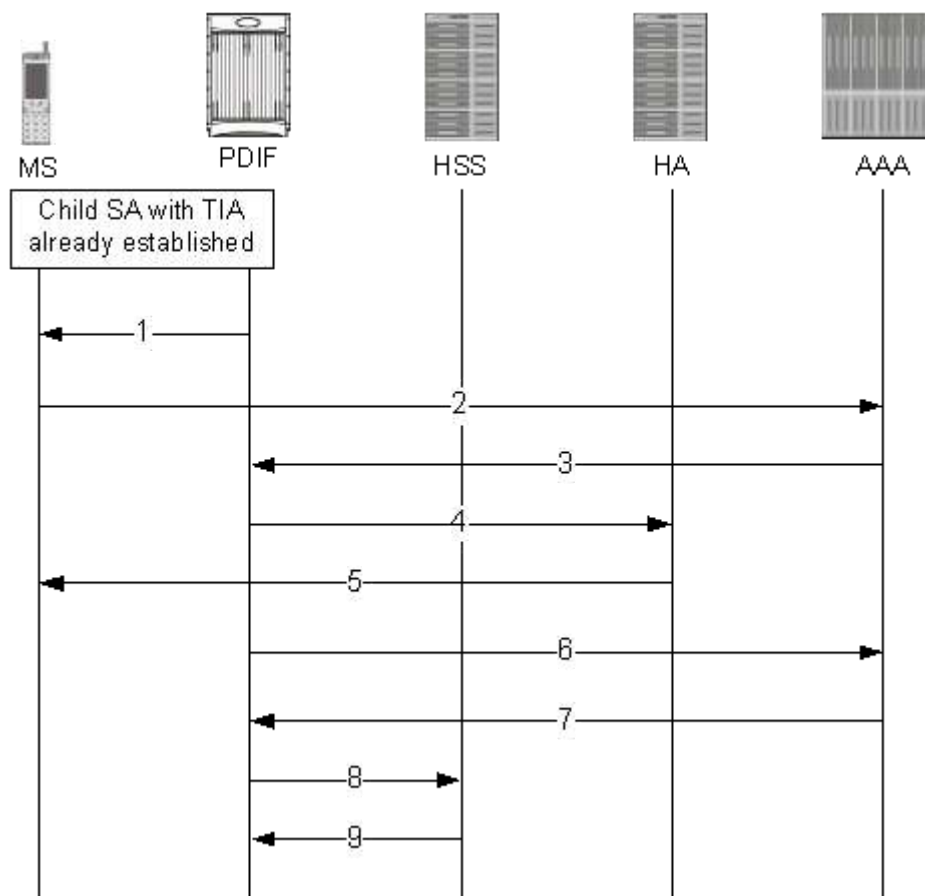


Table 3. Simple IP Fallback Message Sequence

Step	Description
1	With the IPSec Child SA (Security Association) and TIA already in place, the PDIF sends advertisements to the MS.
2	The MS sends a Registration Request (RRQ) message to the PDIF. The PDIF sends an authentication request to the AAA server over the RADIUS interface.
3	The AAA server authenticates successfully and sends the IP address of the HA.
4	The PDIF forwards the RRQ message to the HA.
5	The HA denies the request. The PDIF forwards the denial code to the MS.
6	The session setup timer expires and the PDIF goes into fallback mode. The PDIF sends a RADIUS Accounting Start message.
7	The AAA server sends a RADIUS Accounting Response message.
8	The PDIF updates the HSS with the TIA address of the subscriber.
9	The HSS sends an acknowledgement to the PDIF.

## Simple IP Fallback Minimum Requirements

There are certain minimum requirements for simple IP fallback, as follows:

- There must be a context defined in the CLI configuration.
- The default subscriber must be defined in the CLI configuration.
- Mobile IP Simple IP Fallback must be defined in the CLI configuration. For example:

```
configuration
  context <pdif-in>
    subscriber default
    pdif mobile-ip simple-ip-fallback
  exit
```

- The MS has to request MIP by sending an RRQ message to the PDIF/FA. If the MS indicated an intent to use mobile IP (or was configured with the MIP\_Required parameter) but failed to send an RRQ message, the IPSec session would be disconnected rather than completing a simple IP fallback call.
- On supported networks, the PDIF/FA only assumes simple IP fallback mode if mobile IP is attempted but fails when the MS tries to use mobile IP as the first choice but encounters a problem such as the HA not responding.



## Features and Functionality - Base Software

This section describes the features and functions supported by default in the base PDIF software and the benefits they provide.



**IMPORTANT:** All known restrictions are shown in Appendix B.

The following is a list of the features in this section:

- PSC2 Support
- Duplicate Session Detection
- Unsupported Critical Payload Handling
- Registration Revocation
- CHILD SA Rekey Support
- Denial of Service (DoS) Protection: Cookie Challenge
- MAC Address Validation
- RADIUS Accounting
- Special RADIUS Attribute Handling
- IPv6 Support
- IPv6 Neighbor Discovery
- IPv6 Static Routing
- Port-Switch-On-L3-Fail for IPv6
- IKEv2 Keep-Alive (Dead Peer Detection (DPD))
- Congestion Control and Overload Disconnect
- SCTP (Stream Control Transmission Protocol) Support
- X.509 Digital Trusted Certificate Support
- Custom DNS Handling

### PSC2 Support

The PDIF supports the Packet Services Card 2 (PSC2). The PSC2 is the next-generation packet forwarding card for the ASR 5000. The PSC2 provides increased aggregate throughput and performance, and a higher number of subscriber sessions.

The PSC2 has been enhanced with a faster network processor unit, featuring two quad-core x86 2.5Ghz CPUs, 32 GB of RAM. These processors run a single copy of the operating system. The operating system running on the PSC2 treats the two dual-core processors as a 4-way multi-processor.

The PSC2 has a 2.5 G/bps-based security processor that provides the highest performance for cryptographic acceleration of next-generation IP Security (IPSec), Secure Sockets Layer (SSL), and wireless LAN/WAN security applications with the latest security algorithms.

For more information about PSC2s, see the *Product Overview Guide*.

## Duplicate Session Detection

When an MS sets up a new session, the PDIF automatically checks for any remnants of abandoned calls and if found, clears them.

During a call, the processes of clearing the old session and establishing the new session run in parallel, optimizing processing functions.

With every new session setup, the PDIF supports a mechanism to verify whether there is any old session that is bound with the same International Mobile Subscriber Identity (IMSI) number. This is derived from the Callback-Id AVP in the last DEA message from the HSS after it has verified the subscriber.

For example, if an MS accesses the PDIF and subsequently moves out of the Wi-Fi coverage area, when the MS comes back on line, it could initiate a new session. After authentication, if an old session with the same IMSI is detected, the PDIF starts clearing it by sending a proxy-MIP Deregistration request to the HA. Once a Deregistration request is sent and a Deregistration response is received, the PDIF resumes the new session setup by sending a proxy-MIP Registration request. This setup procedure continues after the PDIF receives a proxy-MIP Deregistration response from the HA.

IMSI-based duplicate session detection is supported per source PDIF context. The PDIF requires only one source context to be configured per PDIF, therefore duplicate session detection across the entire chassis is possible. The feature is designed with the assumption that no more than one call with duplicate identifies are in the setup stage at any time. There is no limit to the number of duplicate session handling iterations.

When an old session is cleared, the PDIF sends Diameter STR messages and Radius Accounting STOP messages to corresponding AAA servers.

The PDIF allows duplicate session detection based on the NAI or IMSI. Note that when detecting based on the NAI, it is the first-phase (Multi-Authentication device authentication phase) NAI that is used.

If NAI-based duplication session handling is enabled, the PDIF sends an INFORMATIONAL (Delete) message to the MS.

Duplicate Session Detection is configured in PDIF-Service mode. The default is NAI-based.

Note that this configuration applies only to calls established after the configuration is made. It is therefore suggested that this selection be made in the boot-time configuration before any calls are established. For example, if NAI-based is used initially and an X number of calls is established, and then the configuration changes to IMSI-based, IMSI-based duplicate session handling does not apply to the calls established before the configuration change.

## Unsupported Critical Payload Handling

This feature provides a mechanism whereby the PDIF ignores all unsupported critical payloads and continues processing as if those payloads were never received.


For MOBIKE IKEv2 messages, the PDIF returns `UNSUPPORTED_CRITICAL_PAYLOAD` in the IKEv2 response messages. The PDIF also drops all NAT-T keep-alive messages.

## Registration Revocation

Registration Revocation is a general mechanism whereby the HA providing mobile IP or proxy mobile IP functionality to a mobile node notifies the PDIF/FA of the termination of a binding. This functionality provides the following benefits:

- Timely release of mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

---

 **IMPORTANT:** Mobile IP registration revocation is also supported for proxy mobile IP. However, in this implementation, only the HA can initiate the revocation.

 **IMPORTANT:** For more information, see Mobile-IP Registration Revocation in the System Enhanced Feature Configuration Guide.

---

## CHILD SA Rekey Support

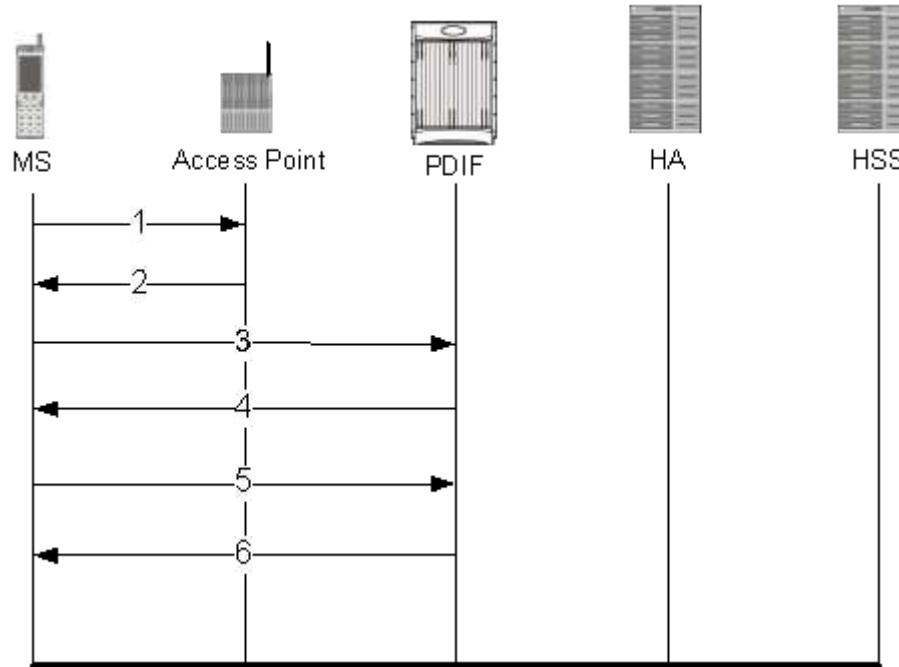
During Child SA (Security Association) rekeying, there exists momentarily (500ms or less) two Child SAs. This is to make sure that transient packets for the old Child SA are still processed and not dropped.

PDIF-initiated rekeying is disabled by default. This is the recommended setting, although rekeying can be enabled through the Crypto Configuration Payload mode commands. By default, rekey request messages from the MS are ignored.

## Denial of Service (DoS) Protection: “Cookie Challenge”

There are several known Denial of Service (DoS) attacks associated with IKEv2. Through a configurable option in the **Config Crypto-Template** mode, the PDIF can implement the IKEv2 “cookie challenge” payload method as described in [RFC 4306]. This is intended to protect against the PDIF creating too many half-opened sessions or other similar mechanisms. The default is not enabled. If the IKEv2 cookie feature is enabled, when the number of half-opened IPsec sessions exceeds the reasonable limit (or the trigger point with other detection mechanisms), the PDIF invokes the cookie challenge payload mechanism to insure that only legitimate subscribers are initiating the IKEv2 tunnel request, and not a spoofed attack.

If the IKEv2 cookie feature is enabled, and the number of half-opened IPsec sessions exceeds the configured limit of any integer between 0 and 100,000, the call setup is as shown in the figure below.

**Figure 6. DoS Cookie-Challenge-Enabled IKEv2 Message Exchange****Table 4. DoS Cookie Challenge Enabled IKEv2 Message Exchange**

Step	Description
1	The MS places a call to the WiFi AP.
2	The WiFi AP returns the IP address of the PDIF.
3	The MS sends an IKE_SA_INIT request. message.
4	The PDIF sends the Notify (cookie) payload to the MS to request retransmission of the IKE_SA_INIT request message to include the Notify (cookie) payload in the message.
5	Upon receipt of the retransmitted message, the PDIF verifies the cookie payload and ensures it is the same cookie as the one it had sent.
6	If the cookie challenge is met, setup continues as normal with an IKE_SA_INIT response message.

## Cookie Challenge Statistics

Cookie challenge statistics appear in the outputs for the following commands:

- **show crypto managers summary ikev2-stats**: Shows the total number of invalid cookies per manager instance.
- **show crypto managers summary npu-stats**: Shows NPU statistics on each IPsec manager.
- **show crypto statistics**: Shows the combined data statistics for the given context name. Includes the number of cookie flows, the number of cookie flow packets, and the total number of cookie errors.
- **show crypto statistics ikev2**: Shows the control statistics for a given context name. Includes the output for **show crypto statistics**, plus Total IKEv2 Cookie Statistics, Cookie Notify Sent, Cookie Notify Received, Cookie Notify Match, Cookie Notify NOT Match, and Invalid Notify Payload Cookie.

## MAC Address Validation

The MS embeds the MAC address from the WiFi AP in the NAI when it sends an IKEv2 AUTH request. If MAC address validation is enabled on the PDIF, it sends a Diameter User-Data-Request (UDR) message to the HSS with the NAI from the MS. The HSS returns a User-Data-Answer (UDA) message to the PDIF containing a list of authorized MAC addresses.

If the PDIF finds the MAC address in this list, the MAC address validation succeeds, and the PDIF continues with the IKEv2 call. The MS starts EAP authentication through IKEv2 AUTH procedures. If configured to do so, the PDIF removes the MAC address from the NAI when sending authentication requests to external RADIUS servers. If the embedded MAC address is not removed, the authentication check fails, because the AAA server cannot accommodate embedded MAC addresses.

If the MAC address is not in the list, the MAC address authorization fails, and the IKEv2 session is terminated with a Notify Message Type 16382 - Private User Errors message.

If the HSS interface is not reachable, it is possible that the IKEv2 session setup could continue as if the MAC authorization had succeeded. However, such error behaviors, including various Diameter error codes from the HSS, are configuration options. That means if an HSS returns an error, the action could be either to continue or to terminate the session. This is discussed in Diameter Failure Handling.



**IMPORTANT:** See also *Diameter Authentication Failure-Handling* in the *Command Line Interface Reference*.

## RADIUS Accounting

RADIUS Accounting messages are not generated while mobile IP setup is in progress.

- A RADIUS accounting START message is generated when the session is established.
- RADIUS INTERIM accounting messages are generated at configured intervals in a call.
- A RADIUS STOP accounting message is sent to the AAA server when the call ends.

There is no session dormancy in the PDIF. Once the session is active, the session never goes to a dormant state.



**IMPORTANT:** RADIUS attributes and customizable dictionary types are described in the *AAA Interface Administration and Reference*. For the impact of attributes in Request and Reply messages, see also [Mobile IP Native Simple IP Call Minimum Requirements](#). There is additional attribute information in the *Session Termination* section in *Troubleshooting*.

## Special RADIUS Attribute Handling

Certain attributes require special handling on the PDIF with the attribute values either controlled by a RADIUS dictionary entry or a PDIF-service configurable. No configuration has no behavioral effect.

- 3GPP2-Serving-PCF. The generation of each new custom dictionary requires a new PDIF image. Configured in the pdif-service mode, the command **aaa attribute 3gpp2-serving-pcf** *<ip-address>* specifies the required values for the attribute without building a new software image. If configured, this attribute is sent in RADIUS accounting messages.

The following attributes are in custom dictionaries but have a customer-requested component.

- Calling-Station-ID. Required for PDIF RADIUS messages, there is a “dummy” value of 000000000000000 (fifteen zeros) set in this attribute. For non-PDIF product lines, the configured value may be taken only if no attributes are received through the corresponding access protocols. Configurable in the PDIF-service.
- NAS-Port-Type. The 3GPP2 X.P0028-200 standard requires this value to be set as “5 (= Virtual).” Controlled through the RADIUS dictionary.
- Service-Type. Cisco specifies a Service Type of “framed” for PDIF messages. Controlled through the RADIUS dictionary.
- Framed-Protocol. There is no attribute value defined for IPSec. Cisco specifies a value of “PPP” for PDIF messages. Controlled through the RADIUS dictionary.
- BSID. Base Station ID is used in billing for calculating time-zone offsets. There is a dummy value set in this attribute for RADIUS messages from the PDIF. Configured in the PDIF-service.
- 3GPP2-MEID and 3GPP2-ESN. Since the customer billing system expects these attributes, a null value is set in these attributes for RADIUS messages from the PDIF. Mobile Equipment Identifier (MEID) uniquely identifies the mobile equipment and is the future replacement for Electronic Serial Number (ESN) of the Mobile Station. Controlled through the RADIUS dictionary.
- 3GPP2-Last-Activity. The event timestamp is set in this attribute where applicable in RADIUS messages from PDIF. This attribute is the same as the 3GPP2-Last-User-Activity-Time standard attribute.
- 3GPP2-Service-Option. Set with a default value of 4095. Configurable in the PDIF-service.
- SN-Disconnect-Reason. This is a Cisco VSA that specifies a more detailed reason for session disconnection.
- 3GPP2-Active-Time. If required for billing purposes, this VSA could be populated with the session length by generating a new RADIUS dictionary with this attribute. Unless specifically requested, a custom RADIUS dictionary does not include the 3GPP2-Active-Time VSA.

## Mobile IP and Proxy Mobile IP Attributes



**IMPORTANT:** The SN-Proxy-MIP attribute is required when PDIF supports proxy mobile IP. The PDIF-Mobile-IP-Required attribute is SN1-PDIF-MIP-Required. These attributes need to be returned in a AAA response message or the mobile IP call fails, although there might be an option for simple IP call setup. See the [Sample Deployments](#) section for more information on attribute messaging.

## IPv6 Support

This section describes the level of IPv6 support. All known restrictions are shown in Engineering Restrictions. Configuration examples are shown in Configuration.

Native IPv6 supports configuration of interfaces and routes with IPv6 (128-bit) addressing. PDIF supports IPv6 for communication with Diameter servers over SCTP. Using the Diameter proxy mechanism, each PSC needs a unique IPv6 address. Multiple IPv6 interfaces per context are supported.

Native IPv6 interfaces communicate with the Diameter servers. PDIF supports the configuration of 32 IPv6 Ethernet interfaces and 32 IPv6 loopback interfaces per context:

- One configured (CIDR global or site-local) IPv6 address per interface.
- Support for auto-configuration of link-local address based on an assigned MAC address. If the MAC address changes, the link-local addresses are updated accordingly. If a virtual MAC address is configured, it uses that MAC address for the link-local IFID. Note that this is distinct from the manual configuration of IPv6 addresses described below.

## IPv6 Neighbor Discovery

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. PDIF supports a subset of IPv6 Neighbor Discovery as defined by [RFC 2461] as follows:

- Uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- Supports configuration of static IPv6 neighbors.
- Adds link-local addresses to Ethernet type interfaces automatically.
- Performs Unsolicited Neighbor Advertisement on line card switchover.
- Responds to neighbor discovery requests for the PDIF IPv6 addresses.

## IPv6 Static Routing

Native IPv6 routing allows the forwarding of IPv6 packets between IPv6 networks. The forwarding lookup is based on destination IPv6 address longest prefix match.

PDIF supports configuration of static routes including a default route. If a default route is configured, all IPv6 traffic is forwarded to the configured next-hop defined by the default route.

## Port-Switch-On-L3-Fail for IPv6

IPv4 port failover redundancy if L3 connectivity is lost is extended to support IPv6 addresses.

For more information on configuring port-switch-on-l3-fail, see *Ethernet Interface Configuration Commands* in the *Command Line Interface Reference* and *Creating and Configuring Ethernet Interfaces and Ports* in the *System Element Configuration Procedures* section of the *System Administration Guide*.

## IKEv2 Keep-Alive (Dead Peer Detection (DPD))

PDIF supports DPD protocol messages originating from both the MS and the PDIF/FA. DPD is configured on a per-PDIF-service basis. The administrator can also disable DPD and the PDIF/FA does not initiate DPD exchanges with the MS when disabled. However, the PDIF/FA always responds to DPD availability checks initiated by the MS regardless of the PDIF/FA idle timer configuration.



**IMPORTANT:** For a number of failure scenarios involving Dead Peer Detection, refer to the *Troubleshooting* chapter.

## Congestion Control and Overload Disconnect

Congestion control is an operator-configurable facility. When the PDIF chassis reaches certain limits (based on CPU utilization, port utilization, and other controls) the system enters a congested state. When in a congested state, existing calls are not impacted but new calls are potentially restricted. There is a separate subscriber-level configuration to enable/disable the feature on a per-subscriber basis. There is also a subscriber-level configurable for **inactivity-time** and **connect-time** thresholds to remove some old and abandoned calls from the system.

The disconnection scenario is as follows:

- If only **idle-time-threshold** is configured, sessions exceeding this threshold would be selected for disconnection.
- If only **connect-time-threshold** is configured, sessions exceeding this threshold would be selected for disconnection.
- If both **idle-time-threshold** and **connect-time-threshold** are configured, sessions with an idle-time greater than the idle-time threshold and a connect-time greater than the connect-time-threshold would be selected for disconnection.



- If neither `idle-time-threshold` nor `connect-time-threshold` is configured, sessions are sorted based on the idle-timer, and sessions with a longer idle-timer are deleted first.

## SCTP (Stream Control Transmission Protocol) Support

PDIF provides support for SCTP (Stream Control Transmission Protocol) for use in communicating with Diameter peers over IPv6.

Diameter/SCTP connections are set up for administratively enabled Diameter peers whenever the system configuration is loaded. In the event of certain card or task-level failures, SCTP connections are torn down and re-established (but note that the Diameter state will still be maintained).


SCTP complies with the description in [RFC 2960 Section 5.1.1] for how to handle the case where the peer is incapable of supporting all of the outbound streams that the endpoint wants to configure. Specifically, PDIF does not abort the session but instead adjusts the association's number of outbound streams to match the number of inbound streams advertised by the peer (in the event that the number sent is less).

## X.509 Digital Trusted Certificate Support

A digital certificate is an electronic credit card that establishes one's credentials when doing business or other transactions on the Web. Some digital certificates conform to ITU-T standard X.509 for a Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, among other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

The PDIF generates an SNMP notification when the certificate is within 30 days of expiration and approximately once a day until a new certificate is provided. The operator needs to generate a new certificate and then configure the new certificate using the CLI. The certificate is then used for all new sessions.

---

 **IMPORTANT:** For more configuration information, refer to *Global Configuration* in the *Command Line Interface Reference*.

---

## Custom DNS Handling

By default, the PDIF always returns a DNS address in the CP payload if one is received from the configuration or the HA. A new CLI has been added defining an alternate series of supported behaviors depending on the number of `INTERNAL_IP4_DNS`. These include, but are not limited to, the following:

- Provides a mechanism whereby the DNS address present in configurations will be sent to the MS in the CP payload only if the MS requests one.
- The address 0.0.0.0 is treated as invalid and not included.



**IMPORTANT:** For more information including full definitions for each of the trigger behaviors, see *Configuring Crypto Template* in *Configuration*, and also see the *Command Line Interface Reference*.

---

# Features and Functionality - Licensed Enhanced Feature Support

This section covers any feature not covered by the base PDIF software and is licensed either separately or in a customized bundle of feature licenses.



**IMPORTANT:** For detailed information on obtaining and installing licenses, refer to the *Managing License Keys* section of *Software Management Operations* in the *System Administration Guide*.

This section describes the following features:

- [PDIF Service](#)
- [Multiple PDIF Services](#)
- [Lawful Intercept](#)
- [Diameter Authentication Failure Handling](#)
- [Online Upgrade](#)
- [Operation Over a Common IPv4 Network](#)
- [Operation Over a Common IPv6 Network](#)
- [Session Recovery Support](#)
- [IPSec/IKEv2](#)
- [Simple IP Fallback](#)
- [Simple IP](#)
- [Proxy Mobile IP](#)
- [Multiple Authentication in a Proxy Mobile IP Network](#)
- [RADIUS Authentication](#)
- [Termination](#)
- [Session Recovery](#)
- [Intelligent Packet Monitoring System \(IPMS\)](#)
- [Multiple Traffic Selectors](#)
- [Selective Diameter Profile Update Request Control](#)

## PDIF Service

The PDIF service and the processes associated with it define the PDIF itself. The PDIF service enables mobile stations to interface with the PDIF.

The PDIF service configuration includes the following:

- **The IPv4 address for the service:** This is the PDIF IP address to which the MS tries to connect. The MS sends IKEv2 messages to this IP address and this address must be a valid address in the context. PDIF service will not be up and running if this IP address is not configured.
- **The name of the crypto template for IKEv2:** A crypto template is used to configure an IKEv2 PDIF IPSec policy. It includes most of the IPSec parameters and IKEv2 parameters for keep-alive, lifetime, NAT-T and cryptographic and authentication algorithms. There must be one crypto template per PDIF service. The PDIF service will not be up and running without a crypto-template configuration.
- **The EAP profile name:** This profile defines the EAP authentication methods.
- **Multiple authentication support:** The multiple authentication configuration is a part of the crypto template.
- **IKEv2 and IPSec transform sets:** These define the negotiable algorithms for IKE SA and CHILD SA setup to connect calls to the PDIF/FA.
- **Configure the setup timeout value:** The MS connection attempt is terminated if the MS does not establish a successful connection within the configured value.
- **Mobile IP foreign agent context and foreign agent service:** This defines the system context where mobile IP foreign agent functionalities are configured.
- **Max-sessions:** The maximum number of subscriber sessions allowed by this PDIF service.
- **PDIF supports a domain template for storing domain related configuration:** The domain name is taken from the received NAI and searched in the domain template database.
- **3GPP2 serving PCF address:** This configurable specifies what value in the RADIUS attribute when sending authentication and accounting messages.
- **Duplicate session detection parameters:** PDIF supports either NAI (first phase authentication) or IMSI to be used for duplicate session detection. This configuration specifies whether duplicate session detection is based on IMSI or NAI. The default is NAI.

When the PDIF service is configured in the system with the IP address, crypto template, etc., the PDIF is ready to accept IKEv2 control packets for establishing IKEv2 PDIF sessions.

There is a limit to the number of CHILD SAs supported by each PDIF service. Traditionally, other Cisco services limit this to the number of subscriber sessions. The PDIF treats this as the number of CHILD SAs. This means that if each subscriber establishes only a single CHILD SA, the limit will be equal to the number of subscriber sessions. During CHILD SA rekeying, for a small duration of time, there are two CHILD SAs in the system. This is to make sure that transient packets for the old CHILD SA are still processed (not dropped).

## Multiple PDIF Services

The PDIF supports multiple PDIF services running simultaneously on the same ASR 5000. This feature enables operators to configure PDIF services with different crypto templates to support multiple subscriber handsets and to set per-service maximum session limits. The total number of sessions for all PDIF services running simultaneously on the same ASR 5000 must fall under the PDIF session counting license limit.

## Lawful Intercept

The PDIF supports the Lawful Interception (LI) of subscriber session information. This functionality provides Telecommunication Service Providers (TSPs) with a mechanism to assist Law Enforcement Agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

The following standards were referenced:

- TR-45 Lawfully Authorized Electronic Surveillance TIA/EIA J-STD-025 PN4465 RV 1.7
- 3GPP TS 33.106 V6.1.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 6)
- 3GPP TS 33.107 V6.2.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 6)
- Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ), Version 4.0

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 Integrated Services Digital Network (MSISDN) number, or their International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the system, functioning as either a GGSN or HA, serves as an Access Function (AF) and performs monitoring for both new PDP contexts or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface. Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

## Diameter Authentication Failure Handling

Diameter EAP failure handling defines error handling for both Session Termination Requests and for EAP Requests.

Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. EAP failure handling is flexible enough that wide ranges of result codes can be defined with the same action, or actions can be bound on a per-result-code basis.

A failure does not necessarily mean a summary termination of a call.

The following configuration:

```
diameter authentication <failure-handling> session-termination-request
```

```
diameter result-code 5001-5005 action continue
```

configures result codes 5001, 5002, 5004 and 5005 to mean the session could continue regardless of the error, and

```
diameter authentication <failure-handling> session-termination-request
```


```
diameter result-code 5003 action terminate
```

configures result code 5003 to mean terminate the session immediately.

In this scenario, the PDIF receives the DEA from an HSS with the failure code 5003 to terminate the IKE setup for the session. The PDIF sends the IKE\_AUTH Response containing a Notify Payload with the type as AUTH\_FAILED plus the EAP payload if one was received in the DEA.

When the PDIF received the last DEA message with AVPs that are not in the dictionary, and with the M-bit set to 1, the PDIF disconnects the session.

---

 **IMPORTANT:** Refer to *Configuring Diameter Authentication Failure Handling* in the *AAA Interface Administration and Reference* and the *Command Line Interface Reference* for more information.


---

## Online Upgrade

The customer has the benefits of upgrading software from a fully redundant device without the expense of maintaining a fully loaded, fully redundant ASR 5000 in a permanent state of standby.

The PDIF supports online software upgrades with a single software version difference between two chassis. For example, upgrading from Release 8.1 to 8.2 is supported. Support for a chassis running greater differences in software versions would be qualified by Cisco on an as-needed basis.


---

 **IMPORTANT:** Refer to the *Maintenance* chapter in this guide for information on how to perform the upgrade.

---

The online upgrade process calls for a spare ASR 5000 to temporarily perform the services currently being provided by a live networked chassis and upgrade the software with minimal service interruption. This model is called Active-Standby, as one chassis is designated as active and the other as standby. The standby chassis does not handle any new, incoming sessions because the DNS allocating new sessions does not know about the backup chassis. The backup is only required to handle sessions that were already on the primary chassis when it was administratively disconnected from the DNS server. Except for the data loss during the brief chassis switch-over, the session information (accounting and timers) are synchronized so that they are accurate when the backup becomes the active PDIF.

---

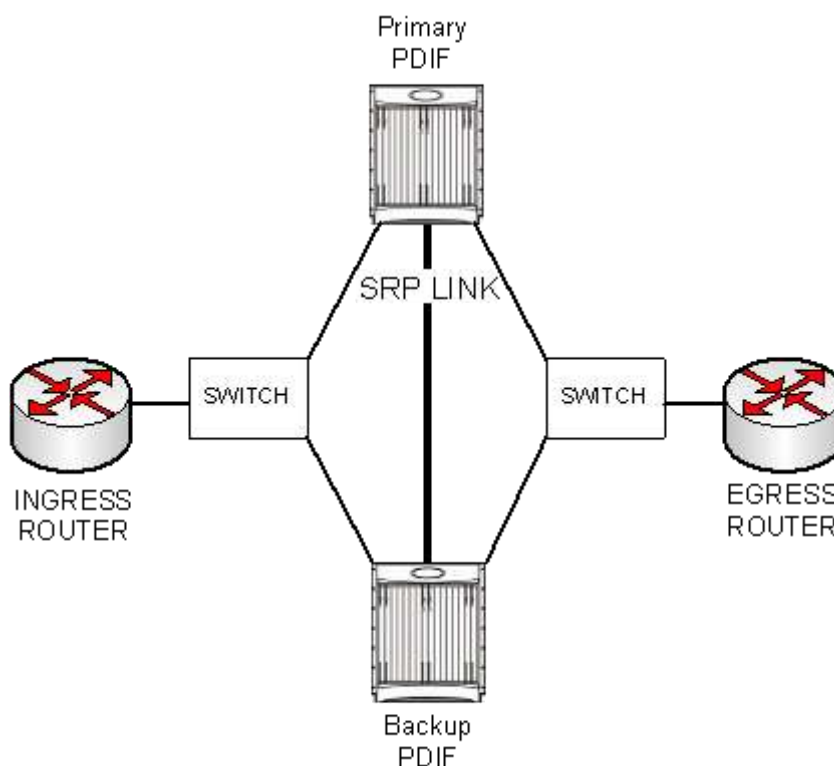
 **IMPORTANT:** Online upgrade requires miscellaneous internal processing that may result in intensive CPU utilization. Up to 50% CPU utilization overhead should be expected during the upgrade.

---

## The Active-Standby Upgrade Model

The Active-Standby model is shown below:

Figure 7. Active-Standby Online Upgrade Model



The active and standby chassis are connected by an SRP redundancy link to monitor and control the chassis state. Both active and standby chassis have SRP-activated resources defined. Resources could mean loopback interfaces, broadcast interfaces, or IP pools, depending on the installation. For this example, use loopback interfaces.

These resources are the same between the active and standby PDIF. Loopback IP addresses in ingress and egress contexts, and IP pools in egress contexts, are usually SRP-activated resources. The result is that only the currently active chassis enables the SRP-activated resources. The activate command is **srp-activate**.

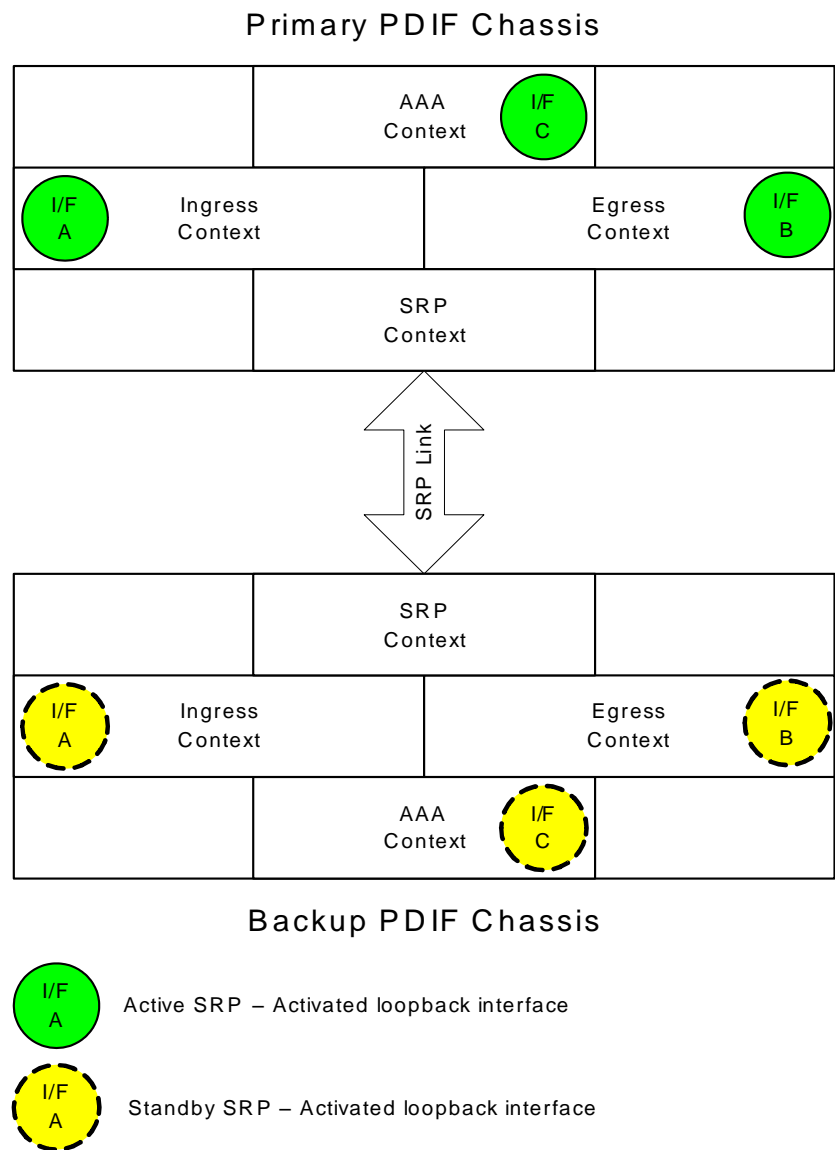


**IMPORTANT:** Ingress and egress contexts could be the same context. The SRP context must be a separate context.

In the network diagram below, each ingress context has loopback interface A defined, which is SRP-activated. PDIF service A is bound to this interface. The standby chassis has the same interface and PDIF service defined. Both interface and service can only be enabled on the active chassis. Similarly, interface B is defined in the egress context, which can be activated only in the active chassis.

When the active chassis switches over, the standby chassis becomes active and enables all SRP-activated IP interfaces and IP pools so that it can function as a mirror image of the former primary PDIF.

Figure 8. Loopback Interface Configuration



## Operation Over a Common IPv4 Network

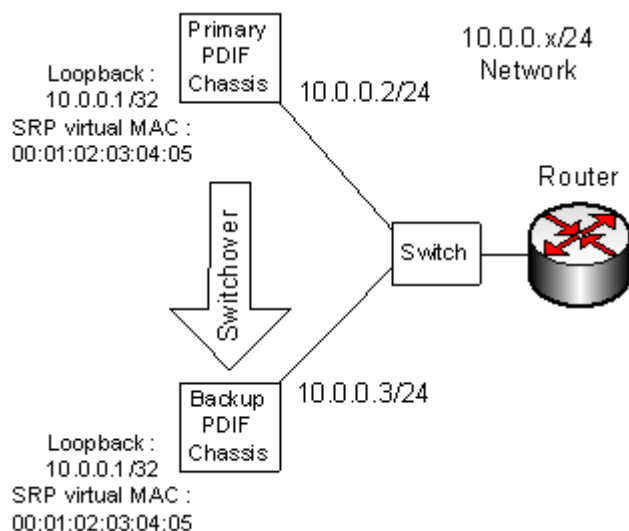
The PDIF supports L2 switching to enable carriers not using dynamic routing between the core nodes to perform an online upgrade.

In the example below, the SRP virtual MAC address is configured for the SRP-activated loopback address for the subnet. This allows the standby chassis to seamlessly assume the active role in the network after a switchover. Attached devices continue to send to the same SRP virtual MAC address and the currently active chassis responds to ARP requests for the shared loopback IP address. This scheme allows fast standby-to-active transitions, since the SRP virtual MAC address does not change during the switchover.



When the ASR 5000 transitions from backup to primary, the PDIF sends Gratuitous ARPs to update the port-MAC table of the adjacent switch.

**Figure 9. Switchover Example for Common IPv4 Subnet**

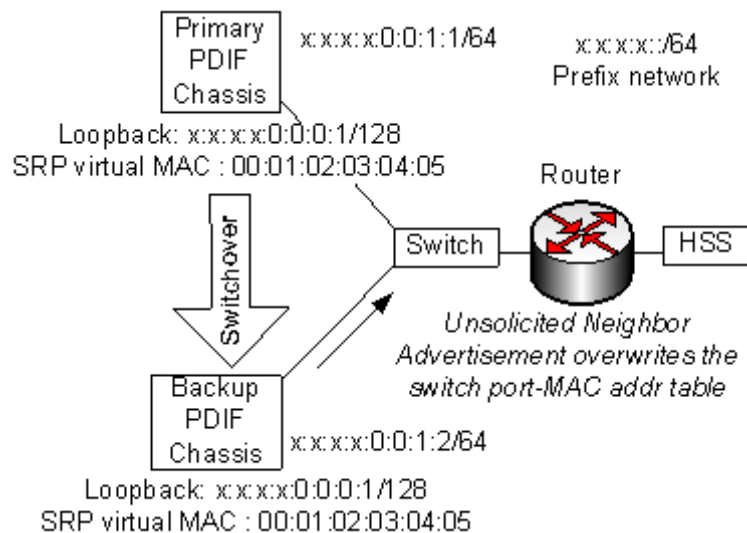


## Operation Over a Common IPv6 Network

For AAA context with Diameter/SCTP/IPv6 configuration, multiple loopback IPv6 addresses are configured as Diameter endpoints. The customer can SRP-activate these loopback addresses and, upon SRP switchover, the HSS/SLF still sees the same Diameter peer endpoint. No new Diameter peer configuration to the HSS/SLF is required.

With SRP switchover operation in effect, the PDIF shuts down all the SCTP connections to the HSS/SLF. Then the former backup PDIF immediately creates new SCTP connections with the HSS/SLF. In this reestablishment process, the backup chassis sends an Unsolicited Neighbor Advertisement message to the adjacent switch, which is then used to overwrite its port MAC address table as shown in the diagram below.

Figure 10. Switchover Example for a Common IPv6 Subnet



## Other Devices

The following table summarizes how other network devices see two ASR 5000s chassis during online upgrade. The table below assumes that a SRP-activated loopback address is configured in the source (toward the MS), the destination (toward the HA), and the AAA contexts (Diameter and RADIUS).

Table 5. The Chassis as seen from Other Network Devices During Upgrade

Network Entity	Consideration in Two-Chassis Configuration
L3 switch (MS ~ PDIF)	This L3 switch sees two chassis as a single entity. Only the physical port in the switch changes due to the switchover operation by G-ARP. The rest of the ASR 5000 information (IP address and MAC address) remain the same.
L3 switch (PDIF ~ HA)	This L3 switch sees two chassis as a single entity. Only the physical port in the switch changes due to the switchover operation by G-ARP. The rest of the ASR 5000 information (IP address and MAC address) remains the same.
Diameter Server	The MS sees two PDIFs as the same entity. However, upon switchover the SCTP connection is disconnected and then a new SCTP connection with ASR 5000 is established immediately. If an L3 switch exists between the PDIF and Diameter server, it sees two chassis as a single entity. Only the physical port in the switch changes due to the switchover operation by IPv6 Unsolicited Neighbor Advertisement. The rest of the ASR 5000 information (IP address and MAC address) remains the same.
RADIUS Server	This L3 switch sees these two chassis as a single entity. Only the physical port in the switch changes due to the switchover operation by G-ARP. The rest of the chassis information (IP address and MAC address) remains the same. If there should be an L3 switch between the PDIF and a RADIUS server, it sees two chassis as a single entity. Only the physical port in the switch changes due to the switchover operation by G-ARP, and the rest of the ASR 5000 information (IP address and MAC address) remains the same.

Network Entity	Consideration in Two-Chassis Configuration
IPMS Server	Each chassis is connected to an independent IPMS Server. When a switchover takes place, the new IPMS Server continues to capture and store the call logs (signaling messages and events).
O&M Device	Each chassis is connected to an independent O&M Device. When a switchover takes place, the new O&M Device continues to perform the function as the original device was configured.

## Session Recovery Support

The session recovery feature provides seamless failover and almost instantaneous reconstruction of subscriber session information in the event of a hardware or software fault within the same chassis, preventing a fully connected user session from being dropped.

Session recovery is performed by mirroring key software processes (the session manager and the AAA manager, for example) within a single PDIF. These mirrored processes remain in an idle state (in standby mode), wherein they perform no processing, until they may be needed in the case of a software failure (a session manager task aborts, for example). The system spawns new instances of standby mode sessions and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks such as VPN manager are performed on a physically separate Packet Services Card (PSC/PSC2) to ensure that a double software fault (the session manager and the VPN manager fail at same time on same card, for example) cannot occur. The PSC used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Management Card (SMC) and a standby PSC.

There are two modes for session recovery.

- **Task recovery mode:** Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby PSC. In this mode, recovery is performed by using the mirrored standby-mode session manager tasks running on active PSCs. The standby-mode task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full PSC recovery mode:** Used when a PSC hardware failure occurs, or when a PSC migration failure happens. In this mode, the standby PSC is made active and the standby-mode session manager and AAA manager tasks on the newly-activated PSC perform session recovery.

Session/call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. To ensure task recovery, these pairs are started on physically different PSCs.



**IMPORTANT:** For more information on session recovery support, refer to *Session Recovery* in the *System Enhanced Feature Configuration Guide*.

## IPSec/IKEv2

IKEv2 and IPSec transform sets configured in the crypto template define the negotiable algorithms for IKE SA and CHILD SA setup to connect calls to the PDIF/FA by creating two secure tunnels. The first, called the Tunnel Inner Address (TIA) is for signaling traffic, but in some cases it can be used for user traffic which can then use the TIA IP address. The second IPSec SA connects the MS to an HA for a mobile IP call.

Refer to *Sample Deployments* for a full description of how a variety of calls are successfully set up (and torn down) in a variety of network scenarios.

At the beginning of IKEv2 session setup, the PDIF and MS exchange capability for multiple authentication. Multiple authentication is configured in the crypto template of the PDIF service. When multiple authentication is enabled in the PDIF service, the PDIF will include MULTIPLE\_AUTH\_SUPPORTED Notify payload in the initial IKEv2 setup response.

The MS first sends an NAI for the device authentication, in which EAP-AKA is used. After the successful EAP-AKA transaction between the MS and the HSS, the HSS is expected to return the IMSI number for this subscriber. The PDIF uses the authorized IMSI number for session management.

Once the device authentication is successful, the MS notifies the PDIF of its intention to continue subscriber authentication only if the PDIF indicates it has multiple authentication support during the initial IKEv2 exchanges. The MS sends the second NAI that may be different from the first one used during the device authentication. The subscriber authentication is completed either using EAP-MD5 or EAP-GTC. Upon successful authentication, the PDIF continues proxy MIP registration before granting its access to the network.

Even if the PDIF sends the MULTIPLE\_AUTH\_SUPPORTED capability in the initial IKEv2 setup response, the MS may not support multiple authentication and hence may not include MULTIPLE\_AUTH\_SUPPORTED Notify payload in the subsequent IKEv2 AUTH exchange. In this case, the MS may only go through the first authentication (which is EAP-AKA authentication). After EAP-AKA authentication, if proxy-mip-required is configured for the session (either through the domain or the default subscriber or the corresponding Diameter AVP), the PDIF will establish a proxy mobile IP session with the HA. The assigned IP address is normally done by the HA and the PDIF receives this address through proxy mobile IP RRP. The PDIF will pass this address back to the MS through the final IKE\_AUTH exchange. On the other hand, if proxy-mip-required configuration is not present or disabled, then the PDIF will continue the simple IP session setup by allocating the IP address for the MS from the locally configured pool.

When the MS sends MULTIPLE\_AUTH\_SUPPORTED Notify payload in subsequent IKE\_AUTH exchanges, the PDIF knows the MS wants to do the second authentication. After the first successful EAP-AKA authentication, the MS will indicate to the PDIF regarding the second authentication (through ANOTHER\_AUTH\_FOLLOWS Notify payload in the final IKEv2 AUTH request). Please note that the IP address of the MS will not be assigned during the first authentication if the second authentication is to happen. The MS will then initiate the second authentication IKEv2 exchanges. In some networks, this second authentication uses the RADIUS AAA interface. The proxy-mip-required attribute will normally be present in the subscriber profile (or in the domain or default subscriber template) through a RADIUS attribute in the Access Accept message. After successful authentication, if proxy-mip-required is enabled, the PDIF will setup a proxy mobile IP session with the HA, and the HA assigns an IP address to the MS. If proxy-mip-required is disabled (or not present in the subscriber/domain profile), the PDIF establishes a simple IP session and routes traffic using the direct IP interface.

## Simple IP Fallback

Network operators with handsets that are mobile IP capable may want the MS to be connected to the network and capable of doing data transfer even though the mobile IP registration process might fail under certain situations. If the mobile IP registration failures are due to HA reachability issues or any authentication problems, the MS should still be

able to connect to the network using a simple IP connection, assuming that simple IP fallback is enabled in the PDIF configuration. See *Simple IP* and *Simple IP Fallback* in this chapter for a full description of this type of network configuration.

## Simple IP

Simple IP is a solution for network providers whose subscribers fall primarily within a limited set of requirements. It provides the following:

- A mobility solution for subscribers who do not typically roam outside their immediate coverage area.
- An appropriate level of service for users who do not use the network in such a way as to need constant service between coverage areas. For example, subscribers who do not perform large file downloads.
- A mechanism to complete a call even if the proxy-mip-required or mip-required attributes are not configured in the subscriber or domain profile.

## Proxy Mobile IP

Proxy mobile IP has the following benefits:

- Allows an MS that does not support mobile IP to have the same roaming benefits of one that does.
- The PDIF communicates with the HA and acts as if the PDIF itself were the handset.
- Proxy mobile IP is configured through the **proxy-mip-required** configuration, or the corresponding Diameter AVP or RADIUS Access Accept messages. If neither are present, the PDIF establishes a simple IP session and the PDIF routes the call to the Internet or corporate network.

Proxy mobile IP provides a mobility solution for subscribers whose mobile nodes do not support mobile IP protocol. The PDIF sets up the mobile IP tunnel with the HA and the PDIF proxies or acts on behalf of the handset as if it were the handset. The subscriber receives an IP address from either the service provider or from their home network. As the subscriber roams through the network as if it were using a full mobile IP connection, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.



**IMPORTANT:** Refer to *Proxy Mobile-IP* in the *System Administration Guide* for more information.

---

## Multiple Authentication in a Proxy Mobile IP Network

Multiple authentication requires authenticating both the device and the subscriber.

At the beginning of the IKEv2 session setup, the PDIF and the MS exchange capability for multiple authentication. Multiple authentication is configured in the PDIF service as part of the crypto template where it is associated with an

EAP profile. The EAP profile defines the authentication mode and method. If multiple authentication is enabled in the crypto template, the PDIF includes a `MULTIPLE_AUTH_SUPPORTED` Notify payload in the initial IKEv2 setup response.



**IMPORTANT:** Even if the PDIF confirms `MULTIPLE_AUTH_SUPPORTED` capability in the initial IKEv2 setup response, the MS may not support multiple authentication and hence may not include a `MULTIPLE_AUTH_SUPPORTED` Notify payload in the subsequent IKEv2 AUTH exchange. In this case, the MS may only go through the first-phase (EAP-AKA) of device authentication.

During initial IKEv2/IPSec security setup exchanges, the MS undergoes both device authentication and subscriber authentication. This is because even if the device is fully authenticated, a PDIF may not be able to tell which service profile is applicable for the MS, nor the correct IP address to assign.



**IMPORTANT:** First-phase authentication refers to device authentication, and second-phase authentication refers to subscriber authentication.

## AAA Group Selection

A maximum of 64 AAA groups is allowed on the ASR 5000. This could be spread across multiple contexts or all groups can be configured within a single VPN context.

A maximum of 320 RADIUS servers is allowed on the chassis.

When the **aaa-large-configuration** command is issued, this number becomes 800 AAA groups and 1600 RADIUS servers configured within the chassis.

The PDIF service allows you to specify a different AAA group for each authentication phase. A given AAA group supports either Diameter or RADIUS authentication, but not both. In deployments where the NAI used in the first-phase authentication is different from the NAI used in the second-phase authentication, each NAI can point to different domain profiles in the PDIF.

## RADIUS Authentication

Please see the document *AAA Interface and Administration* for information on AAA, RADIUS, and Diameter groups.

The second authentication uses RADIUS for subscriber authentication. The PDIF supports EAP termination mode during the second half of multiple authentication. In this mode, EAP exchange takes place between the MS and the PDIF, and the PDIF takes the information exchanged in the EAP payload over IKEv2 into RADIUS attributes to support CHAP/PAP authentication with the RADIUS server, and vice versa.

By default, the PDIF initiates EAP-MD5 authentication and sends an EAP payload with an MD5-Challenge to the MS. The MS returns an MD5-Challenge response in the EAP payload. Upon receipt, the PDIF sends an RADIUS Access Request message which includes an NAI, a CHAP-Password, a CHAP-challenge (derived from the EAP payload), and an IMSI number (which is the calling station ID). Once the AAA server returns an Access-Accept message, optional attributes such as Framed-IP-Address and HA address are expected for the subsequent session setup processing. The PDIF translates this Access-Accept message into an EAP Success message, and returns this in an `IKE_AUTH` Response message.

It is possible that some MSs may not support CHAP authentication. In this case, the MS is expected to return the EAP payload with a legacy-Nak message when the PDIF sends an MD5-Challenge message. Upon receipt of the legacy-Nak message, the PDIF initiates an EAP-GTC procedure. When the MS returns EAP-GTC including its own password, the PDIF sends a RADIUS Access Request message which includes an NAI, a password, and an IMSI number. Once the AAA server returns an Access-Accept message, attributes such as Framed-IP-Address and HA address are expected for the subsequent session setup processing. The PDIF translates the Access-Accept message as EAP success, and returns this in an IKE\_AUTH Response message.

If EAP-GTC is configured, then the EAP-GTC method is used instead of the EAP-MD5 method.

The PDIF does the following for IKEv2 and RADIUS authentication:

The PDIF terminates EAP-MD5/GTC authentication. The PDIF understands the values in the EAP payload, and maps them as RADIUS attributes for CHAP/PAP authentication.

Upon request from the MS, the PDIF performs EAP-GTC authentication instead of EAP-MD5.

Each domain profile may be configured with two AAA groups, one for Diameter and the other for RADIUS.

In deployments where both NAI happen to be the same for both authentications, it will point to the same AAA group and thereafter only one protocol (either RADIUS or Diameter) is used.

There are cases where the domain template may not be associated with a given NAI. In such cases, the default AAA groups are used for authentication. Since authentication happens in two phases, and each using Diameter and RADIUS AAA groups respectively, there needs to be two default AAA groups (one for Diameter authentication and one for RADIUS authentication) for multiple authentication. The default AAA groups are configured in the PDIF service.

## First-Phase Authentication

During first-phase authentication, the HSS authenticates the device. The MS first sends an NAI for device authentication. After the successful EAP-AKA transaction between the MS and the HSS, the HSS is expected to return an IMSI number for this subscriber. The PDIF takes this authorized IMSI number for session management.

This authentication method uses EAP between the MS and the AAA server, and the PDIF acts as a pass-through agent.



**IMPORTANT:** First-phase authentication must use the EAP-AKA method.

Depending on the number of HSSs in the network, it is possible that a Subscription Locator Function (SLF) would be introduced into the network as a Diameter proxy or relay agent. If deployed, the SLF would be the first point of contact for the PDIF.

The protocol stack between the PDIF and the HSS/SLF is Diameter over SCTP over IPv6.

## Second-Phase Authentication

Second-phase authentication uses EAP-MD5 or EAP-GTC authentication with IKEv2 using a legacy RADIUS server, which does not understand or implement EAP. This could be the same AAA server as those deployed in any existing EV-DO network. In this case, EAP authentication happens between the MS and the PDIF.

The protocol stack between the PDIF and the AAA server is RADIUS over UDP over IPv4.

The two algorithms for second-phase authentication are EAP-MD5 (which is the same as CHAP authentication) and EAP-GTC (which is the same as PAP authentication). When the MS sends the NAI to identify the subscriber, the PDIF initiates the EAP-Request with a challenge. Once the MS returns the challenge response, the PDIF maps it to a RADIUS

ACCESS\_REQUEST message to complete CHAP authentication. There is an internal mechanism to inform each peer if one method is not supported and to renegotiate to use the other supported method.

In general, session attributes during first-phase authentication are overwritten by those from second-phase authentication, unless specified separately. Exceptions to this include **session-timeout** and **idle-timeout**, when the lower values are taken.

## Termination

During session setup, if there are any configuration mismatches or the PDIF cannot get the required information, the session setup process is terminated and appropriate log messages are generated.

If **multiple-auth-supported** is not enabled on the PDIF, and the MS still sends a MULTIPLE\_AUTH\_SUPPORTED Notify payload marked with the critical bit set, the PDIF returns UNSUPPORTED\_PAYLOAD. Otherwise, the PDIF ignores it and processes the IKE packet as if the payload was never received. This is non-standard MS behavior.



**IMPORTANT:** The multiple authentication process in a proxy mobile IP network is described in Proxy-MIP in the System Enhanced Features Guide.

## Session Recovery

The session recovery feature provides reconstruction of subscriber session information in the event of a hardware or software fault within the system, providing seamless failover and preventing a fully connected user session from being dropped.

In addition to maintaining call state information, information is retained in order to:

- Recover IPsec manager policies, all template maps, and all subscriber maps.
- Use the policies (including templates) to recover CHILD SA tunnels, flow IDs, and statistics.
- Recover or reconfigure NPU flow IDs and data path handles.
- Recover and restore the IKEv2 stack state for all tunnels.
- Supply the IKEv2 stack with needed data statistics to determine rekey and DPD states.
- Recover Diameter session information.

Recovery requires a complex interaction between IPsec and session subsystems. The IPsec subsystem also interacts with a Datapath that includes daughter cards, daughter card managers, and the NPU. The session recovery feature is disabled by default on the system, even when the feature use key is present.

The IPsec controller does not send an IPsec manager death notification to any subsystem. This allows the daughter card to continue to receive and decrypt IPsec tunnel data. It also allows both the session manager and daughter card to continue carrying subscriber traffic using NPU flows and IPsec SAs to transmit the data.



A session manager is created on a PSC and a corresponding AAA manager is created on a different PSC but is created with the same instance number. A session manager saves (check-points) its Call Recovery Record (CRR) on the AAA manager with an instance ID the same as its own. This pairs up the session manager and the AAA manager and at the same time guarantees session recovery in the event of a single PSC failure.

IPSec manager is also created on a PSC. When a PDIF call request arrives, the IPSec manager picks a session manager for this particular call using a demux library on the same PSC. This means the IPSec manager is associated with the session managers on the PSC.

The session subsystem continues to use the AAA manager as its storage system for the PDIF because AAA needs to provide other subscriber-related information to the session manager. Now that the session manager and the IPSec manager are paired on the same PSC, the IPSec manager is assured of data recovery in case of PSC failure. This is because the session manager saves its data on the AAA manager on a backup PSC.

---


 **IMPORTANT:** For more information, refer to the *PDIF Session Recovery* chapter in the *System Enhanced Features Configuration Guide*.

---

## Intelligent Packet Monitoring System (IPMS)

The IPMS provides a control-packet capture, database, and query facility. It provides the functions to assist operators to analyze and investigate call-related events at a later time.

---


 **IMPORTANT:** IPMS is described in the *IPMS System Administration Guide*.

---

## Multiple Traffic Selectors

The PDIF can be configured with multiple IPSec traffic classes, each containing up to 128 traffic selectors, which are used during traffic selector negotiation with UEs. Multiple traffic selectors allow the PDIF to direct outbound traffic to selected IP addresses based on the following protocols: IP, TCP, UDP, and ICMP. The PDIF can also direct TCP and UDP traffic to selected IP addresses and port ranges.

---

 **IMPORTANT:** In this software release, the PDIF supports IPv4 traffic selectors only.

---

Per RFC 4306, when a packet arrives at an IPSec subsystem and matches a 'protect' selector in its Security Policy Database (SPD), the subsystem must protect the packet via IPSec tunneling. Traffic selectors enable an IPSec subsystem to accomplish this by allowing two endpoints to share information from their SPDs. Traffic selectors can be used to assure that both endpoint SPDs are consistent and can aid in the dynamic update of an SPD. Traffic selector payloads contain the selection criteria for packets being sent over IPSec security associations (SAs).

During traffic selector negotiation, each endpoint sends two traffic selector payloads in the messages exchanged during the creation of an IPSec SA. The first traffic selector payload is known as the TSi (Traffic Selector-initiator) and the second is known as the TSr (Traffic Selector-responder). Each traffic selector payload contains one or more traffic selectors, and each traffic selector can contain an IP address range, a port range, and an IP protocol ID. During traffic selector negotiation between the UE and the PDIF, the UE assumes the role of the initiator as it initiates an IPSec SA for

its traffic, and the PDIF assumes the role of the responder. The PDIF can use multiple traffic selectors in its role as the responder.

Traffic selectors are applied to calls via an AAA attribute. During call setup, the PDIF's AAA manager selects the traffic class to use for a call based on the Radius vendor-specific attribute (VSA) TrafficSelector-class, which is received from the AAA server. The PDIF's Session Manager passes the selected traffic class configuration from its AAA Manager to its IPsec Manager, which then sends the traffic selectors to the UE in the TSr for all CHILD SAs in the call. If no matching traffic selector classes or traffic selectors have been configured on the PDIF, or if the PDIF does not receive the TrafficSelector-class attribute from the AAA server, or if the value of the received TrafficSelector-class attribute is 0, the PDIF returns the default traffic selector to the UE in the TSr, which allows all inbound traffic.

The PDIF saves the traffic class configuration in each call during call setup. Configuration changes made to the existing traffic class configuration will apply to new calls only. There is no hard limit to the maximum number of allowed traffic classes, but the recommended limit is 50.

When incoming traffic from a UE does not match any of the configured traffic selectors, the PDIF does not reject the traffic. Instead, the PDIF keeps a per-call counter to record the number of packets that do not match the configured traffic selectors. Outgoing traffic from the PDIF to the UE is not subject to traffic selection or checking.

## Selective Diameter Profile Update Request Control

For mobile IP calls, the Selective Diameter Profile Update Request Control feature allows WiFi data-only sessions to co-exist with VoIP sessions on the PDIF platform.

When the PDIF is accessed by voice-enabled devices, it needs to interact with the HSS in order for a subscriber session to access the IP core network. When the PDIF is accessed by data-only devices, there is no need to interact with the HSS.

This feature is used to identify which subscriber sessions need to have the PDIF and the HSS exchange Diameter Profile Update Request (PUR) and Profile Update Answer (PUA) messages, and allows the PDIF to handle the call setup for a data-only client without having to interact with the HSS.

Selective PUR profiles on the AAA server are mapped to subscribers during AAA authentication via the Radius vendor-specific attribute (VSA) FMC-Type. FMC-Type has these possible values: voice or data. When the AAA server sets the FMC-Type value to voice, the PDIF and the HSS exchange PUR and PUA messages. When the AAA server sets the FMC-Type value to data, the PDIF and the HSS do not exchange PUR and PUA messages.

This feature is enabled by default and requires no configuration.

# Supported Standards and RFCs

## 3GPP2 References

- P.S0001-B Version 2.0 cdma2000 Wireless IP Network Standard
- X.S0011-001-C v3.0 cdma2000 Wireless IP Network Standard; Introduction
- X.S0011-002-C v3.0 cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Services
- X-S0013-000-A v1.0 All-IP Core Network Multimedia Domain - Overview
- X.S0013-010-0 v2.0 All-IP Core Network Multimedia Domain - IP Multimedia Subsystem Sh Interface; Signaling Flows and Message Contents – Stage 2
- X.S0013-010-A v1.0 All-IP Core Network Multimedia Domain - IP Multimedia Subsystem Sh Interface; Signaling Flows and Message Contents – Stage 2
- X.S0013-011-A v1.0 All-IP Core Network Multimedia Domain - Sh Interface Based on Diameter Protocol; Protocol Details – Stage 3
- X.S0016-000-B v1.0 3GPP2 MMS Specification Overview Multimedia Messaging System Specification
- X.S0016-000-C v1.0 Multimedia Messaging Service - Overview
- X.S0028-000-0 v1.0 cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking - List of Parts
- X.S0028-100-0 v1.0 cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking - Access to Internet
- X.S0028-200-0 v1.0 cdma2000 Packet Data Services: Wireless Local Area Network (WLAN) Interworking - Access to Operator Service and Mobility

## IETF References

- RFC 1594 (March 1994): “FYI on Questions and Answers to Commonly asked “New Internet User” Questions”
- RFC 2104 (February 1997): “HMAC: Keyed-Hashing for Message Authentication”
- RFC 2401 (November 1998): “Security Architecture for the Internet Protocol”
- RFC 2403 (November 1998): “The Use of HMAC-MD5-96 within ESP and AH”
- RFC 2404 (November 1998): “The Use of HMAC-SHA-1-96 within ESP and AH”
- RFC 2405 (November 1998): “The ESP DES-CBC Cipher Algorithm With Explicit IV”

- RFC 2451 (November 1998): “The ESP CBC-Mode Cipher Algorithms”
- RFC 3526 (May 2003): “More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)”
- RFC 3539: (June 2003): “Authentication, Authorization and Accounting (AAA) Transport Profile”
- RFC 3588 (September 2003): “Diameter Base Protocol”
- RFC 3602 (September 2003): “The AES-CBC Cipher Algorithm and Its Use with IPSec”
- RFC 3706 (February 2004): “A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers”
- RFC 3775 (June 2004): “Mobility Support in IPv6”
- RFC 4187 (January 2006): “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement”
- RFC 4301 (December 2005): “Security Architecture for the Internet Protocol”
- RFC 4302 (December 2005): “IP Authentication Header”
- RFC 4303 (December 2005): “IP Encapsulating Security Payload (ESP)”
- RFC 4305 (December 2005): “Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”
- RFC 4306 (December 2005): “Internet Key Exchange (IKEv2) Protocol”
- RFC 4307 (December 2005): “Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)”
- RFC 4308 (December 2005): “Cryptographic Suites for IPSec”
- RFC 4718 (October 2006): “IKEv2 Clarifications and Implementation Guidelines”
- RFC 4835 (April 2007): “Cryptographic Algorithm Implementation RFC Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)”

## Object Management Group (OMG) Standards

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

# Chapter 2

## Configuration

---

This chapter provides configuration information for the PDIF software. It contains the following procedures:

- [Configure the PDIF for Mobile IP or Proxy Mobile IP](#)
- [Configuring IPSec Traffic Classes and Traffic Selectors](#)



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

---

# Configure the PDIF for Mobile IP or Proxy Mobile IP

The PDIF supports two network types:

- Networks in which subscribers use handsets with IP stacks that support mobile IP and simple IP fallback when mobile IP calls fail.
- Networks in which the handsets do not support mobile IP, but use proxy mobile IP instead. Although not a requirement for proxy mobile IP per se, this document describes proxy mobile networks as configured using multiple authentication, whereby two authentication modes are configured.

This section explains how to configure the PDIF for mobile IP with the option for simple IP fallback, or mobile IP with multiple authentication.



**IMPORTANT:** Because of the complexities inherent in networks, this section provides the minimum configuration to start a basic system. Follow the references to other manuals for complete information on all commands and their options.

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to function as a PDIF in a test environment.

- Step 1** Set system configuration parameters such as activating PSCs/PSC2s, configuring administrators, and configuring remote access by applying the example configurations found in the *System Administration Guide*.
- Step 2** Set initial PDIF configuration parameters such as creating the PDIF context and PDIF service by applying the example configurations found in the section [Initial Configuration](#).
- Step 3** Configure the system to function as a PDIF that supports mobile IP and proxy mobile IP sessions by applying the example configurations found in section [PDIF Configuration](#).
- Step 4** Save the configuration as described in the chapter *Verifying and Saving Your Configuration* in this guide.

## Initial Configuration

- Step 1** Set local system management parameters by applying the example configuration in the section [Modify the Local Context](#).
- Step 2** Create the PDIF context by applying the example configuration in the section [Create the PDIF Context](#).

## Modify the Local Context

Use the following example to set the default subscribers and configure remote access capability in the local context.

```
configure
    context local
```

```
interface <lcl_cntxt_intrfc_name>
    ip address <ip_address> <ip_mask>
    exit
server ftpd
    exit
server telnetd
    exit
subscriber default
    exit
administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> next hop <next_hop_addr>
<lcl_cntxt_intrfc_name>
    exit
aaa default-domain subscriber <defdomsub1>
aaa last-resort context subscriber <lastressub1>
port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
end
```

## Create the PDIF Context

Use the following example to create the PDIF context and Ethernet interface and bind the interface to an Ethernet port.

config

```
context <pdif_context_name>
    interface <pdif_iface_name>
        ip address <ip_addr> <netmask>
        exit
    ip route <default_gateway IP_address> nexthop <ip_addr> <pdif_iface_name>
exit
```

```
port ethernet <slot_num/port_num>

no shutdown

bind interface <pdif_iface_name> <pdif_context_name>

end
```

## PDIF Configuration

- Step 1** Configure the PDIF service and the FA context and service by applying the configuration in the section [Create the PDIF Service](#).
- Step 2** Create an EAP authentication profile by applying the configuration in the section [Create the EAP Profile](#).
- Step 3** Create from one to six IKEv2 transform sets and from one to four IPSec transform sets by applying the configuration in the section [Create the IKEv2 and IPSec transform sets](#).
- Step 4** Create the crypto template for the IKEv2 SA negotiation and apply the EAP authentication profile by applying the configuration in the section [Create the Crypto Template](#).
- Step 5** Establish the IKEv2 crypto negotiation set based on the crypto template to create the initial Tunnel Inner Address for signaling or simple IP traffic by applying the configuration in the section [Establish the Initial IKEv2 SA Tunnel Inner Address \(TIA\)](#).
- Step 6** Establish whether there is to be a second IPSec SA for mobile IP calls by applying the configuration in the section [Establish the IPSec Child SAs for MIP Sessions](#).
- Step 7** Create the default subscriber by applying the configuration in the section [Configuring the Default Subscriber](#).
- Step 8** Configure the IMS-SH service so the PDIF can validate the WiFi AP MAC address per subscriber and bind it to an interface by applying the configuration in the section [Configuring the IMS-SH Service](#).
- Step 9** Configure the Diameter endpoint with the PDIF hostname, peer configuration, and other Diameter base information by applying the configuration in the section [Configuring the Diameter Endpoint](#).
- Step 10** Configure AAA interfaces and AAA groups by applying the configuration in the section [Configuring AAA Interfaces and AAA Groups](#).
- Step 11** Configure the FA service by adding the fa-ha-spi number and binding the interface to the fa-ha interface address configured in the PDIF context by applying the configuration in the section [Configuring the FA Service](#).
- Step 12** Configure the HA context and service by adding the fa-ha-spi number and binding the interface to the ha-fa interface address configured in the PDIF context by applying the configuration in the section [Configuring the HA Service](#).
- Step 13** Bind the logical interfaces to physical ports by applying the configuration in the section [Binding the Interfaces to Physical Ports](#).



## Create the PDIF Service

Use the following example to create the PDIF-Service and the FA context and service and bind them to the crypto template.

```
config
    context <pdif_context_name>
        pdif-service <pdifserv1>
            mobile-ip foreign-agent context <fa_context> fa-service <fa-1>
            aaa authentication first-phase context-name <pdif_context_name> aaa-
group <Diameter>
            aaa authentication second-phase context-name <pdif_context_name> aaa-
group <Radius>
            bind <ip_address> crypto-template <crypto_template_name>
        end
```

## Create the EAP Profile

Use the following commands to configure an EAP authentication profile.

```
config
    context <pdif_context_name>
        eap-profile <profile_name>
    end
```

Optional: For a proxy mobile IP application, create a second profile as shown below. The first profile must use the defaults.

```
config
    context <pdif_context_name>
        eap-profile <profile_2_name>
            mode authenticator-terminate method eap-md5 eap-gtc
        end
```

## Create the IKEv2 and IPSec transform sets

Use the following configuration example to create the required number of transform sets.

```
configure

  context <pdif_context_name>

    ikev2-ikesa transform-set <ikev2-tset1>

    exit

  ipsec transform-set <ipsec-tset1>

end
```

## Create the Crypto Template

Use the following configuration example to create the crypto template and apply the subscriber EAP authentication profile.

```
config

  context <pdif_context_name>

    crypto template <crypto_template_name> ikev2-pdif

    authentication eap profile <profile_name>

  end
```

Optional: For a proxy mobile IP installation, apply both EAP profiles with the **authentication eap profile** <profile\_name> **second-phase eap profile** <profile\_2\_name> command in the Crypto Template mode.

## Establish the Initial IKEv2 SA Tunnel Inner Address (TIA)

Use the following configuration example to begin IKEv2 cryptographic exchange based on the crypto template to try to create an initial Security Association (SA) signaling tunnel.

```
config

  context <pdif_context_name>

    crypto template <template_1> ikev2-pdif

    ikev2-ikesa transform-set list <ikesa-tset1>

    payload <load-1> match childsa

    ip-address-allocation home-address
```

```
ipsec transform-set list <ipsec_tset1>
exit
```

## Establish the IPSec Child SAs for MIP Sessions

Use the following configuration example to establish whether or not there will be a Child SA to allow a mobile IP call based on payload contents.

```
payload <load-2> match childsa
ipsec transform-set list <ipsec-tset1>
end
```

Note:

There is a maximum of two payloads allowed.

## Configuring the Default Subscriber

Use the following example to configure the Default Subscriber.

```
config
context <pdif_context_name>
subscriber <default>
aaa group <diameter-group1>
ip context-name <egress_context_name>
mobile-ip home-agent <ip-address>
```

Optional: Enable proxy mobile IP with the **proxy-mip-required** command in the default subscriber mode.

Optional: Enable simple IP fallback with the **pdif mobile-ip simple-ip-fallback** command in the default subscriber mode.

Optional: Release the Tunnel Inner Address IP address back to the IP pool when the IPSec SA is created with the **pdif mobile-ip release-tia** command in the default Subscriber mode.

## Configuring the IMS-SH Service

Use the following example to configure the ims-sh service.

```
config
context <pdif_context_name>
```

```

pdif-service <service-1>
    ims-sh-service name <sh-service-name>
    exit
ip route <ip_address> <netmask> nexthop <ip_address> <egress-1>
interface <ims-Sh-1>
    ip address <ip_address> <netmask>
    exit
ims-sh-service <sh-service_name>
    diameter dictionary <custom_dictionary_number>
    diameter endpoint <endpoint_name>
end

```

## Configuring the Diameter Endpoint

Use the following example to configure the Diameter endpoint.

```

config
    context
        diameter endpoint <endpoint_name>
            origin realm <carriername.com>
            use proxy
            origin host <host-name.carriername.com> address <hss-interface-
ip_address>
            peer <peer.hss1.carriername.com> realm <carriername.com> address
<ip_address>
            route-entry realm <carriername.com> peer <peer.hss1.carriername.com>
        exit
    exit

```

## Configuring AAA Interfaces and AAA Groups

Use the following example to configure AAA interfaces and AAA groups.

```

config

```

```

context <pdif_context_name>
    interface <pdif-1AAA-link>
        ip address <ip_address> <subnet_mask>
    interface <pdif-hss-diameter-link>
        ip address <ip_address> <subnet_mask>
    interface <pdif-MS-link>
        ip address <ip_address> <subnet_mask>
    interface <fa-ha-interface>
        ip address <ip_address> <subnet_mask>
    exit
aaa group <default_RADIUS>
    radius attribute nas-ip-address address <ip_address>
    radius accounting interim interval <integer>
    radius dictionary <custom_number_X>
    radius server <ip_address> encrypted key <key> port <port_num>
    radius accounting server <ip_address> encrypted key <encrypted_key> port
<port_num>
    aaa group <DIAMETER>
        diameter authentication dictionary <aaa_custom-dictionary>
        diameter authentication endpoint <point-1>
    end

```

Note:

You cannot set the **radius attribute nas-ip-address** command if **large configuration** was not previously configured.

## Configuring the FA Service

Use the following example to configure the FA service and bind it to an interface.

```

config
    context <pdif_context_name>
        fa-service <fa-1>

```

```

        fa-ha-spi remote-address <ha-spi-ipaddress> spi-number <integer>
encrypted secret <secret>

        authentication mn-ha allow-noauth

        bind address <fa-ha-int_ip_address>

        proxy-mip allow

        revocation enable

```

Note:

For Proxy-MIP installations, registration revocation can only be enabled on the HA. See the “Proxy Mobile IP” chapter of the *System Enhanced Feature Configuration Guide* for more information.

## Configuring the HA Service

Use the following example to configure the HA context and service and bind it to an interface.

```

config

    context <ha_context>

        interface <ha-fa_int>

            ip address <ha-fa-int_ip_addr/netmask>

            exit

        subscriber <default>

        dns primary <ip_addr>

            ip context-name <context-isp2>

            exit

        aaa group <default>

            exit

    context <ha-context>

        ha-service <ha-1>

            fa-ha-spi remote-address <ha-fa-int_ip_addr/netmask> spi-number
<integer> encrypted secret <secret> timestamp-tolerance <integer>

            authentication mn-aaa allow-noauth

            authentication mn-ha allow-noauth

            revocation enable

```

```
bind address <mip-ha_ip_address>
end
```

## Binding the Interfaces to Physical Ports

Use the following example to bind the various logical interfaces to physical ports.

```
config
    context <context_name>
        fa-ha-spi remote-address <ip_address> spi-number <integer> encrypted
secret <password>
        bind address <ip_address>
        exit
    ha-service <ha-serv1>
        mn-ha-spi spi-number <integer> encrypted secret <password>
        fa-ha-spi remote-address <ip_address> spi-number <integer> encrypted
secret <password>
        authentication mn-ha allow-noauth
        revocation enable
        bind address <ip_address>
        exit
    port ethernet <slot/port>
        no shutdown
        bind interface <spi01> <local-name>
        exit
    port ethernet <slot/port>
        no shutdown
        bind interface <pdif_iface1> pdif
        exit
    port ethernet <slot/port>
        no shutdown
```

```
    bind interface <AAA-interface> pdif
    exit
port ethernet <slot/port>
    no shutdown
    bind interface <ims-Sh-1> pdif
end
configure
    no autoconfirm
```



# Configuring IPsec Traffic Classes and Traffic Selectors

To configure IPsec traffic classes and traffic selectors:

- Step 1** Create inbound access control lists (ACLs) to define the required traffic classes and traffic selectors, as described below in [Creating Access Control Lists to Define IPsec Traffic Classes and Traffic Selectors](#).
- Step 2** Verify your ACL configuration by following the steps below in [Verifying the ACL Configuration](#).
- Step 3** Save your configuration as described in the chapter *Verifying and Saving Your Configuration* in this guide.



**IMPORTANT:** This section includes information on how to use ACLs to configure IPsec traffic classes and traffic selectors on the PDIF platform. For more complete information on ACLs, see the *Access Control Lists* chapter in the *System Enhanced Feature Configuration Guide*.

## Creating Access Control Lists to Define IPsec Traffic Classes and Traffic Selectors

A single ACL consists of one or more ACL rules. An ACL rule is a filter configured to take a specific action for packets matching specific criteria. To configure traffic classes and traffic selectors, you create inbound ACLs that conform to the following guidelines:

- Each traffic class is represented by one ACL.
- Each ACL name must match a traffic class name defined on the AAA server.
- An ACL name representing a traffic class must be an integer.
- Each traffic selector is represented by one 'permit' entry in an ACL. Each 'permit' entry defines one selection criterion for packets being sent over IKE security associations (SAs).
- Traffic selectors are created using 'permit' entries only (no 'deny' or 'redirect' entries are allowed).
- The specified source address must be 'any'.
- The criteria used for traffic selectors can be based on these protocols: IP, TCP, UDP, and ICMP.
- You can specify a port range only if the criteria is TCP or UDP.
- ACLs created for traffic classes and traffic selectors are not applied to individual interfaces, all traffic within a context (known as a policy ACL), individual subscribers, multiple subscribers, or multiple subscribers via access point names (APNs).

## Defining Traffic Classes

To define traffic classes, create inbound ACLs by issuing the following command in Context Configuration Mode for the egress context:

```
ip access-list acl_name
```

Each ACL that you create by issuing this command defines a unique traffic class. Executing this command enters the Access Control List Configuration Mode, in which rules and criteria are defined for the ACL. In this mode, you issue the **permit** command to create traffic selectors.

## Defining Traffic Selectors

For traffic selectors based on IP packets, issue the following CLI command in Access Control List Configuration Mode:

```
permit ip any { dest_address dest_wildcard } { protocol num }
```

For traffic selectors based on TCP or UDP packets, issue the following CLI command in Access Control List Configuration Mode:

```
permit {tcp | udp} any { dest_address dest_wildcard } [ range start_port  
end_port | eq dest_port | gt dest_port | lt dest_port | neq dest_port ]
```

To specify a port range of 10 to 3000, you would enter: **range 10 3000**

You can also use these options to define a port or port range: lt (less than), gt (greater than), eq (equal to), and neq (not equal to).

For ACL rules that define IPSec traffic selectors using the range option with the neq (not equal to) option, the PDIF translates each rule into two traffic selectors (except 0 and 65535). For example, the PDIF splits the result of **range neq 3** into two traffic selectors defining port ranges 0-2 and 4-65535.

In addition, if the PDIF translates the configured ACL rules into more than 128 traffic selectors (which is the limit), the PDIF includes the first 128 traffic selectors in the TSr in the outgoing IKE-AUTH packet to the MS.

For traffic selectors based on ICMP packets, issue the following CLI command in Access Control List Configuration Mode:

```
permit icmp any { dest_address dest_wildcard }
```

Use the following configuration example to create an ACL for a traffic class that contains two traffic selectors, one each for inbound TCP and UDP traffic:

```
configure
  context <egress_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp any <dest_address> <dest_wildcard> range
        <start_port> <end_port>
      permit udp any <dest_address> <dest_wildcard> range
        <start_port> <end_port>
    end
```



**IMPORTANT:** For definitions of all keywords and options available for ACLs, see the *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

## Verifying the ACL Configuration

Verify that your ACL rules and actions are configured properly by entering the following command in Exec Mode for the egress context:

```
show ip access-list
```

Sample output for this command is shown below. In this example, you would use the output to verify that ACL 100 was created with two traffic selectors, one each for inbound TCP and UDP traffic:

```
ip access list 100
    permit tcp any 1.2.3.4 0.0.0.0 range 10 3000
    permit udp any 1.2.3.0 0.0.0.255 range 20 4000
1 ip access-lists are configured.
```



# Chapter 3

## Maintenance

---

This chapter explains the online upgrade process for the PDIF chassis. It contains the following procedure:

[Configuring an Online Upgrade](#)

## Configuring an Online Upgrade

This section explains how to configure an online upgrade so that an online PDIF can be shut down for an upgrade without dropping any completed sessions.

A primary PDIF chassis (P) is temporarily connected to a backup PDIF chassis (B). PDIF (B) has the same configuration as PDIF (P). Once PDIF (P) and PDIF (B) are synchronized with established calls, switchover is initiated. PDIF (B) temporarily assumes the role of the active PDIF chassis while the original primary chassis (P) is upgraded. During the upgrade process, the DNS prevents all new calls to PDIF (P) and redirects them to PDIF (B).

Once the upgrade is complete, PDIF (P) is rebooted, and after PDIF (P) and PDIF (B) are synchronized, the switchover puts PDIF (P) back on line. PDIF (B) is removed from the system and configured for another upgrade elsewhere in the network.



**IMPORTANT:** There is no fault detection or redundancy enabled during the upgrade process.

To configure an online upgrade:

- Step 1** Make sure you have appropriate provisions for a successful upgrade as described in the section [Prerequisites](#).
- Step 2** Familiarize yourself with the organizational flow by referring to the chart found in the section [Software Upgrade Process](#).
- Step 3** Configure an SRP context and bind it to an interface as described in the section [Configuring and Binding an SRP Context](#).
- Step 4** Create interfaces and apply the Virtual MAC Address as described in the section [Creating Interfaces and the SRP Virtual MAC Address](#).
- Step 5** Upgrade the Primary chassis as described in the section [Upgrading the Primary Chassis](#).
- Step 6** Restore the Primary chassis to a live condition as described in the section [Completing the Upgrade](#).



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

## Prerequisites

The following lists the prerequisites for a successful upgrade:

- PDIF Primary (P) is an online chassis, with PDIF Backup (B) used solely for upgrades in a non-redundant system.
- The backup chassis needs to have at least as many SMC and PSC cards as the primary chassis. It is not important if the backup has additional cards.
- Provide a secure transfer protocol like SFTP. FTP is not recommended.

- The initial primary chassis configuration should use loopback interfaces in the ingress, egress, and AAA contexts, and for the IP pools. This is required because SRP can be activated only for loopback interfaces. The only exception to this would be the SRP context interface. This interface should be on a physical port that does not use an SRP virtual MAC address. This is required because the SRP context interface is active at the same time in both the Primary and Backup chassis.

Only Administrator and Config-Administrator-level users can provision online upgrades. Refer to the *Configuring System Settings* chapter of the *System Administration and Configuration Guide* for additional information on administrative user privileges.

## Software Upgrade Process

Follow the high-level steps below to perform a software upgrade. The figure below illustrates these steps.

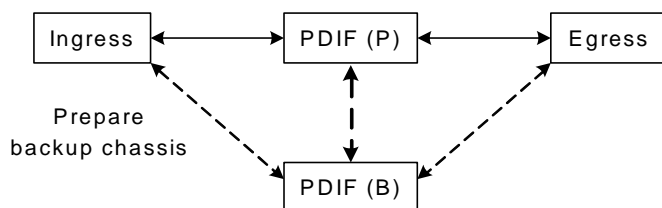
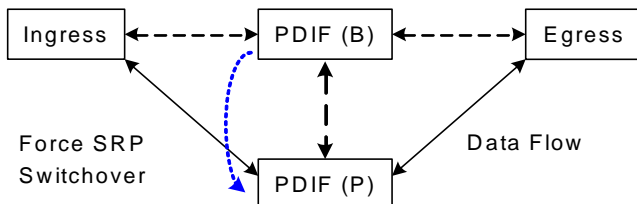
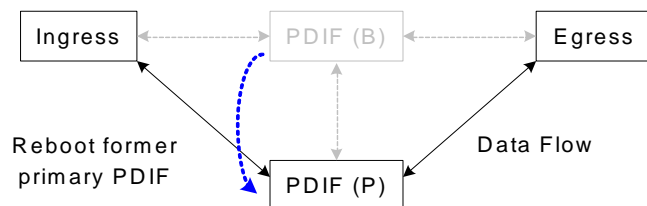
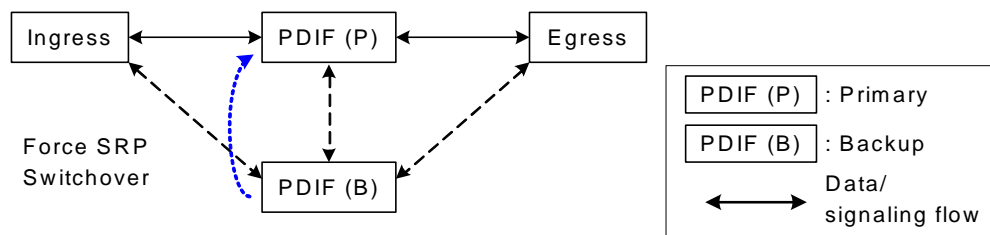
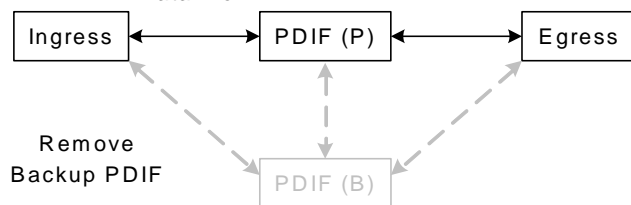
- Step 1** On PDIF (B), create a mirror-image of the configuration on PDIF (P). The DNS disconnects PDIF (P) and sends all new calls to other PDIFs on the network.
- Step 2** Once the upgrade configuration has been verified through the CLI commands, allow time for PDIF (B) to synchronize with PDIF (P). Force an SRP switchover so that PDIF (B) becomes active and begins processing the traffic that PDIF (P) handled.
- Step 3** Upgrade the offline PDIF (P).



**IMPORTANT:** During the upgrade, the configuration with the neighboring routers or switches remains unchanged, because PDIF (P) and PDIF (B) share a virtual IP address.

- Step 4** Reboot PDIF (P). Allow time for PDIF (P) and PDIF (B) to synchronize over the SRP link. Force an SRP switchover so that PDIF (P) is active once again. Once the switchover has completed, the DNS makes PDIF (P) live on the network and calls are again sent to PDIF (P).
- Step 5** At this point the upgrade is complete and the PDIF (B) can be reconfigured to upgrade another primary PDIF.

## Software Upgrade Process

**STEP 1: Data Flow****STEP 2:****STEP 3:****STEP 4: Data Flow****STEP 5: Data Flow**

## Configuring and Binding an SRP Context

This section explains how to configure SRP to enable an online upgrade.



- Step 1** The SRP context needs to be configured and bound to an interface to enable SRP. This must be configured first on PDIF (P) with the command **chassis-mode primary**.
- Step 2** Apply the configuration to PDIF (B) with the command **chassis-mode backup**.
- Step 3** Add the new software to Primary (P).

```
context <srp>
    service-redundancy-protocol
        bind address <ip-address>
        peer ip-address <ip-address>
        hello-interval <value>
        default configuration-interval
        dead-interval <value>
        chassis-mode primary
        route-modifier threshold <integer>
        checkpoint session duration <integer>
        srp-monitor authentication-probe context <string> address <ip-
address>
        port <portnum>
        exit
    interface srp
        ip address <ip_address> <subnet_mask>
        srp validate-configuration
        srp initiate-switchover timeout <value> -noconfirm
        exit
```

Notes:

- Configure the dead-interval value to be low (num = 1), and once the state is Active, set it to a higher value to ensure that PDIF (P) maintains primary status until the **srp-switchover** command is invoked.
- **peer ip-address** configures the remote peer IP address. If this configuration is being loaded on PDIF (P), then the peer IP address is the IP address of PDIF (B). If this configuration is being loaded on PDIF (B), the peer IP address is the IP address of PDIF (P). Exercise caution here: the **chassis-mode** command changes the device status on the primary and backup PDIFs such that whichever chassis (P) or (B) is actively

processing sessions is automatically considered Primary. This command can only be executed on the chassis that is acting as the primary chassis.

- The **srp validate-configuration** command initiates a configuration validation check from the primary chassis before making the switchover.
- The **srp initiate-switchover** command changes the device status of the PDIF that is acting as the Primary to become the Backup and vice versa.



**IMPORTANT:** The **srp initiate-switchover** command can only be executed on the primary chassis.

## Creating Interfaces and the SRP Virtual MAC Address

```
context <context-name1>

  interface <interface_1>

    ip address <ip-addr> <subnet mask>

  exit

  interface <loop1> loopback

    ip address <ip-addr> <netmask>

  exit

exit

port ethernet <slotnum/portnum>

  bind interface <interface_1> <context-name_1>

  srp virtual-mac-address <mac_address>

exit

vlan <vlan_1>

  no shutdown

  bind interface <interface_1> <context-name1>

  exit

vlan <vlan_2>

  no shutdown

  bind interface <interface_2> <context-name2>

  exit
```

Notes:

- The SRP virtual MAC address is applied to the port when the chassis is in SRP Active state. The default is **no srp virtual-mac-address**.
- The loopback address should be 0.0.0.0/32

## Upgrading the Primary Chassis


You can now upgrade the Primary chassis.

- Step 1** Force an SRP switchover using the **srp initiate-switchover** command so that PDIF (B) becomes the active chassis. Once the switchover is complete, PDIF (B) is able to dispose of all the calls that used to be on Primary (P). The primary PDIF, PDIF (P), can now be upgraded through an offline upgrade without affecting the network.
- At this stage PDIF (P) is in SRP STANDBY state. The loopback interface *loop1* is disabled and the MAC address of the loopback interface is the same as the original MAC address of the physical port *<slotnum/portnum>*. The SRP virtual MAC address is used by PDIF (B) while in SRP ACTIVE state.
- Step 2** Reboot PDIF (P). Once the PDIF (P) has come back on line, and the chassis are synchronized, force an SRP switchover so that PDIF (P) is the active chassis.
- Step 3** Once the switchover is complete, add PDIF (P) back to the DNS active list so it can send new sessions to PDIF (P).

## Completing the Upgrade

At this point, the SRP configuration for online upgrade can be removed from the primary PDIF, and the backup PDIF can be physically removed. The upgrade is complete and the standby chassis can be reconfigured to upgrade another PDIF.

---

 **IMPORTANT:** Note that during the upgrade, the configuration to the neighboring routers/switches did not change because the ASR 5000s are sharing a virtual IP address.

---



# Chapter 4

## Troubleshooting

---

This chapter defines procedures for troubleshooting problems on a PDIF. It includes the following section:

[Troubleshooting the PDIF](#)

# Troubleshooting the PDIF

The following sections provide a variety of ways to troubleshoot a PDIF, from the physical (checking LEDs and port condition lights), to the analytical, with a large assortment of commands designed to show a wide array of statistics and counters.

## System Monitoring Tools

This section provides methods for monitoring a PDIF and ascertaining if it is running at optimal performance.

Useful monitoring commands are described in the chapters *Monitoring Hardware Status* and *Monitoring the System* in the *System Administration Guide*.

Hardware monitoring using the LEDs and replacing faulty line and application cards is covered in the *Hardware Installation and Administration Guide*.

SNMP notifications are configured in the chapter *Configuring Management Settings* in the *System Administration Guide*. All SNMP MIBs and traps are compiled in SNMP MIBs.

Event logging is described in the chapter *Configuring and Viewing System Logs* in the *System Administration Guide*.

Protocol monitoring is described in the chapter *Using the System's Diagnostic Utilities* in the *System Administration Guide*.

Bulk Statistics are described in the *System Administration Guide*. They are also listed in the *Command Line Interface Reference*.


## Generating Statistics

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Many commands have optional keywords in addition to those shown here. Full commands and keywords are found in the *Command Line Interface Reference*.

Output descriptions for most of the commands are located in the *Show Command Output Descriptions* appendix in the *Command Line Interface Reference*.

Table 6. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Subscriber Information	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	

To do this:	Enter this command:
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   all }</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 pdf-only subscriber sessions	<code>show subscribers pdf-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>
Display Session State PDIF Statistics	
View session state PDIF statistics	<code>show session progress pdf all</code>
Display Session Subsystem and Task Statistics	
 <b>IMPORTANT:</b> Refer to the <i>System Software Task and Subsystem Descriptions</i> appendix of the <i>System Administration Guide</i> for additional information on the Session subsystem and its various manager tasks.	
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 Session Manager statistics	<code>show session subsystem facility sessmgr all</code>

To do this:	Enter this command:
View IPSec Manager Statistics	<code>show session subsystem facility ipsecmgr all</code>
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	<code>show session disconnect-reasons all</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	
View Mobile IP FA counters for individual subscriber sessions	<code>show mipfa counters</code>
View Mobile IP Home Agent Statistics	
Display Mobile IP HA Information for a Specific Subscriber	
View Mobile IP HA counters for a specific subscriber	<code>show mipha full username <i>subscriber_name</i></code>
Display Mobile IP Statistics for HA Services	
View statistics for a specific HA service	<code>show mipha statistics fa-service <i>service_name</i></code>
Display Mobile IP HA Counters	
View Mobile IP HA counters for individual subscriber sessions	<code>show mipha counters</code>
Display IKEv2 IKESA Security Association Statistics	
View IKEv2 security associations	<code>show crypto ikev2 security-associations { summary   statistics }</code>
Display Crypto Statistics	
View cumulative IPSec statistics	<code>show crypto ipsec security associations</code>
View crypto template statistics	<code>show crypto statistics { [ service-ip-address <i>ip-address</i>] [ service-name <i>name</i>] [ crypto-template <i>name</i>] }</code>
View crypto managers statistics	<code>show crypto managers all</code>
Display PDIF statistics	
View cumulative PDIF statistics	<code>show pdif-service statistics all</code>
View statistics per PDIF-service	<code>show pdif-service statistics name <i>service-name</i></code>



## Clearing Statistics and Counters

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

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

## Network Connectivity Testing

The PDIF supports the normal Ping and Traceroute tests. However, Ping has been extended to provide IPv6 support. Note that the command is “**ping6**” and not “**PingV6**.”

The PDIF provides a debugging facility (through CLI commands and appropriate console outputs) to dynamically validate IPSec connectivity to the MS. This will be implemented via an IP ping sent over the tunnel to the IP address of the MS (either the HoA in the case of Mobile-IP or the TIA in the case of simple IP fallback). The subscriber session may be identified using NAI or MS IP address (such as TIA or HoA).

Traceroute users should be aware that the RADIUS attribute SN-IP-Hide-Service-Address can be used to prevent subscribers from using traceroute to discover the public domain network addresses configured for HA and other services.

## Session Termination Attributes

The following table is derived from the Acct-Termination-Cause RADIUS attribute (column 1), and from the 3GPP2-Release-Indicator attribute (column 5).

There are several disconnect scenarios on the PDIF (described below). Any single Acct-Termination-Cause value from Column 1 in the following table may be tied to multiple disconnect scenarios. The PDIF supports the Release-Indicator attribute values in Column 5 to differentiate each scenario and provide possible insight into the call failure cause.

**Table 7. Acct-Term-Cause and 3GPP2-Release-Indicator**

Acct-Terminate-Cause Value	Name	Definition in the RFC	Applicable condition in PDIF	Release-IndicatorValue
1	User Request	The user requests to terminate the service, with LCP termination or logout.	PDIF received INFORMATIONAL Request (Delete) and released the session.	3 - PPP-Termination
2	Lost Carrier	DCD of the port has dropped.	--	0- Unknown
3	Lost Service	Service cannot be provided; e.g., user access to the host was terminated.	a. IKE session was released because SA lifetime timer had expired.	7 - Service-Instance-Released

Acct-Terminate-Cause Value	Name	Definition in the RFC	Applicable condition in PDIF	Release-IndicatorValue
			b. MIP/SIP Lifetime expired.	1 - PPP/Service-Timeout
			c. MIP RRP Type2 included Reject Code.	4 - Mobile-IP-Registration-Failure
4	Idle Timeout	Idle-timeout timer expired.	Idle-timeout timer expired.	1 - PPP/Service-Timeout
5	Session Timeout	Session-timeout timer expired.	a. Session timeout timer expired.	1 - PPP/Service-Timeout
			b. Long-Duration-Timer expired.	1 - PPP/Service-Timeout
6	Admin Reset	Administrator reset a port or session.	--	0 - Unknown
7	Admin Reboot	Administrator stopped NAS service in order to prepare for the NAS reload.		0 - Unknown
8	Port Error	NAS detected a port error which required termination.		0 - Unknown
9	NAS Error	NAS detected an error (other than port error) which required session termination.	Registration Revocation from HA triggered session termination.	1008 - MIP-Registration-Revocation
10	NAS Request	Session was terminated for any reason that was not specific to errors listed in NAS.	a. PDIF detects MS has not responded with a keepalive and terminates the session.	0 - Unknown
			b. Overflow occurs in the accounting information.	0 - Unknown
			c. VisitorList was deleted.	0 - Unknown
11	NAS Reboot	Session was terminated because of NAS crash.	--	5 - Abnormal-Termination
12	Port Unneeded	Session terminated because the available resource is below configured value.		6 - Termination-Due-To-Resource-Mgmt
13	Port Preempted	NAS terminated the session to re-allocate the port		3 - PPP-Termination
14	Port Suspended	NAS terminated the virtual session.	a. Existing session released because duplicate HA Home Address detected.	3 - PPP-Termination
			b. Junk session detected and deleted upon receipt of new IKE_SA_INIT Request from MS.	7-Service-Instance-Released

Acct-Terminate-Cause Value	Name	Definition in the RFC	Applicable condition in PDIF	Release-IndicatorValue
15	Service Unavailable	NAS can not provide the requested service.	--	0 - Unknown
16	Callback	NAS has terminated the existing session because it needs to setup a new session for callback.	--	0 - Unknown
17	User Error	User input included errors, causing session termination.	a. If IKE_SA Rekeying fails	5 - Abnormal-Termination
			b. If CHILD_SA Rekeying fails	5 - Abnormal-Termination
			c. Counter value of Ingress Address filtering exceeded the threshold.	0 - Unknown
18	Host Request	Login host closed the session without any problem.	PMIP RRP (Code=0x80/0x82) was received.	4 - Mobile-IP-Registration-Failure

## Call Failure Scenarios

The following are some potential call failure scenarios. Note that these scenarios make the following assumptions:

- If a Callback-Id AVP is not received in the final DEA message during the first authentication, the session setup is terminated with appropriate error logs being generated.
- A DNS server provides IP addresses to the MS.
- Unless stated otherwise, the starting condition for these scenarios is that the MS established an IPSec session with the primary PDIF and registered with the MIP HA.

## MS Power-Down or Failure

If the MS powers down or fails without first deleting the IPSec session with the PDIF, the PDIF has no way to know this if no DPD is configured to notify the MS.

The PDIF tears down the IPSec session to the MS when the IPSec session timer expires or when the inactivity timer expires (whichever occurs first). When the MS comes back on line, it attempts to establish a new IPSec session with the PDIF. If the MS attempts to establish this new session before the old one times out, the PDIF detects that the IMSI of the MS is already registered to another IPSec session. The PDIF establishes the new session and then clears the old session, but only if the new IPSec session is successfully established.

However, with DPD configured to be sent to the MS, the PDIF actively deletes the IPSec session. If the MS attempts to establish a new session before the DPD mechanism triggers the session tear down, the PDIF detects that the IMSI of the

MS is already registered to another IPSec session, establishes the new session, and then clears the old session, but only if the new IPSec session is successfully established.

## The MS Temporarily Roams Away From the WiFi Access Point

The PDIF can detect this event if the MS temporarily roams away from the WiFi AP for sufficient amount of time and DPD is configured on the PDIF side. The PDIF deletes the IPSec session. However, it would not be able to detect this event if the DPD was not configured, since it could not initiate DPD exchanges with the MS.

Since the PDIF is no longer receiving DPD exchanges or user data from the MS, eventually the PDIF inactivity timer expires and the PDIF deletes the IPSec session.

If the MS roams back into the WiFi AP coverage area before the inactivity timer expires or before the DPD mechanism on the PDIF triggers session tear down, the MS resumes the existing IPSec session. Normal DPD exchanges resume, and the IPSec tunnel is available for FMC calls or other data activity.

This scenario does not address the question of how the MS knows that the roaming is temporary. If the MS roams into the CDMA network and registers with the HA, the IPSec session would be deleted. Thus, for this scenario to be valid, the MS must avoid roaming into the CDMA network during this temporary period.

Should it do so, the MIP registration with the HA is updated, causing the HA to send a MIP Registration Revocation Request to the PDIF, which deletes the IPSec session with the MS.

## MS Proxy-MIP Registration Failure

If the MS establishes an IPSec session but the Proxy-MIP registration attempt fails, the IPSec session is disconnected.

## MS Proxy-MIP Registration Renew Failure

If the MS establishes an IPSec session but the Proxy-MIP registration renew attempt fails because no RRP response is received or an RRP response indicating a failure is received, the PDIF deletes the IPSec session.

## MS MIP Registration Failure

If the MS establishes an IPSec session but the MIP registration attempt fails, the PDIF can fall back to simple IP mode on session setup timer expiry if an RRP response indicating failure has been received. If no RRP response is received, the PDIF will fall back to simple IP when the setup timer expires. Note that fallback to simple IP must also be enabled in the system configuration for this to occur.

## WiFi or Access Network Failure

The PDIF can detect the event if DPD is configured on the PDIF and if the failure lasts long enough for DPD to trigger a session teardown. The PDIF has no way to actively determine that the WiFi or access networks have failed if DPD is not configured. The behavior now becomes similar to that described in “MS Temporarily Roams Away From WiFi Access Point.”

## Total PDIF Failure

The MS can not detect a PDIF failure without DPD. It can only detect the failure when it no longer sends traffic or when some timers start to expire.

However, if DPD is configured on the MS, the MS can detect the PDIF failure. When the PDIF does not respond to the DPD exchange request, the MS declares the IPSec session failed and so attempts to establish a new IPSec session.

Since the primary PDIF is incapable of establishing a new IPSec session with the MS, it attempts to establish an IPSec session with a secondary PDIF if there is one available, with an IP address provided by the DNS server.

Assuming a secondary PDIF is available, the MS establishes a new IPSec session. Since the primary PDIF has failed completely, it is assumed that the old IPSec session from the MS has been lost. If this is not the case, the primary PDIF tears down the IPSec session with the MS when one of the following events happens:

- The MS receives mobile IP revocation from the HA.
- The IPSec session timer expires.
- The inactivity timer expires.

## Partial or Transient PDIF Failure

The MS can not detect a PDIF failure without DPD. It can only detect the failure when it no longer sends traffic or when some timers start to expire.

However, if DPD is configured on the MS, the MS can detect the PDIF failure. When the PDIF does not respond to the DPD exchange request, the MS declares the IPSec session failed and so attempts to establish a new IPSec session.

If the primary PDIF is capable of establishing a new IPSec session because the failure was partial or transitory, the MS establishes a new IPSec session with the original PDIF. When the PDIF determines that the IMSI of the MS is already registered to another IPSec session, it establishes the new session and then clears the old one.

If the primary PDIF is incapable of establishing a new IPSec session, the MS attempts to establish an IPSec session to the secondary PDIF provided by the DNS server. Assuming this secondary PDIF is available, the MS establishes a new IPSec session.

If the old IPSec session on the primary PDIF still exists despite the failure, the primary PDIF tears down the IPSec session to the MS when one of the following events happens:

- The MS receives MIP revocation from the HA.
- The IPSec session timer expires.
- The inactivity timer expires.

## HA Failure

If the HA fails, there is a health monitoring mechanism in the PDIF to generate an SNMP notification. At this time, all traffic to and from the MS is black-holed. DPD/liveness checks from the MS are still in order, so the connection remains in a hung state until the Proxy-MIP lifetime timer expires. When the PDIF attempts to re-register with the HA, the re-registration attempt fails, and the PDIF tears down the IPSec session. In this case, the MS attempts to establish a new IPSec session with the PDIF. If the HA has recovered, the IPSec session and Proxy-MIP session are re-established.

## General Error Cases for Mobile-IP Networks

The following are possible scenarios for mobile IP installations.

**Table 8. Mobile IP Error Scenarios**

	Error Description	Comments
1	For Mobile-IP session, CREATE_CHILD_SA should not include CP payload for INTERNAL_IP4_ADDRESS	If it is included, the session attempts are rejected and the complete IKEv2 session is disconnected.
2	For mobile IP session, CREATE_CHILD_SA request should have Tsi = HoA	If Tsi is not the same as HoA, PDIF falls back to simple IP when session setup timer expires (if this is allowed by configuration).
3	Diameter Error codes received from HSS	PDIF allows configurable for each error code whether to continue with the session setup or disconnect the session. Error logs are created.
4	MS does not initiate CREATE_CHILD_SA after PDIF/FA sends successful RRP	The session setup timer in PDIF/FA expires and session falls back to simple IP (if this is allowed by configuration).
5	If MS does not send RRQ when first/implicit TIA based SA created.	The session setup timer expires and session is disconnected clearing both IKEv2 SA and implicit TIA-based IPSec SA.
6	CREATE_CHILD_SA request fails after successful MIP registration.	Session falls back to simple IP when session setup timer expires (if this is allowed by configuration).
7	TIA pool is full and hence no address to assign during the initial IKEv2 negotiations	PDIF tears down the whole session attempt.
8	MS does not specify INTERNAL_IP4_ADDR attribute during IKEv2 negotiations.	PDIF tears down the whole session attempt since there is no way of assigning IP address to mobile
9	MS does specify a valid IP address INTERNAL_IP4_ADDR attribute during IKEv2 negotiations.	If MS gives an IP address, and if it is available in the static pool configured in the PDIF, then PDIF allows session to be established using the specified IP address. If MS gives the IP address of 0.0.0.0 then PDIF assigns an IP address from the pool. If MS gives an IP address that is not available in any of the static pools defined on the PDIF, then the PDIF disconnects the session.

## General Error Cases for Proxy Mobile IP Networks

The following are possible scenarios for proxy mobile IP installations where the MS handset is not capable of supporting mobile IP.

**Table 9. Proxy Mobile IP Error Scenarios**

	Error Description	Comments
1	PDIF and MS fail in negotiating security association algorithms through IKEv2 exchange	The session attempts are rejected and the IKEv2 session is disconnected.
2	MS authentication failure in any of the authentication procedures	The session attempts are rejected and the IKEv2 session is disconnected.
3	Diameter Error codes received from HSS	PDIF allows configurable for each error code whether to continue with the session setup or disconnect the session. Error logs are created.
4	MS Proxy-MIP registration fails	The session attempts are rejected and IKEv2 session is disconnected unless simple IP is allowed in the configuration.
5	IKEv2 packet from MS missing required payload.	The packet is dropped and the most likely scenario is that the IKEv2 session disconnects due to time out.
6	IKEv2 packet from MS is malformed or contains unsupported payload	The PDIF sends back IKEv2 response with appropriate notify payload if error notification is enabled or drops the IKEv2 packet quietly if error notification is disabled. The IKEv2 session is deleted when session setup timer expires or when retransmission time out times out. The connected session is deleted when session expires or when inactivity timer expires.
7	MS fails to respond to IKEv2 request packet from PDIF after configured number of retransmission attempts	The session attempts are rejected and IKEv2 session is disconnected.
8	There is no address to assign during the initial IKEv2 negotiations	PDIF will tear down the whole session attempt.
9	MS does not specify INTERNAL_IP4_ADDR attribute during IKEv2 negotiations	PDIF tears down the whole session attempt since there is no way of assigning IP address to mobile
10	MS does specify a valid IP address INTERNAL_IP4_ADDR attribute during IKEv2 negotiations.	If MS gives an IP address, and if it is available in the static pool configured in the PDIF, then PDIF allows session to be established using the specified IP address. If MS gives the IP address of 0.0.0.0 then PDIF assigns an IP address from the pool. If MS gives an IP address that is not available in any of the static pools defined on the PDIF, then the PDIF disconnects the session.

## IPMS Errors

IPMS is discussed in its own documentation set, but instructions for configuring PDIF to connect to an IPMS server appear in the Overview.

## IPMS Disconnect Reasons

IPMS disconnect reasons are typically generated in the session manager asynchronous to any actual package. The placeholder MISC event defined in the IPMS protocol is typically used to supply a disconnect reason.

Early in the demultiplexing phase, before any session manager is involved, it is possible that a disconnect reason is reported to the IPMS from the demux manager. These may be sent in a MISC placeholder event or, more commonly, attached to the buffered packet event of the aborted session.

## Show IPMS All Command

Enter the following command at the Exec mode prompt:

**show ipms status all**

The following is a sample output:

```
IPMS Server 1.1.1.1

Server State: UP

Heartbeats Sent: 100

Heartbeats Received: 99

Heartbeats Lost: 1

Last successful heartbeat: 2008-03-31:14:00:00

Last heartbeat roundtrip time: 5 ms

Last failed heartbeat: 2008-03-30:15:00:00

Assigned Client Tasks: 55

Transmit Overrun Errors: 321

Transmit Unreachable Errors: 123

Event Count
-----

IKEv2_SA_INIT Request 10

IKEv2_SA_INIT Response 10 IKEv2_AUTH Request 10

IKEv2_AUTH Response 10

IKEv2_CREATE_CHILD_SA Request 10

IKEv2_CREATE_CHILD_SA Response 10

AAA RADIUS Access Request 10
```



```
AAA RADIUS Access Reply 10
AAA RADIUS Accounting Start 10
AAA RADIUS Accounting Interim 10
AAA RADIUS Accounting Stop 10
MIP Registration Request 10
Total Events: 12345678
```



# Chapter 5

## Verifying and Saving Your Configuration

---

This chapter describes how to save the system configuration.

## Verifying the Configuration

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

### Feature Configuration

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

**show apn all**

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

```
access point name (APN): apn1
authentication context: test
pdp type: ipv4
Selection Mode: subscribed
ip source violation: Checked drop limit: 10
accounting mode: 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
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"> <li>• <code>{ /flash   /pcmcia1   /pcmcia2 } [ /dir ] /file_name</code></li> <li>• <code>file://{ /flash   /pcmcia1   /pcmcia2 } [ /dir ] /file_name</code></li> <li>• <code>tftp://{ ipaddress   host_name [ :port# ] } [ /directory ] /file_name</code></li> <li>• <code>ftp://{ username [ :pwd ] @ } { ipaddress   host_name } [ :port# ] [ /directory ] /file_name</code></li> <li>• <code>sftp://{ username [ :pwd ] @ } { ipaddress   host_name } [ :port# ] [ /directory ] /file_name</code></li> </ul> <p><b>/flash</b> corresponds to the CompactFlash on the SPC/SMC.  <b>/pcmcia1</b> corresponds to PCMCIA slot 1.  <b>/pcmcia2</b> 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"> <li>• tftp: 69 - data</li> <li>• ftp: 20 - data, 21 - control</li> <li>• sftp: 115 - data</li> </ul> <p>Note: <i>host_name</i> can only be used if the <b>networkconfig</b> 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 .cfg 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
```

# Appendix A

## Sample Configuration

---

This appendix contains a sample configuration file for a PDIF/FA with mobile IP operation. It includes the following section:

[Sample Mobile IP Configuration](#)

## Sample Mobile IP Configuration

This is a sample configuration file for a PDIF/FA configured for mobile IP operation.

In this sample, commented lines are labeled with the number symbol (#) and variables are identified using *<italics>*.

```
configure

license key <encrypted-key>

crash enable encrypted url <encrypted-url>

logging active

autoconfirm

aaa default-domain subscriber <sub_name_pdif>
aaa last-resort context subscriber <sub_name>
aaa large-configuration

threshold pdif-current-sessions <> clear <integer>
threshold poll pdif-current-sessions interval <integer>

card 4

    mode active psc

    exit

context local

    interface <spio1_interface>

        ip address <ip_address> <netmask>

        exit

    server ftpd

        exit

    ssh key <encrypted key>
    ssh key <encrypted key>
    ssh key <encrypted key>

    server sshd

        subsystem sftp
```

```
        exit
    server telnetd
    exit
    subscriber default
    exit
administrator admin-1 encrypted password <password> ftp
    ip route 0.0.0.0 0.0.0.0 3.2.2.1 <destination_context>
    ip domain-lookup
    ip domain-name <domain.com>          ip name-servers 1 <ip_address>
    exit
snmp engine-id local 800007e5805c83c5c1423b0bab
snmp community 1234567890 read-write
exit
ntp
enable
server <ip_address>
exit
context <pdif_context>
    interface <ethernet_iface_name>
        ip address <ip_address> <subnet_mask>
        port-switch-on-l3-fail address <ip_address_IPv6_address>
        exit
    pdif-service <servername>
    interface <pdif_interface_name> pdif_iface1
    ip address <ip_address> <netmask>
    exit
eap-profile <eap_profile_name>
mode authenticator-pass-through
exit
```

```
subscriber name <default_sub_name>

  pdif mobile-ip simple-ip-fallback

  pdif mobile-ip release-tia

  ip address <ip_address> <netmask>

  exit

ipsec transform-set <ipsec-tset_name>

exit

ikev2-ikesa transform-set <ikesa-tset1_name>

  crypto template <template_name> ikev2-pdif

    dos cookie-challenge notify-payload half-open-sess-count start
    <integer> stop <integer>

    authentication eap-profile <profile_name>

    exit

ikev2-ikesa policy error-notification invalid-message-id

ikev2-ikesa policy error-notification invalid-syntax

exit

ikev2-ikesa transform-set list <ikesa-tset_name>

ikev2-ikesa keepalive-user-activity

ikev2-ikesa setup-timer <integer>

  payload foo-sa0 match childsa

  ip-address-alloc dynamic

ipsec transform-set list <ipsec_tset_name>

  payload ipsec_tset1 match childsa

  ip-address-allocation home address

  no rekey

  natt

  no mobike

  no ikev2-ikesa rekey

  exit
```

```
interface <aaa-interface>
    ip address <ip_address> <netmask>
    exit
aaa group <default>
radius attribute nas-ip-address address <ip_address>
radius accounting interim interval <integer>
radius dictionary <custom_number_num>
radius server <ip_address> encrypted key <key> port <portnum>
radius accounting server <ip_address> encrypted key <key> port
<udp_port>
#Name the PDIF Service and configure FA context
    pdif-service <service-name>
        mobile-ip foreign-agent context <context_name> fa-service <fa-
service-name>
#Configure AAA attributes
    aaa attribute calling-station-id <string>
    aaa attribute 3gpp2-bsid <string>
    aaa attribute 3gpp2-service-option <integer>
    username mac-address-stripping
    hss mac-address-validation
    hss update-profile
    bind address <ip_address> crypto-template <template_name>
#Name Diameter Sh-service
    ims-sh-service name <sh_service_name>
    exit
ip route <ip_address_static> <netmask> nexthop <ip_address> local
interface <ims-sh-1_interfacename>
    ip address <ip_address> <netmask>
    exit
ims-sh-service <sh-service_name>
```

```
diameter endpoint <endpoint_name>

diameter dictionary <dictionary_custom_num>

exit

diameter endpoint <endpoint_name>

#Define origin realm

origin realm <realm-name>

origin host host-name.carrier.com address <ip_address>

peer <diameter-peer_name> realm carrier.com address
<ip_address>

route-entry realm carrier.com peer <peer-name>

exit

exit

#Create and bind FA context

context <fa_context>

interface <facontext-name>

ip address <ip_address>

exit

#Select default subscriber

subscriber <default>

exit

#Select AAA group default

aaa group <default>

exit

fa-service <fa-serv_name>

revocation enable

#Configure fa-ha SPI

fa-ha-spi remote-address <ip_address> spi-number <integer>
encrypted secret <secret>

bind address <ip_address>

exit
```



```
ha-service <ha-service-name>

#Configure mn-ha SPI

mn-ha-spi spi-number <integer> encrypted secret <secret>

fa-ha-spi remote-address <ip_address> spi-number <integer>
encrypted secret <secret>

authentication mn-ha allow-noauth

revocation enable

bind address <ip_address>

end

port ethernet <slotnum/portnum>

no shutdown

bind interface spio1 local

exit

port ethernet <slotnum/portnum>

no shutdown

bind interface <pdif_iface1> pdif

exit

# Bind the AAA logical interface to a physical port

port ethernet <slotnum/portnum>

no shutdown

bind interface <aaa-interface> pdif

exit

port ethernet <slotnum/portnum>

no shutdown

bind interface <ims-sh-1> pdif

end

configure

no autoconfirm

save configuration url <encrypted url> -redundant -noconfirm showsecrets
verbose
```



# Appendix B

## Engineering Rules

---

The following are known rules for the PDIF application. These rules apply to installations using mobile IP with simple IP fallback, and to installations using proxy mobile IP, unless where stated.

General and network-specific rules are located in Appendix A of the *System Administration Guide*.

The following rules are covered in this appendix:

- [IKEv2/IPSec Restrictions](#)
- [X.509 Certificate \(CERT\) Restrictions](#)
- [IPv6 Restrictions](#)
- [ICMPv6 Restrictions](#)
- [SCTP Restrictions](#)

## IKEv2/IPSec Restrictions

The following is a list of known restrictions for IKEv2 and IPSec:

- Each PDIF service must specify one crypto template.
- The PDIF supports traffic selectors with just IPv4 address values. IPv6 address values are not supported.
- The NAI must be unique per MS. If NAI is not unique, other attributes such as IMSI must be unique per MS and are used for session management.
- The PDIF supports IKEv2 only between the Mobile Station (MS) and the PDIF.
- IKEv2 does not support PFS (perfect forward secrecy) of individual CHILD SAs. While the PFS for MS-initiated IKE SA rekeying will be implemented, the rate for rekeying (with PFS enabled) shall not exceed the rate of the IKEv2 call setup rate. This is because PFS would require performing a new D-H exchange each time a rekey is negotiated, and a performance impact is expected. Also, note that the call setup rate and the rekeying rate are mutually exclusive.
- All IKEv2 packets are sent over IPv4.
- Per [RFC-4306] and [RFC-4718], the following known restrictions apply with respect to the payload and its order. Violations result in INVALID\_SYNTAX being returned which is being enabled or disabled through a configurable, except when the processing is noted as below.
- While [RFC-4306] Section 2.19 specifies “CP payload MUST be inserted before the SA payload,” the PDIF does not force strict ordering of this. The PDIF processes these payloads as long as the mobile sends a CP payload anywhere inside the encryption data.
- While [RFC-4306] Section 2.23 specifies “The location of the payloads (Notify payloads of type NAT\_DETECTION\_SOURCE\_IP and NAT\_DETECTION\_DESTINATION\_IP) in the IKE\_SA\_INIT packets are just after the Ni and Nr payloads (before the optional CERTREQ payload),” PDIF does not force strict ordering of this and still can process these NOTIFY payloads.
- The PDIF supports transform selector payloads with only one traffic selector. The number in the TS field must be set to “1”.
- Traffic selector payloads from the MS support only traffic selectors by IP address range. In other words, the IP protocol ID must be 0. The start port must be 0 and the end port must be 65535.
- The Configuration Payload (CP) is specified in [RFC-4306], Section 2.19 (Requesting an Internal Address on a Remote Network) for the situation where dynamic IP address assignment is required. Since the PDIF does not support INTERNAL\_IP6\_ADDRESS, the CP must include at least the attribute INTERNAL\_IP4\_ADDRESS.
- As described above, when the PDIF receives IKEv2 messages, the PDIF does not enforce the payloads to be in order. However, when the PDIF sends the response or generates any IKEv2 messages, the PDIF will ensure that payloads are ordered according to [RFC-4306].
- Only IKE and ESP protocol IDs are supported. AH is not supported since AH is deprecated in [RFC-4306].
- The IKE Protocol ID specification may not use the NONE algorithm for authentication or the ENCR\_NULL algorithm for encryption as specified in Section 5 (Security Considerations) of [RFC-4306].
- In ESP, ENCR\_NULL encryption and NONE authentication cannot be simultaneously used.

- Only one single proposal number can be used. Because [RFC-4306] states that the first proposal must be numbered 1, this implies that only proposals with the proposal number value of 1 are supported. The mobile device must send a list of transforms within this single proposal number.
- No more than 16 transform types may be present in a single IKE\_SA\_INIT or IKE\_AUTH Request message. If a deviation from this format is used in the proposal format, the PDIF returns an error of INVALID\_SYNTAX.

## X.509 Certificate (CERT) Restrictions

The following are known restrictions for the creation and use of X.509 CERT:

- The maximum size of CERT configuration is 1K bytes.
- The PDIF includes the CERT payload only in the first IKE\_AUTH Response for the first authentication.
- The CERT payload will be sent in the AUTH response, if configured, irrespective of receiving CERT-REQ payload in the first IKEv2 AUTH request.
- The PDIF will not process a CERT payload from the MS and will respond accordingly (with INVALID\_SYNTAX) if the CRITICAL bit is set in the payload.
- If the PDIF receives the CERT-REQ payload with the CRITICAL bit set in the IKE\_AUTH request, the PDIF will reject the exchange. If the CRITICAL bit is not set, then the PDIF ignores the payload and proceeds with the exchange.
- Only a single CERT payload is supported. While [RFC-4306] mandates the support of up to 4 certificates, the PDIF service will support only one X.509 certificate per context. This is due to the size of an X.509 certificate. Inclusion of multiple certificates in a single IKE\_AUTH may result in the IKE\_AUTH message not being properly transmitted.

# IPv6 Restrictions

The following is a list of known restrictions for the PDIF and IPv6:

- IPv6 ACLs are not supported.
- Path MTU discovery is not supported. The PDIF uses a fixed MTU size of 1500 for all IPv6 interfaces.
- IPv6 fragmentation is not supported. The PDIF does support reassembly of received IPv6 fragments that are addressed to an application (e.g., a Diameter application) within the PDIF.
- Routing protocols sent over IPv6 addresses are not supported.
- Routing protocols that manage IPv6 addresses are not supported.
- IP-in-IP 6to4 and 4to6 tunneling is not supported.
- Management services that use IPv6 addresses (e.g., SSH, SNMP, syslog, etc.) are not supported.
- MIPv6 and Proxy MIPv6 are not supported.
- IKEv2 IPv6 server addresses are not supported.
- Any service not explicitly listed in this document will not support IPv6 by default.
- The CLI commands that accept URLs, e.g., the “copy” command, do not support IPv6 URLs.
- IPv6 DNS is not supported.
- Jumbograms are not supported.
- An interface can be configured with a single IPv6 address, or some number of IPv4 addresses, but not both. Therefore if the same physical port is being used to access both IPv4 and IPv6 networks, multiple interfaces will need to be configured using separate VLANs.
- IPv6 addresses can be configured on Ethernet and loopback interfaces only.
- The PDIF does not send Router Solicitation messages.
- The PDIF permits at most one IPv6 address to be configured on an interface. Each interface that is configured with an IPv6 address will not support additional IPv6 addresses.
- The PDIF supports Neighbor Solicitation/Advertisement messages only.
- The PDIF does not support Redirect messages.
- The PDIF does not support Anycast Neighbor Advertisements.
- The PDIF does not support sending Router Advertisements.
- The PDIF does not support duplicate address detection.

# ICMPv6 Restrictions

- There are no CLI configuration commands.
- Only the types and codes listed in the Overview chapter are supported.
- Security Considerations (Section 5 of [RFC-4443]) are not supported.
- The PDIF routing protocols do not support IPv6 routes. There is no support for RIP-NG, OSPFv3, or IPv6 in BGP.



# SCTP Restrictions

None of the options defined in the SCTP RFCs will be provided for.