

Cisco Proxy Mobile IP Configuration Notes with Cisco Access Point

Last updated: October 2007

Introduction

This configuration note provides a Proxy Mobile IP (PMIP) configuration example on an AP1200, using a Cisco ACS to retrieve security associations (SA) for a mobile device. The document focuses on the SA retrieving aspect of PMIP configurations. It assumes that the user has already completed other parts of PMIP configuration tasks (ie: such as enabling proxy mobile IP and configuring Authoritative Access Point (AAP) information).

In order to enable an PMIP AP to use a Cisco ACS server to retrieve SAs from the mobile node, the user must complete three main configurations tasks:

- 1. Configure Cisco ACS information on an access point enabled with PMIP
- 2. Configure an AP enabled with a PMIP as an AAA Client on a ACS server
- 3. Configure mobile nodes' SA on a ACS server

Software Components

This configuration example is based on the following software components:

- Cisco Aironet Access Point 1200: Cisco IOS Software Release 12.0(2)T1
- Cisco ACS Server: version 3.1

Configure Authentication Server—Cisco ACS—Information on a PMIP Enabled Access Point

Step 1. Setup Screen, click on "Proxy Mobile IP"

AP5-2.4G Sec lisce 1200 Series Al Home Map Ner	tup 12.02T1 work Associa	tions Setup	Legs Help	CISCO SYSTEMS
		Express Se	aup	
		Associati	ons	
Display Defaults		Po	rt Assignments	Advanced
Address Filters	Protocol Fil	tere VL	AN	Service Sets
		Event L	og	
Display Defaults	1	Event Hara	fling	Notifications
		Service	s	August we second doc.
Console/Telnet	Boot Serve	r Ro	uting	Name Server
Tume Server	ETP	W	eb Server	SNMP
Cisco Services	Security	دة ا	recunting	Prony Mobile IP
		Network F	Ports	Diagnostics
Ethernet	Identification	Hardware	Editors	Advanced
AP Radio: Internal	Identification	Hardware	Filters	Advanced

AP5-2 Cisco 12	.4G Proxy N 100 Series AP 12.02T1	Mobile IP S	Setup	CISCO SYSTEMS
Home	Map Network	Associations	Setup Logs Help	Uptime: 21:31:40
General	1			
Authenti	ication Server			
Local S.	A Bindings			
Statistic	5			
View St	ubnet Map Table			Done

Step 2. Click on "Authentication Server"

Step 3. Configure the ACS server IP address, Server Type, Port, and Shared Secret Key. The ACS server IP address is the server IP address. The Server Type should be "RADIUS," and the Port can be either 1812 or 1645 if the ACS server version is v3.1. For an earlier version of ACS server, the ACS server may by default listen only port 1645. The Shared Secret must match the one configured on the ACS server (the ACS server configuration is in the section 3.0 below). Finally, remember to check on the "MIP Authentication" box and click "OK".



Note: Repeat Steps 1-3 for the other PMIP-enabled APs.

Configure a PMIP enabled AP as an AAA Client on a ACS server

Click on "Network Configuration" button and configure the "AAA Client IP Address", "Key", and the "Authenticate Using" fields. The "AAA Client IP Address" is the PMIP AP IP address, which is 10.20.1.112 in this example. The 'Key" is the shared secret key configured on the PMIP AP side as described in previous section. These two shared secret keys MUST match each other. The "Authenticate Using" should be "RADIUS (Cisco IOS/PIX)".

ISCO SYSTEMS	Network Configuration			
	Edit			
User Setup Setup Setup	AAA Client Setup For PMIP-AP2			
Network Configuration	AAA Chent IP 10.20.1.112			
System Configuration	Key sharekey			
Interface Configuration Administration Control Ecternal User Databases Reports and Activity	Authenticate Using PADIUS (Cisco IOS/PIX) Single Connect TACACS+ AAA Client (Record stop in accounting on failure). Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client			
Online Documentation	Submit Submit + Restart Delete			

Note: This part of configuration can be applied for a HA router that is also using an ACS server to retrieve mobile node's SA information.

Configure mobile nodes' SA on a ACS server

Step 1. Click on the "User Setup" button. Enter a mobile device's IP address, and click the "Add/Edit" button. The mobile device in this example is 10.10.1.201.

Cisco Systems	User Setup
-	Select
User Setup Setup Setup Setup Setup	User 10.10.1.201 Find Add/Edit
Network Coofiguration System Configuration Interface Configuration	List users beginning with letter/number. <u>A B C D E F G H I J K L M</u> <u>N O P Q R S T U V U X Y Z</u> <u>O 1 2 3 4 5 6 7 8 9</u>
Administration Control	List All Users
Content of the second s	Back to Help

Step 2. Configure the "User Setup" section. In this section, make sure the "Password Authentication:" is "CiscoSecure Database" and the "Password" section is configured with "cisco".

Note: This password must be "cisco". Cisco Access Points use this default password when communicating with the Radius server.

User	User: 10.10.1.201
Lig Setup	
Group Setup	Account Disabled
Shared Profile Components	Supplementary User Info 🤶
Configuration	Real Name PMIP Users
System Configuration	Description 10.10.1.0 on AP1
Configuration	
Administration Control	User Setup
Administration Control	User Setup ? Password Authentication:
Administration Control External User Databases	User Setup ? Password Authentication:
Administration Control External User Databases Reports and Activity	User Setup ? Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS-
Administration Control External User Databases Reports and Activity	User Setup ? Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)
Administration Control External User Databases Reports and Activity Online Documentation	User Setup Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password
Administration Control	User Setup ? Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm
Administration Control External User Databases Reports and Activity Online Documentation	User Setup ? Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password

Step 3. Configure the "Cisco IOS/PIX Radius Attributes" section. This section is in the bottom of the User Setup Page.

	Cisco IOS/PIX RADIUS Attributes	?
600] 되	\001] cisco-av-pair	
	mobileip:spi#0=spi 100 key hex 123456781234567812345678123456 78	

In this section, check the "cisco-av-pair" box and configure the av-pair with the following format:

mobileip:spi#0=spi <num> key hex <key>

The spi number should equal or exceed 100, and the key must be 32 hex digits. These values (SPI and Key) must match the one configured on the HA.

Note: If the HA is also using a ACS to retrieve the mobile device's SA, make sure this key is matched to the one configured on that ACS. If the HA is using the same ACS as this PMIP AP to retrieve the mobile device's SA, the match will be guaranteed).

Repeat Steps 1-3 for each mobile node.

Note: The "Cisco IOS/PIX Radius Attributes" section above may not appear as an option in a "User Setup" configuration. If this option is not visible, go to the "Interface Configuration" and check on the User and Group "cisco-av-pair" boxes as highlighted below.

Cisco Systems	Interface Configuration			
dilline ad the .	Edit			
User Setup				
Setup				RADIUS (Cisco IOS/PIX)
Shared Profile Components				
Network Configuration		User	Gr	buû.
System	<	ų	9	[026/009/001] cisco-av-pair
I come a far a come a			5	[026/009/101] cisco-h323-credit-amount
Configuration			5	[026/009/102] cisco-h323-credit-time
Administration			$\overline{\mathbf{v}}$	[026/009/103] cisco-h323-return-code
Centrol			4	[026/009/104] cisco-h323-prompt-id
Databases			$\overline{\mathbf{v}}$	[026/009/105] cisco-h323-day-and-time
Reports and			5	[026/009/106] cisco-h323-redirect-number
Activity			5	[026/009/107] cisco-h323-preferred-lang
0 Online Documentation			9	[026/009/108] cisco-h323-redirect-ip-addr
Cont. Sectors and interesting			₽	[026/009/109] cisco-h323-billing-model
			5	[026/009/110] cisco-h323-currency

Enabling the Cisco IOS/PIX Radius Attributes Field

Reference

[1] Configuring Proxy Mobile IP

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/bkscgch6.h tm

Appendix

HA Configuration for Retrieving SA information from An ACS Server

The configuration below enables aHA router retrieving mobile nodes' SA information from a Radius server with IP address 172.19.192.137. The mobile nodes are in the range of 10.99.2.1 to 10.99.2.100. Note only relevant configurations are shown below.

version 12.2 service password-encryption

hostname 72R1-hal

Enable AAA Authorization

aaa new-model

Enable AAA Authorization for Mobile IP

aaa authorization ipmobile default group radius

aaa session-id common

router mobile

ip mobile home-agent address 200.1.1.1

Retrieve SAs for MNs with IP address between 10.99.2.1 to 10.99.2.100 and cache the SA on the HA once loaded

ip mobile host 10.99.2.1 10.99.2.100 interface fa0/0 aaa load-sa

This command tells the HA to use the IP address assigned to Loopback1 as the source IP address in the packets sent to Radius Server.

This IP address of the loopback1 should match the one configured on the Radius Client list

ip radius source-interface Loopback1

Define IP address of the Radius server 172.19.192.137 and the ports it is listening to

radius-server host 172.19.192.137 auth-port 1645 acct-port 1646 radius-server retransmit 3

Define the radius server and shared secret.

radius-server key 7 094F471A1A0A



Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax. 408 527-0883 Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. 168 Robinson Road #28-01 Capital Tower Singapore 068912 www.cisco.com Tel: +65 6317 7777 Fax: +65 6317 7799 Europe Headquarters Cisco Systems International BV Haarlerbergpark Haarlerbergweg 13-19 1101 CH Amsterdam The Netherlands www-europe.cisco.com Tel: +31 0 800 020 0791 Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.: Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.: and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherSatt, EtherSatt, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0710R)

Printed in USA

10/07