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

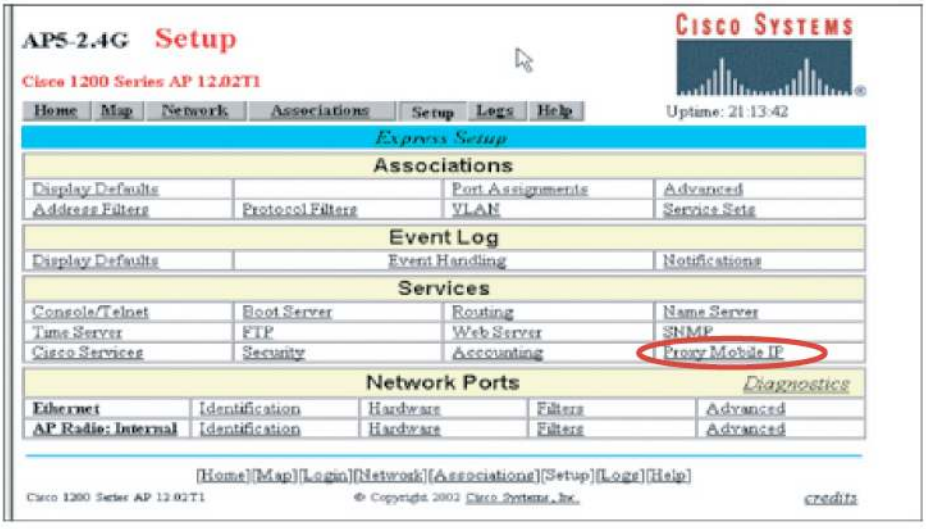
Software Components

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

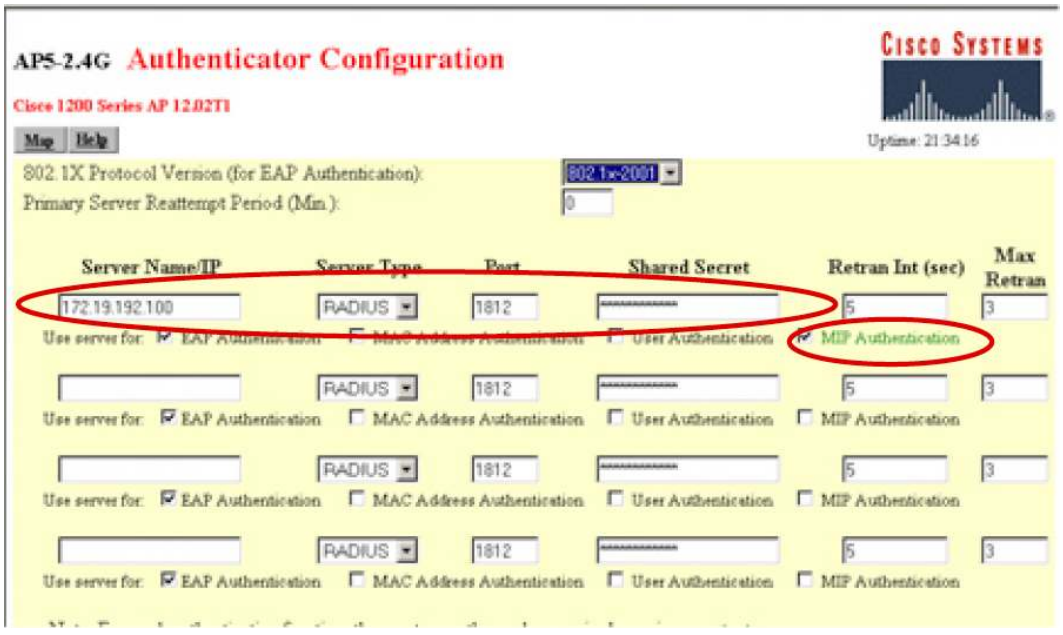
Configure Authentication Server—Cisco ACS—Information on a PMIP Enabled Access Point

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



Step 2. Click on “Authentication Server”

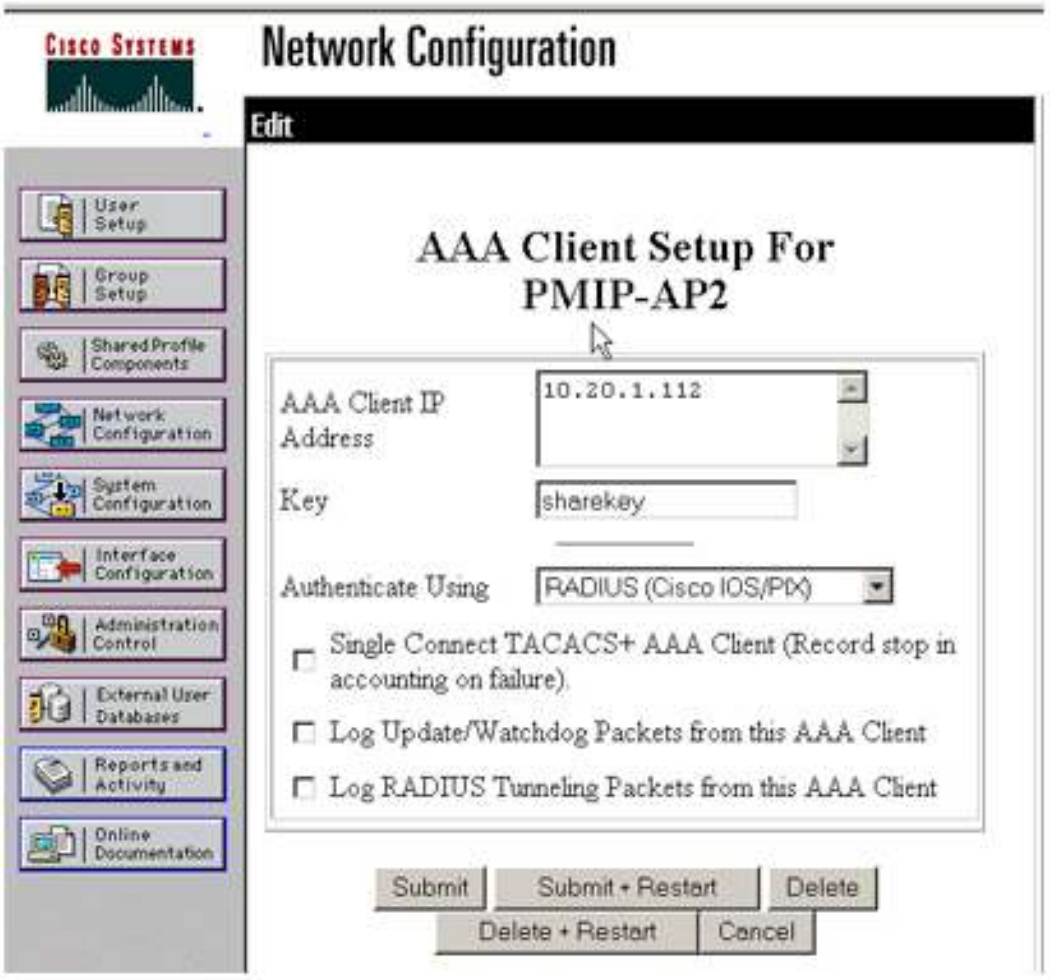
Step 3. Configure the ACS server IP address, Server Type, Port, and Shared Secret Key. The ACS server IP address is the server IP address. The Server Type should be “RADIUS,” and the Port can be either 1812 or 1645 if the ACS server version is v3.1. For an earlier version of ACS server, the ACS server 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

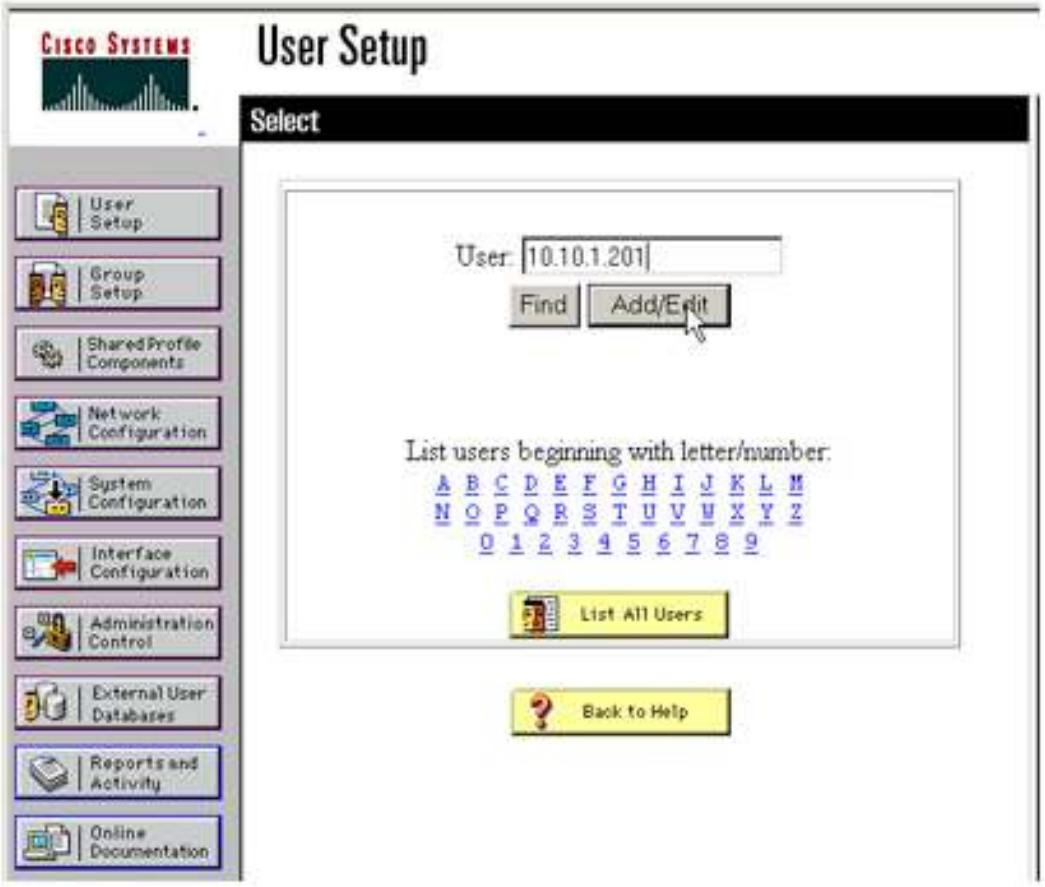
Click on “Network Configuration” button and configure the “AAA Client IP Address”, “Key”, and the “Authenticate Using” fields. The “AAA Client IP Address” is the PMIP AP IP address, which is 10.20.1.112 in this example. The ‘Key” is the shared secret key configured on the PMIP AP side as described in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



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.

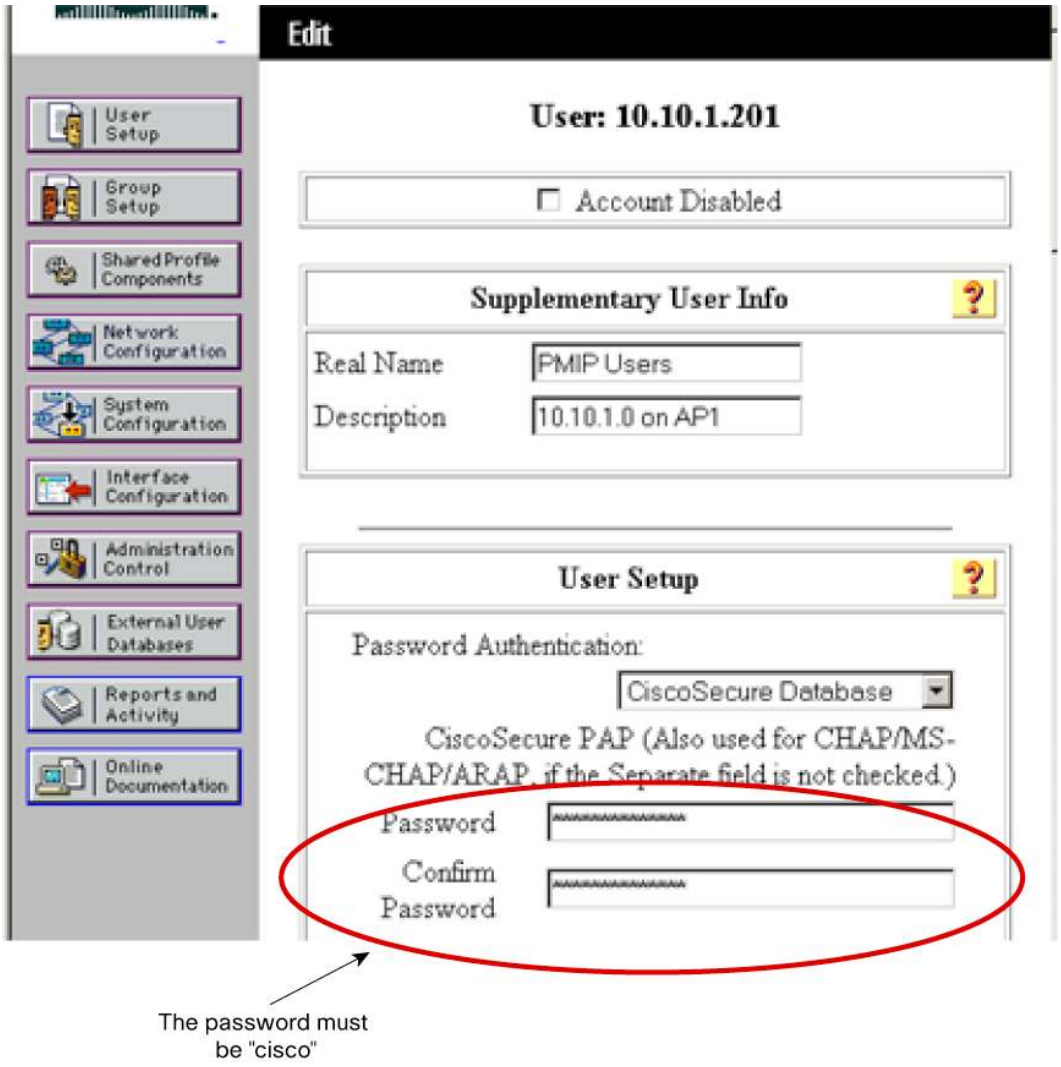
Configure mobile nodes' SA on a ACS server

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.

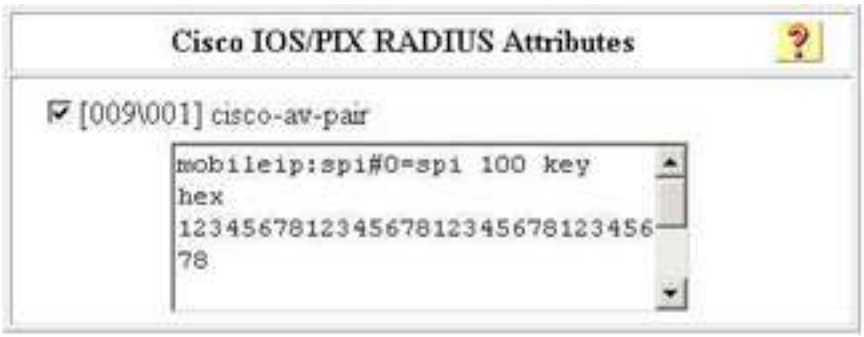


Step 2. Configure the “User Setup” section. In this section, make sure the “Password Authentication:” is “CiscoSecure Database” and the “Password” section is configured with “cisco”.

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



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



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>
```

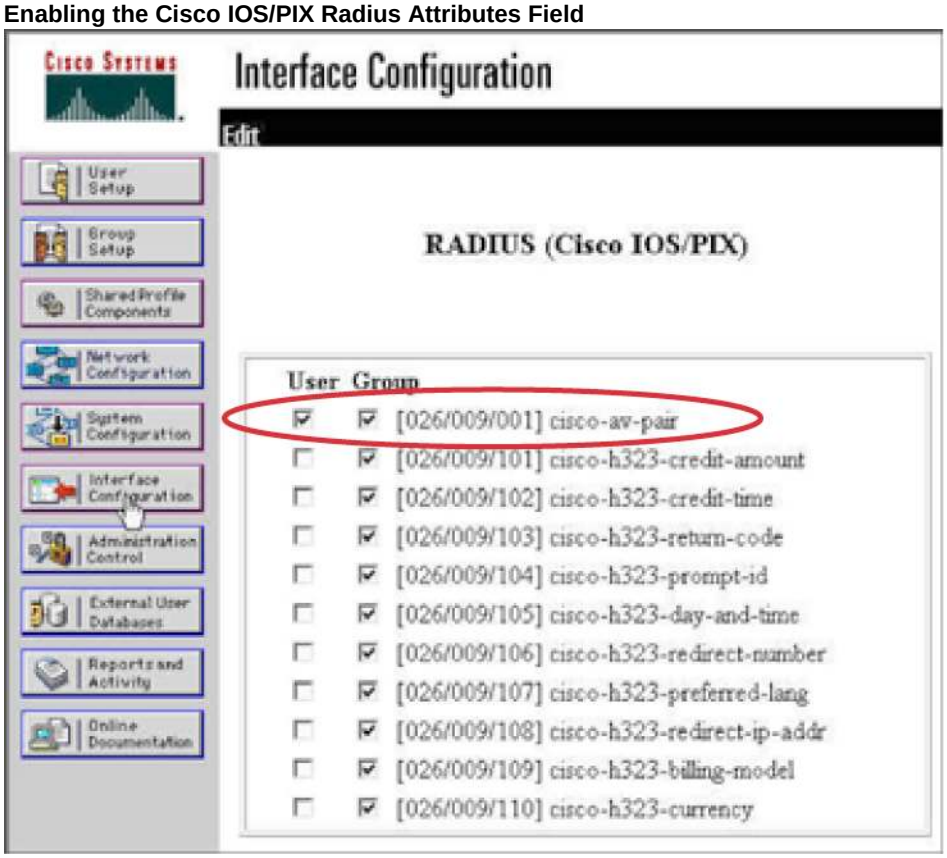
The spi number should equal or exceed 100, and the key must be 32 hex digits. These values (SPI and Key) must match the one configured on the HA.

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.

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.htm

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-ha1
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.

Printed in USA 10/07

