



## CHAPTER 4

# User Authentication and Authorization

---

This chapter discusses User Authentication and Authorization, and how to configure this feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

- [User Authentication and Authorization, page 4-1](#)
- [Skip HA-CHAP with MN-FA Challenge Extension \(MFCE\), page 4-2](#)
- [Configuration Examples, page 4-3](#)
- [Authentication and Authorization RADIUS Attributes, page 4-3](#)

## User Authentication and Authorization

You can configure the Home Agent to authenticate a user with either Password Authentication Protocol (PAP), or Challenge Handshake Authentication Protocol (CHAP). The Foreign Agent Challenge procedures are supported (RFC 3012) and include the following extensions:

- Mobile IP Agent Advertisement Challenge Extension
- MN-FA Challenge Extension
- MN-AAA Authentication Extension



### Note

---

PAP is used if no MN-AAA extension is present, and CHAP is always used if MN-AAA is present. The password for PAP users can be set using the **ip mobile home-agent aaa user-password** command.

---

If the Home Agent receives the MN-AAA Authentication Extension in the Registration Request (when configured to authenticate the user with the Home AAA-server), the contents are used. If the extension is absent, a default configurable password is used. This default password is a locally defined string such as “vendor”.

The HA accepts and maintains the MN-FA challenge extension and MN-AAA authentication extension (if present) from the original registration for use in later registration updates.

If the Home Agent does not receive a response from the AAA server within a configurable timeout, the message can be retransmitted a configurable number of times. You can configure the Home Agent to communicate with a group of AAA servers; the server is chosen in round-robin fashion from the available configured servers.

Step 1	Command	Purpose
	<pre>Router(config)# <i>{lower [upper]   nai string</i> {static-address {addr1 [addr2] [addr3] [addr4] [addr5]   local-pool name}   address {addr   pool {local name   dhcp-proxy-client [<b>dhcp-server</b> <i>addr</i> <b>interface</b> <i>name</i>   <b>virtual-network</b> <i>network_address mask</i> <b>skip-chap</b>   <b>aaa</b> <b>load-sa</b> <b>care-of-access</b> <i>acl</i> seconds</pre>	

The HA supports 3GPP2 and Cisco proprietary security extension attributes in RADIUS access accept packet. Sending 3GPP2 MN-HA SPI in Access Request to RADIUS server and processing the MN-HA Secure Key Received from RADIUS server is configurable on HA.

Cisco IOS provides a mechanism to authorize subscribers based on their realm. This can be done using a feature called “Subscriber Authorization”, the details of which can be found here: [http://www.cisco.com/en/US/partner/products/ps6350/products\\_configuration\\_guide\\_chapter09186a0080455cf0.html#wp1056463](http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463).



The Home Agent will accept user profiles, it will not authorize a mobile subscriber based on information returned in a group profile.

## Skip HA-CHAP with MN-FA Challenge Extension (MFCE)

# Configuration Examples

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network          aaa load-sa
```

```
                nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

## Authentication and Authorization RADIUS Attributes

**Table 4-1** Authentication and Authorization AVPs Supported by Cisco IOS

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In	
						Access Request	Access Accept
			>=18 && <=130	string	Password for authentication when using PAP. Password configured using CLI at Home Agent.	Yes	No
CHAP-Password	3	NA	19	string	CHAP password	Yes	No
NAS-IP-Address	4	NA	4	IP address	IP address of the HA interface used for communicating with RADIUS server.	Yes	No
Service Type	6	NA	4	integer	Type of service the user receives. Supported values: Outbound sent for PAP Framed sent for CHAP Framed received in both cases	Yes	Yes
Framed-Protocol	7	NA	4	integer	Framing protocol user is using. Sent for CHAP, received for PAP and CHAP. Supported values: PPP	Yes	Yes

**Authentication and Authorization AVPs Supported by Cisco IOS (continued)**

Framed Compression	13	NA	4	integer	Compression method Supported values: 0 - None	No	Yes
Framed-Routing	10	NA	4	integer	Routing method Supported values: 0 - None	No	Yes
Vendor Specific	26	NA			Vendor specific attributes	Yes	Yes
CHAP-Challenge (optional)	60	NA	>=7	string	CHAP Challenge	Yes	No
NAS-Port-Type	61	NA	4	integer	Port Type Supported: 0 - Async	Yes	No
spi#	26/1	Cisco	>=3	string	is a numeric identifier beginning with <b>0</b> that allows multiple SAs per user.  Provides the Security Parameter Index (SPI), for authenticating a mobile user during MIP registration.  The information is in the same syntax as the <b>ip mobile secure host</b> configuration command. Essentially, it contains the rest of the configuration command that follows that string, verbatim.	No	Yes
static-ip-addresses	26/1	Cisco	>=3	string	IP address list for static addresses for same NAI but multiple flows.	No	Yes
static-ip-pool	26/1	Cisco	>=3	string	IP address pool name for static address for same NAI with multiple flows.	No	Yes
ip-addresses	26/1	Cisco	>=3	string	IP address list used for dynamic address assignment.	No	Yes
ip-pool	26/1	Cisco	>=3	string	IP address pool name used for dynamic address assignment.	No	Yes
dhcp-server	26/1	Cisco	>=3	string	Get an address from the specified DHCP server.	No	Yes
MN-HA SPI Key	26/57	3GPP2	6	integer	SPI for MN HA Shared Key.	Yes	No
MN-HA Shared Key	26/58	3GPP2	20	string	Secure Key to authenticate MHAE.	No	Yes