CHAPTER 5

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

The Home Agent can be configured to authenticate a user using either PAP or CHAP. The Foreign Agent Challenge procedures are supported (RFC 3012) and includes 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.

When configured to authenticate the user with the Home AAA-server, if the Home Agent receives the MN-AAA Authentication Extension in the Registration Request, 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.

To configure authorization and authentication on the HA, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile host {lower [upper] | nai string {static-address {addr1 [addr2] [addr3] [addr4] [addr5] | local-pool name} | address {addr | pool {local name | dhcp-proxy-client [dhcp-server addr]} {interface name | virtual-network network_address mask} [skip-chap | aaa [load-sa [permanent]] [authorized-pool pool name] [skip-aaa-reauthentication] [care-of-access acl] [lifetime seconds]`	Configures the mobile host or mobile node group on the HA. If the **aaa load-sa** option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration. If **aaa load-sa skip-aaa-reauthentication** is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration. The **aaa load-sa permanent** option is not supported on the Mobile Wireless Home Agent, and should not be configured.

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.

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

Authentication Configuration Extension

The Home Agent allow you to configure when external authentication with AAA occurs for specific mobile IP events. Handoffs across foreign agents is treated as a registration and a de-registration event, and there is no specific configuration for handoff.

In the event that a re-registration request is received with a different SPI than used for a previous registration or re-registration for that session, the configuration options **enable | disable** for authentication on re-registration are ignored for this user.

Applying or modifying any configuration occurs at the next event for a given binding.

The following configuration is for the re-registration and de-registration events that may be on a per-realm (VRF) basis.

ip mobile host nai *string* aaa **load-sa skip-aaa-reauth** [*reregistration* | *deregistration*]

The default configuration is that authentication occurs for all three events (**ip mobile host nai** *string* **aaa load-sa**).

Here are some examples that assume the default configuration is in place:

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** results in AAA authentication occurring for registration only.

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *deregistration* results in AAA authentication occurring for registration and reregistration.

ip mobile host nai *string* **aaa skip-chap** results in no authentication occurring for initial registration, reregistration, and deregistration events.

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *reregistration* results in AAA authentication occurring for registration and deregistration only.

The **load-sa** keyword causes the HA to download and locally store the security attributes for mobile-home authentication during the entire session. Without this parameter the HA does not locally store the security attributes for mobile-home authentication, and must retrieve them from AAA for subsequent re-registration or de-registration.

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

This feature allows the HA to download a Security Association (SA) and cache it locally on the disk, rather than performing a HA-CHAP procedure with Home AAA server to download the SA for the user for each registration request. When a user first registers with the HA, the HA does HA-CHAP (MN-AAA authentication), downloads the SA, and caches it locally. On subsequent re-registration requests, the HA uses the locally cached SA to authenticate the user. The SA cache entry is removed when the binding for the user is deleted.

You can configure this feature on the HA using the **ip mobile host** command, noted above.

Configuration Examples

The following example configures a mobile node group to reside on virtual network 10.99.1.0 and retrieve and cache mobile node security associations from a AAA server. The cached security association is then used for subsequent registrations.

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached permanently until cleared manually.

```
ip mobile host 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

The Home Agent, and the RADIUS server support RADIUS attributes listed in Table 1 for authentication and authorization services.

Table 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	Allowed In Access Accept
User-Name	1	NA	64	string	User name for authentication and authorization.	Yes	No
User-Password	2	NA	>=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 is getting. 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
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

Table 1 Authentication and Authorization AVPs Supported by Cisco IOS (continued)

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In Access Request	Allowed In Access Accept
spi#*n*	26/1	Cisco	>=3	string	*n* is a numeric identifier beginning with **0** which 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 **ip mobile secure host** *addr* 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