



CHAPTER 14

Other Configuration Tasks

Other Configuration Tasks

This chapter discusses important concepts and provides configuration details for the following features in the Cisco IOS Mobile Wireless Home Agent software:

- [Support for ACLs on Tunnel Interface, page 14-1](#)
- [Configuring Mobile IP Tunnel Template Feature, page 14-2](#)
- [Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY, page 14-3](#)
- [User Profiles, page 14-3](#)
- [Mobility Binding Association, page 14-4](#)
- [HA Binding Update, page 14-4](#)
- [Selective Mobile Blocking, page 14-5](#)
- [Mobile Equipment Identifier \(MEID\) Support, page 14-5](#)

Support for ACLs on Tunnel Interface

The Cisco Tunnel Templates feature allows the configuration of ACLs on statically created tunnels to be applied to dynamic tunnels brought up on the Home Agent. A tunnel template is defined and applied to the tunnels between the Home Agent and PDSN/Foreign Agent.

Configuring Mobile IP Tunnel Template Feature

To enable the Mobile IP Tunnel Template feature, perform these tasks:

	Command	Purpose
Step 1	Router(config)# interface tunnel 10 ip access-group 150	Configures an interface type and enters interface configuration mode. tunnel interface; a virtual interface. The number is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
Step 1	Router(config)# access-list 150 deny any 10.10.0.0 0.255.255.255 access-list permit any any	Configures the access list mechanism for filtering frames by protocol type or vendor code
Step 1	Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1	Configures the template tunnel and the template tunnel address.

Here is a sample configuration used to block certain traffic using template tunnel feature:

1. Configure a tunnel template

```
interface tunnel 10
 ip access-group 150 in -----> apply access-list 150
```

2. Configure the ACL

```
access-list 150 deny any 10.10.0.0 0.255.255.255
access-list permit any any
-----> permit all but traffic to 10.10.0.0 network
```

3. Configure the Home Agent to use the template tunnel.

```
ip mobile home-agent template tunnel 10 address 10.0.0.1
```



Note

If you enable the Mobile IP Tunnel Template feature and remove the tunnel interface from the configuration, you should also manually remove the corresponding **mobileip tunnel template** command. If necessary, you can reconfigure the **mobileip tunnel template** command after you configure a new tunnel interface.

Limitations

When you use PMIP with session redundancy and you choose the “msec” option for the timestamp (**ip mobile foreign-service revocation timeout 5 retransmit 4 timestamp msec**), and open a PMIP flow with PDSN SR setup, the **cdma redundancy debug** output shows that the “revocation timestamp” value on the active and standby PDSNs are the same.

If you perform a switchover, the standby PDSN takes over as active. If you try to close the PMIP flow, the revocation message sent from the PDSN to the HA is ignored on HA because the timestamp is mismatched. Thus, after several re-tries, the PDSN deletes the revocation entry pending for Ack, and the binding on the HA is not deleted.

This limitation is not related to synching the attribute, but to the uptime of the router, because the **msec** option puts the uptime in the timestamp field and the uptime of the standby router is expected to be lower. If you utilize the default **seconds** based option (which puts a timestamp in UTC), this may not be an issue. Additionally, **msec** has another issue of wrap-around in 49+ days, so it cannot be used in an always-on setup.

Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY

The Cisco Home Agent supports the following 3GPP2 standard attributes:

MN-HA-SPI (26/57)

MN-HA-SHARED-KEY (26/58)

The following procedure illustrates this support:

-
- | | |
|---------------|---|
| Step 1 | The HA receives a RRQ from the PDSN/FA |
| Step 2 | The HA sends an Access Request to AAA. The HA adds the MHAЕ SPI of the RRQ to the Access Request as MN-HA-SPI(26/57) attribute. |
| Step 3 | The AAA server matches the MN-HA-SPI (26/57) against the corresponding MN-HA-SHARED-KEY (26/58). |
| Step 4 | The AAA server includes that MN-HA-SHARED-KEY (26/58) in the access reply. |
| Step 5 | The HA authenticates the MHAЕ of RRQ using the downloaded shared key MN-HA-SHARED-KEY (26/58). |
-

User Profiles

The Home Agent maintains a per NAI profile that contains the following parameters:

- User Identification - NAI
- User Identification - IP Address
- Security Associations
- Reverse Tunnel indication - the parameter specifies the style of reverse tunneling that is required for the user data transfer with Mobile IP services.
- Timestamp window for replay protection
- State information is maintained for all Registration Request flags requested, and then granted (for example, SIBIDIMIGIV flags).

The profile, identified by the NAI, can be configured locally or retrieved from a AAA server.

Additionally, the Home Agent supports an intelligent security association caching mechanism that optimizes the session establishment rate and minimizes the time for session establishment.

The Home Agent supports the local configuration of a maximum of 200000 user profiles; on the MWAM, the HA supports 5 x 200000 user profiles. The User profile, identified by the NAI, can be configured locally, or retrieved from a AAA server.

Mobility Binding Association

The mobility binding is identified in the Home Agent in the following ways:

- For static IP address assignment, NAI+IP
- For dynamic IP address assignment, NAI
- The **show ip mobile binding** command will show mobility binding information for each user.

The binding association contains the following information:

- Care-of-Address
- Home address
- Lifetime of the association
- Signalling identification field

HA Binding Update

When a mobile first registers for packet data services, a PPP session and associated Mobile IP flow(s) are established at the PDSN. In the event of an inter-PDSN handoff, another PPP session is established at the target PDSN, and the mobile registers with the Home Agent using the new PDSN/FA. If PPP idle-timeout is configured on the PDSN virtual-template, the maximum mobile IP lifetime advertised to the mobile will be 1 second less than the idle-timeout.

Idle, or unused PPP sessions at a PDSN/Foreign Agent consume valuable resources. The Cisco PDSN/Foreign Agent and Home Agent support Binding Update and Binding Acknowledge messages to release such idle PPP sessions as soon as possible. In the event of an inter-PDSN handoff and Mobile IP registration, the Home Agent updates mobility binding information for the mobile with the Care-of-Address (CoA) of the new PDSN/FA.

If simultaneous bindings are not enabled, the Home Agent sends a notification in the form of a Binding Update message to the previous PDSN/FA. The previous PDSN/FA acknowledges with a Binding Acknowledge, if required, and deletes the visitor list entry for the Mobile IP session. The previous PDSN/FA initiates the release of the PPP session when there are no active flows for that mobile station.

**Note**

You can configure the Home Agent to send the binding update message on a global basis.

**Note**

This feature works with a Cisco FA that has bind update enabled on the box. Security association between the FA and HA has to be configured on both the boxes for this feature to be enabled.

Selective Mobile Blocking

You might want to block access to a specific mobile for reasons such as prepaid quota is over, service is disabled due to non-payment of bills, or other reasons. You can accomplish this by adding the “mobileip:prohibited” cisco-avpair attribute to the user profile on AAA server. When the “mobileip:prohibited” attribute is returned to Home Agent in access accept, the behavior is as follows:

- If the AAA server returns “mobileip:prohibited=1” in an access accept, and if the MN-HA Security Association for the mobile is configured on the AAA server and also returned to Home Agent in an access accept, the Home Agent sends a registration request (failure) with error code 129 (Administratively Prohibited) to the MN.
- If the AAA server returns “mobileip:prohibited=0” in an access accept, or if the attribute is not returned to the HA in an access accept, the HA performs normal processing of the registration request.

**Note**

The “mobileip:prohibited” attribute should not be set to any value other than 0 and 1.

Mobile Equipment Identifier (MEID) Support

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. It is a globally unique 56-bit identification number for a physical piece of mobile station equipment. In the interim period though, both the attributes need to be supported on the Home Agent.

The MEID NVSE will be appended by the PDSN node to the Mobile IP RRQ. When the MEID NVSE is received on the HA, and the **ip mobile cdma ha-chap send attribute A3** command is configured, the MEID value is included in the HA-CHAP access request.

