



# IP Mobility Commands

---

# aaa authorization ipmobile

To authorize Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS, use the **aaa authorization ipmobile** command in global configuration mode. To remove authorization, use the **no** form of this command.

```
aaa authorization ipmobile {[radius | tacacs+] | default} [group server-group-name]
```

```
no aaa authorization ipmobile {[radius | tacacs+] | default} [group server-group-name]
```

## Syntax Description

<b>radius</b>	Authorization list named radius.
<b>tacacs+</b>	Authorization list named tacacs+.
<b>default</b>	Default authorization list.
<b>group</b> <i>server-group-name</i>	(Optional) Name of the server group to use.

## Defaults

AAA is not used to retrieve security associations for authentication.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(1)T	This command was introduced.

## Usage Guidelines

Mobile IP requires security associations for registration authentication. The security associations are configured on the router or on a AAA server. This command is not needed for the former; but in the latter case, this command authorizes Mobile IP to retrieve the security associations from the AAA server.

Once the authorization list is named, it can be used in other areas such as login. You can only use one named authorization list; multiple named authorization lists are not supported.

The **aaa authorization ipmobile default group** *server-group-name* command is the most commonly used method to retrieve security associations from the AAA server.



### Note

The AAA server does not authenticate the user. It stores the security association that is retrieved by the router to authenticate registration.

## Examples

The following example uses TACACS+ to retrieve security associations from the AAA server:

```
aaa new-model
aaa authorization ipmobile tacacs+
tacacs-server host 1.2.3.4
tacacs-server key mykey
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

The following example uses RADIUS as the default group to retrieve security associations from the AAA server:

```
aaa new-model
aaa authentication login default enable
aaa authorization ipmobile default group radius
aaa session-id common
radius-server host 128.107.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

#### Related Commands

Command	Description
<b>aaa new-model</b>	Enables the AAA access control model.
<b>ip mobile host</b>	Configures the mobile host or mobile node group.
<b>radius-server host</b>	Specifies a RADIUS server host.
<b>radius-server key</b>	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
<b>show ip mobile host</b>	Displays mobile node information.
<b>tacacs-server host</b>	Specifies a TACACS host.
<b>tacacs-server key</b>	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

# address (mobile router)

To set the home IP address of the mobile router, use the **address** command in mobile router configuration mode. To remove the address, use the **no** form of this command.

**address** *address mask*

**no address** *address mask*

Syntax Description		
	<i>address</i>	Home IP address.
	<i>mask</i>	Mask for the associated subnet.

**Defaults** No default behavior or values.

**Command Modes** Mobile router configuration

Command History	Release	Modification
	12.2(4)T	This command was introduced.

**Usage Guidelines** The **address** command configures the home IP address and subnet mask of the mobile router. The address and subnet mask identify the home network of the mobile router and are used to discover when the mobile router is at home.

**Examples** The following example sets the home IP address and subnet mask of the mobile router:

```
ip mobile router
address 10.1.0.1 255.255.0.0
```

Related Commands	Command	Description
	<b>show ip mobile router</b>	Displays configuration information and monitoring information about the mobile router.

## address (Proxy Mobile IPv6)

To configure the IPv4 or the IPv6 address for the Mobile Access Gateway (MAG), use the **address** command in MAG configuration mode. To remove the IP address, use the **no** form of this command.

```
address {ipv4 ipv4-address | ipv6 ipv6-address}
```

```
no address {ipv4 ipv4-address | ipv6 ipv6-address}
```

### Syntax Description

<b>ipv4</b> <i>ipv4-address</i>	Specifies the IPv4 address for the MAG.
<b>ipv6</b> <i>ipv6-address</i>	Specifies the IPv6 address for the MAG.

### Command Default

No IPv4 address or IPv6 address is configured for the MAG.

### Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

### Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

### Usage Guidelines

The MAG can have only one IPv4 address and one IPv6 address.

### Examples

The following example shows how to configure an IPv6 address for the MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# address ipv6 2001:0DB8:2:5::1
```

### Related Commands

Command	Description
<b>ipv6 mobile pmipv6-domain</b>	Configures a PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

## apn\_(Proxy Mobile IPv6)

To specify an access point name (APN) to the subscriber of the mobile node (MN) or for the Mobile Access Gateway (MAG) within the Proxy Mobile IPv6 (PMIP) domain, use the **apn** command in mobile node or MAG configuration mode. To remove the APN specification, use the **no** form of this command.

**apn** *apn-name*

**no apn**

### Syntax Description

<i>apn-name</i>	APN identifier.
-----------------	-----------------

### Command Default

No APN is specified.

### Command Modes

MAG configuration (config-ipv6-pmipv6-mag)  
Mobile node configuration (config-ipv6-pmipv6-domain-mn)

### Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

### Usage Guidelines

To specify the APN identifier for the MN, use the **apn** command in mobile node configuration mode.  
To specify the APN identifier for the MAG, use the **apn** command in MAG configuration mode.

### Examples

The following example shows how to specify the APN for the MN within the PMIP domain:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# nai example@abc.com
Router(config-ipv6-pmipv6-domain-mn)# apn apn1
```

The following example shows how to specify the APN for the MAG within the PMIP domain:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# apn apn1
```

### Related Commands

Command	Description
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.
<b>nai</b>	Configures the Network Access Identifier for the MN within the PMIP domain.

# auth-option

To configure the authentication for the Proxy Mobile IPv6 (PMIP) domain or the Local Mobility Anchor (LMA) within the Mobile Access Gateway (MAG), use the **auth-option** command in PMIP domain or MAG-LMA configuration mode. To disable the authentication, use the **no** form of this command.

**auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** | **hex**} *string*

**no auth-option**

## Syntax Description

<b>spi</b> <i>spi-hex-value</i>	Specifies the Security Parameter Index (SPI) in hexadecimal format. The range is from 64 to FFFFFFFF.
<b>decimal</b> <i>spi-decimal-value</i>	Specifies the SPI value in decimal format. The range is from 256 to 12345678.
<b>key</b>	Specifies the security key.
<b>ascii</b>	Specifies the security key in ASCII format.
<b>hex</b>	Specifies the security key in hexadecimal format.
<i>string</i>	Key entered as a string.

## Command Default

No authentication is set.

## Command Modes

MAG-LMA configuration (config-ipv6-pmipv6mag-lma)  
PMIP domain configuration (config-ipv6-pmipv6-domain)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Usage Guidelines

Use the **auth-option** command in PMIP configuration mode to configure the SPI and the key value for the PMIP domain. The LMAs and the MAGs within the PMIP domain use this configuration as the default.

Use the **auth-option** command in MAG-LMA configuration mode to configure the authentication for the LMA within the MAG.

## Examples

The following example shows how to configure the authentication in PMIP configuration mode, with the SPI in hexadecimal format and an ASCII string key value:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# auth-option spi 67 key ascii key1
```

The following example shows how to configure the authentication in MAG-LMA configuration mode, with the SPI in decimal format and a string key value:

```
Router(config)# ipv6 mobile pmipv6-domain dn1  
Router(config-ipv6-pmipv6-domain)# exit  
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1  
Router(config-ipv6-pmipv6-mag)# lma lma1 dn1  
Router(config-ipv6-pmipv6mag-lma)# auth-option spi decimal 258 key hex BDF
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.
<b>lma</b>	Configures the LMA for the PMIP domain.

## binding (proxy mobile IPv6)

To configure the binding update parameters for the Mobile Access Gateway (MAG), use the **binding** command in MAG configuration mode. To remove the binding updates configuration, use the **no** form of this command.

```
binding { { init-retx-time | max-retx-time } milliseconds | { lifetime | refresh-time } seconds |
maximum number }
```

```
no binding { init-retx-time | max-retx-time | lifetime | refresh-time | maximum }
```

Syntax Description		
<b>init-retx-time</b> <i>milliseconds</i>		Specifies the initial timeout, in milliseconds (ms), between the Proxy Binding Updates (PBUs) and the Proxy Binding Acknowledgment (PBA), until the PBA is received. The range is from 100 to 65535.
<b>lifetime</b> <i>seconds</i>		Specifies the maximum lifetime, in seconds, permitted for the binding update entry. The range is from 10 to 65535.
<b>max-retx-time</b> <i>milliseconds</i>		Specifies the maximum timeout in ms, between the PBUs and the PBAs, until the PBA is received. The range is from 100 to 65535.
<b>maximum</b> <i>number</i>		Specifies the maximum number of binding update entries allowed. The range is from 1 to 40000.
<b>refresh-time</b> <i>seconds</i>		Specifies the binding update entry refresh time in seconds. The range is from 4 to 65535, and in multiples of 4. If the value entered is not a multiple of 4, the value configured may be rounded to the nearest lowest multiple of 4.

### Command Default

The default value for the keywords are as follows:

- **init-retx-time**: 1 second
- **lifetime**: 65535 seconds
- **max-retx-time**: 32 seconds
- **refresh-time**: 300 seconds

### Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

### Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

### Usage Guidelines

The value for the **init-retx-time** keyword should be less than that for the **max-retx-time** keyword.

The **no binding max-retx-time** command configures the **init-retx-time** and **max-retx-time** values to the default values.

**Examples**

The following example shows how to configure binding update parameters for the MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# binding init-retx-time 110
Router(config-ipv6-pmipv6-mag)# binding max-retx-time 4000
Router(config-ipv6-pmipv6-mag)# binding lifetime 5000
Router(config-ipv6-pmipv6-mag)# binding maximum 200
Router(config-ipv6-pmipv6-mag)# binding refresh-time 2000
```

**Related Commands**

Command	Description
<b>ipv6 mobile pmipv6-domain</b>	Configures a PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# bri

To configure Binding Revocation Indication (BRI) message parameters, use the **bri** command in MAG configuration mode. To remove BRI message parameters, use the **no** form of this command.

```
bri {delay {max | min} milliseconds | retry number}
```

```
no bri {delay {max | min} | retry number}
```

Syntax Description	Parameter	Description
	<b>delay</b>	Specifies the delay option.
	<b>max</b> <i>milliseconds</i>	Specifies the maximum time, in milliseconds (ms) during which the Local Mobility Anchor (LMA) should wait for the Binding Revocation Acknowledgment (BRA) before retransmitting the BRI message. The range is from 500 to 65536.
	<b>min</b> <i>milliseconds</i>	Specifies the minimum time, in ms during which the LMA should wait before transmitting the BRI message. The range is from 500 to 65536.
	<b>retry</b> <i>number</i>	Specifies the maximum number of times the LMA should retransmit the BRI message until a BRA is received. The range is from 1 to 10.

**Command Default** The default value for the **max** keyword is 2, for the **min** keyword is 1, and for the **retry** keyword is 1.

**Command Modes** MAG configuration (config-ipv6-pmipv6-mag)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** The **max**, **min**, and **retry** keywords are MAX\_BRACK\_TIMEOUT, InitMINDelayBRIs, and BRIMaxRetriesNumber variables described in RFC 5846.

The **no bri delay {max | min}** command sets the **max** and **min** values to the default values configured in the Proxy Mobile IPv6 domain.

**Examples** The following example shows how to configure BRI retransmission parameters for the MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# bri delay max 4500
Router(config-ipv6-pmipv6-mag)# bri delay min 500
Router(config-ipv6-pmipv6-mag)# bri retry 6
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# clear ip mobile binding

To remove mobility bindings, use the **clear ip mobile binding** command in privileged EXEC mode.

```
clear ip mobile binding {all [load standby-group-name] | ip-address [coa care-of-address] | nai
string [session-id string] | vrf realm realm} [synch]
```

## Syntax Description

<b>all</b>	Clears all mobility bindings.
<b>load</b> <i>standby-group-name</i>	(Optional) Downloads mobility bindings for a standby group after a clear operation.
<i>ip-address</i>	IP address of a mobile node or mobile router.
<b>coa</b> <i>care-of-address</i>	(Optional) The binding corresponding to the IP address and its care-of address.
<b>nai</b> <i>string</i>	Network access identifier (NAI) of the mobile node.
<b>session-id</b> <i>string</i>	(Optional) Session identifier. The string value must be fewer than 25 characters in length.
<b>vrf realm</b> <i>realm</i>	Specifies the VRF realm.
<b>synch</b>	(Optional) Specifies that the bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The following keywords and argument were added: <ul style="list-style-type: none"> <li><b>all</b></li> <li><b>load</b></li> <li><i>standby-group-name</i></li> </ul>
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The <b>session-id</b> keyword was added.
12.4(9)T	The <b>coa</b> <i>care-of-address</i> keyword and argument combination were added.
12.4(11)T	The <b>vrf realm</b> <i>realm</i> and <b>synch</b> keywords and argument were added.

## Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. Associated with the mobility binding is the tunnel to the visited network and a host route to forward packets destined for the mobile node. Typically, there should be no need to clear the binding because it expires after the lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed through use of this command, the number of users on the tunnel is decremented and the host route is removed from the routing table. The mobile node is not notified.

If the **nai *string* session-id *string*** option is specified, only the binding entry with that session identifier is cleared. If the **session-id** keyword is not specified, all binding entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id *string*** value by using the **show ip mobile binding** command.

When the **synch** option is specified, bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent. When the redundancy mode is active-standby, the **synch** option will not take effect if the clear command is issued on the standby home agent.

Use this command with care, because it will disrupt any sessions used by the mobile node. After you use this command, the mobile node will need to reregister to continue roaming.

### Examples

The following example administratively stops mobile node 192.168.100.10 from roaming:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
192.168.100.10:
  Care-of Addr 192.168.6.1, Src Addr 192.168.4.2,
  Lifetime granted 02:46:40 (10000), remaining 02:46:32
  Flags SbdmGvt, Identification B750FAC4.C28F56A8,
  Tunnel100 src 192.168.1.2 dest 192.168.6.1 reverse-allowed
  Routing Options - (G)GRE

Router# clear ip mobile binding 10.2.0.1

Router# show ip mobile binding
```

### Related Commands

Command	Description
<b>show ip mobile binding</b>	Displays the mobility binding table.

# clear ip mobile host-counters

To clear the mobility counters specific to each mobile node, use the **clear ip mobile host-counters** command in EXEC mode.

```
clear ip mobile host-counters [[ip-address | nai string] undo]
```

## Syntax Description

<i>ip-address</i>	(Optional) IP address of a mobile node.
<b>nai</b> <i>string</i>	(Optional) Network access identifier of the mobile node.
<b>undo</b>	(Optional) Restores the previously cleared counters.

## Command Modes

EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	The <b>nai</b> keyword was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

This command clears the counters that are displayed when you use the **show ip mobile host** command. The **undo** keyword restores the counters (this option is useful for debugging).

## Examples

The following example shows how the counters can be used for debugging:

```
Router# show ip mobile host

10.0.0.1:
  Allowed lifetime 10:00:00 (36000/default)
  Roaming status -registered-, Home link on virtual network 10.15.15.0/8
  Accepted 2, Last time 04/13/02 19:04:28
  Overall service time 00:04:42
  Denied 0, Last time -never-
  Last code '-never- (0)'
  Total violations 1
  Tunnel to MN - pkts 0, bytes 0
  Reverse tunnel from MN - pkts 0, bytes 0

Router# clear ip mobile host-counters

Router# show ip mobile host-counters

10.0.0.1:
  Allowed lifetime 10:00:00 (36000/default)
  Roaming status -Unregistered-, Home link on virtual network 10.20.0.0/8
  Accepted 0, Last time -never-
  Overall service time -never-
  Denied 0, Last time -never-
  Last code '-never- (0)'
```

```
Total violations 0
Tunnel to MN - pkts 0, bytes 0
Reverse tunnel from MN - pkts 0, bytes 0
```

**Related Commands**

Command	Description
<b>show ip mobile host</b>	Displays mobile node counters and information.

# clear ip mobile router agent

To delete learned agents and the corresponding care-of address of the foreign agent from the mobile router agent table, use the **clear ip mobile router agent** command in privileged EXEC mode.

**clear ip mobile router agent** [*ip-address*]

## Syntax Description

<i>ip-address</i>	(Optional) IP address of an agent. If not specified, all agents are deleted from the agent table.
-------------------	---

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(4)T	This command was introduced.

## Usage Guidelines

The mobile router maintains an agent table listing active agents and the corresponding care-of address of the foreign agent. The mobile router uses this agent table to decide which foreign agent to register with. The mobile router updates the table when it receives advertisements. If an advertisement expires, its entry is automatically deleted from the table.

The **clear ip mobile router agent** *ip-address* option allows you to remove a specific agent.

## Examples

The following example removes all agents from the mobile router agent table:

```
Router# clear ip mobile router agent
```

## Related Commands

Command	Description
<b>show ip mobile router interface</b>	Displays information about the agents for the mobile router.

# clear ip mobile router registration

To delete registration entries from the mobile router registration table, use the **clear ip mobile router registration** command in privileged EXEC mode.

```
clear ip mobile router registration [ip-address]
```

## Syntax Description

<i>ip-address</i>	(Optional) IP address of a specific agent. If not specified, all registration entries are deleted.
-------------------	--

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.2(4)T	This command was introduced.

## Usage Guidelines

The mobile router maintains a registration table listing registration entries that are used for retransmissions. For example, a registration request is sent when no reply is received or the lifetime is about to expire.

A registration request can be removed from the table to prevent further registration requests from being sent to the agent. The **clear ip mobile router registration** *ip-address* option allows you to remove a registration to a specific agent.

Clearing an active registration will cause the mobile router to attempt to deregister.

## Examples

The following example removes all registration entries from the mobile router registration table:

```
Router# clear ip mobile router registration
```

## Related Commands

Command	Description
<b>show ip mobile router registration</b>	Displays the pending and accepted registrations of the mobile router.

# clear ip mobile router traffic

To clear the counters that the mobile router maintains, use the **clear ip mobile router traffic** command in privileged EXEC mode.

## clear ip mobile router traffic

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(4)T	This command was introduced.

**Usage Guidelines** Mobile router counters are accumulated during operation. They are useful for debugging and monitoring.

**Examples** The following example shows how the mobile router counters can be used for debugging:

```
Router# show ip mobile router traffic

Mobile Router Counters:

Agent Discovery:
  Solicitations sent 90, advertisements received 17
  Agent reboots detected 0
Registrations:
  Register 70, Deregister 0 requests sent
  Register 70, Deregister 0 replies received
  Requests accepted 68, denied 1 by HA 1 /FA 0
  Denied due to mismatched ID 1
  .
  .
  .
Router# clear ip mobile router traffic

Router# show ip mobile router traffic

Mobile Router Counters:

Agent Discovery:
  Solicitations sent 0, advertisements received 0
  Agent reboots detected 0
Registrations:
  Register 0, Deregister 0 requests sent
  Register 0, Deregister 0 replies received
  Requests accepted 0, denied 0 by HA 0 /FA 0
  Denied due to mismatched ID 0
  .
  .
  .
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip mobile router traffic</b>	Displays the counters that the mobile router maintains.

# clear ip mobile secure

To clear and retrieve remote security associations, use the **clear ip mobile secure** command in EXEC mode.

```
clear ip mobile secure {host lower [upper] | nai string | empty | all} [load]
```

## Syntax Description

<b>host</b>	Mobile node host.
<i>lower</i>	IP address of mobile node. Can be used alone, or as lower end of a range of IP addresses.
<i>upper</i>	(Optional) Upper end of a range of IP addresses.
<b>nai</b> <i>string</i>	Network access identifier of the mobile node.
<b>empty</b>	Load in only mobile nodes without security associations. Must be used with the <b>load</b> keyword.
<b>all</b>	Clears all mobile nodes.
<b>load</b>	(Optional) Reload the security association from the AAA server after security association has been cleared.

## Command Modes

EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>nai</b> keyword was added.
12.2(13)T	The <b>nai</b> keyword was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

Security associations are required for registration authentication. They can be stored on an AAA server. During registration, they may be stored locally after retrieval from the AAA server. The security association on the router may become stale or out of date when the security association on the AAA server changes.

This command clears security associations that have been downloaded from the AAA server.



### Note

Security associations that are manually configured on the router or not stored on the router after retrieval from the AAA server are not applicable.

## Examples

In the following example, the AAA server has the security association for user 10.2.0.1 after registration:

```
Router# show ip mobile secure host 10.2.0.1

Security Associations (algorithm,mode,replay protection,key) :
10.2.0.1:
  SPI 300, MD5, Prefix-suffix, Timestamp +/- 7,
  Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

If you change the security association stored on the AAA server for this mobile node, the router clears the security association and reloads it from the AAA server:

```
Router# clear ip mobile secure host 10.2.0.1 load
```

```
Router# show ip mobile secure host 10.2.0.1
```

```
10.2.0.1:  
  SPI 300, MD5, Prefix-suffix, Timestamp +/- 7,  
  Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip mobile secure</b>	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.

---

# clear ip mobile traffic

To clear counters, use the **clear ip mobile traffic** command in EXEC mode.

**clear ip mobile traffic [undo]**

<b>Syntax Description</b>	<b>undo</b> (Optional) Restores the previously cleared counters.				
<b>Command Modes</b>	EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(1)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.0(1)T	This command was introduced.
Release	Modification				
12.0(1)T	This command was introduced.				

## Usage Guidelines

Mobile IP counters are accumulated during operation. They are useful for debugging and monitoring. This command clears all Mobile IP counters. The **undo** keyword restores the counters (which is useful for debugging). See the **show ip mobile traffic** command for a description of all counters.

## Examples

The following example shows how counters can be used for debugging:

```
Router# show ip mobile traffic

IP Mobility traffic:
Advertisements:
  Solicitations received 0
  Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
  Register 8, Deregister 0 requests
  Register 7, Deregister 0 replied
  Accepted 6, No simultaneous bindings 0
  Denied 1, Ignored 1
  Unspecified 0, Unknown HA 0
  Administrative prohibited 0, No resource 0
  Authentication failed MN 0, FA 0
  Bad identification 1, Bad request form 0
.

Router# clear ip mobile traffic

Router# show ip mobile traffic

IP Mobility traffic:
Advertisements:
  Solicitations received 0
  Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
  Register 0, Deregister 0 requests
  Register 0, Deregister 0 replied
  Accepted 0, No simultaneous bindings 0
  Denied 0, Ignored 0
  Unspecified 0, Unknown HA 0
  Administrative prohibited 0, No resource 0
```

```
Authentication failed MN 0, FA 0  
Bad identification 0, Bad request form 0
```

**Related Commands**

Command	Description
<b>show ip mobile traffic</b>	Displays protocol counters.

# clear ip mobile visitor

To remove visitor information, use the **clear ip mobile visitor** command in privileged EXEC mode.

```
clear ip mobile visitor [ip-address | nai string [session-id string] [ip-address]]
```

Syntax Description		
<i>ip-address</i>	(Optional) IP address. If not specified, visitor information will be removed for all addresses.	
<b>nai</b> <i>string</i>	(Optional) Network access identifier (NAI) of the mobile node.	
<b>session-id</b> <i>string</i>	(Optional) Session identifier. The string value must be fewer than 25 characters in length.	
<i>ip-address</i>	(Optional) IP address associated with the NAI.	

**Command Modes** EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(2)XC	The <b>nai</b> keyword and associated variables were added.
	12.2(13)T	The <b>nai</b> keyword and associated variables were integrated into Cisco IOS Release 12.2(13)T.
	12.3(4)T	The <b>session-id</b> keyword was added.

**Usage Guidelines**

The foreign agent creates a visitor entry for each accepted visitor. The visitor entry allows the mobile node to receive packets while in a visited network. Associated with the visitor entry is the Address Resolution Protocol (ARP) entry for the visitor. There should be no need to clear the entry because it expires after lifetime is reached or when the mobile node deregisters.

When a visitor entry is removed, the number of users on the tunnel is decremented and the ARP entry is removed from the ARP cache. The visitor is not notified.

If the **nai** *string* **session-id** *string* option is specified, only the visitor entry with that session identifier is cleared. If the **session-id** keyword is not specified, all visitor entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id** *string* value by using the **show ip mobile visitor** command.

Use this command with care because it may terminate any sessions used by the mobile node. After you use this command, the visitor will need to reregister to continue roaming.

**Examples** The following example administratively stops visitor 172.21.58.16 from visiting:

```
Router# clear ip mobile visitor 172.21.58.16
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip mobile visitor</b>	Displays the table containing the visitor list of the foreign agent.

---

# clear ipv6 mobile pmipv6 mag

To reset the Proxy Mobile IPv6 (PMIP) domain Mobile Access Gateway (MAG) sessions, use the **clear ipv6 mobile pmipv6 mag** command in privileged EXEC mode.

```
clear ipv6 mobile pmipv6 mag { binding { all | lma lma-v6-address | nai nai-string [interface type number] } | stats [domain domain-name peer peer-name] }
```

Syntax Description		
<b>binding</b>		Specifies the binding sessions.
<b>all</b>		Resets all sessions.
<b>lma</b> <i>lma-v6-address</i>		Resets the binding sessions for the Local Mobility Anchor (LMA).
<b>nai</b> <i>nai-string</i>		Resets the binding sessions for the mobile node (MN).
<b>interface</b> <i>type number</i>	(Optional)	Resets the binding sessions for the MN interface.
<b>stats</b>		Specifies all MAG statistics.
<b>domain</b> <i>domain-name</i>	(Optional)	Resets the statistics for the LMA in the PMIP domain.
<b>peer</b> <i>peer-name</i>		Specifies the LMA.

**Command Default** No reset is initiated.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

## Examples

The following example shows how to clear the binding sessions for the MN:

```
Router(config)# show ipv6 mobile pmipv6 mag bindings
!
Total number of bindings: 1
-----
[Binding][MN]: Domain: D1, Nai: MN3@cisco.com
      [Binding][MN]: State: ACTIVE
      [Binding][MN]: Interface: Ethernet0/0
      [Binding][MN]: Hoa: 0x11110106, att: 3, llid: aabb.cc00.ce00
      [Binding][MN][LMA]: Id: LMA2
      [Binding][MN][LMA]: lifetime: 3600
!
Router(config)# clear ipv6 mobile pmipv6 mag binding nai MN3@example.com
Router(config)# show ipv6 mobile pmipv6 mag bindings
!
Total number of bindings: 0
```

The following example shows how to clear all MAG statistics:

```
Router(config)# clear ipv6 mobile pmipv6 mag stats
```

The following example shows how to clear MAG statistics for the LMA:

```
Router(config)# clear ipv6 mobile pmipv6 mag stats domain D1 peer lma1
```

Related Commands	Command	Description
	show ipv6 mobile pmipv6 mag bindings	Displays MAG bindings.
	show ipv6 mobile pmipv6 mag globals	Displays the MAG configuration.
	show ipv6 mobile pmipv6 mag stats	Displays MAG statistics.

# collocated single-tunnel

To configure the number of tunnels between the mobile router and home agent when registering with a collocated care-of address (CCoA), use the **collocated single-tunnel** command in mobile router configuration mode.

## collocated single-tunnel

**Syntax Description** This command has no arguments or keywords.

**Defaults** Defaults to single-tunnel enabled.

**Command Modes** Mobile router

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** This command is used as a “placeholder” only and defaults to single-tunnel enabled. This command can not be unconfigured. In future Cisco IOS releases, a dual-tunnel capability will be needed for IPSec between the mobile router and the home agent. At that time, this command will be optional with dual tunnels (**no collocated single-tunnel**) being the default. This command is provided now for backward compatibility when the dual-tunnel capability is implemented.

# debug ipv6 mobile mag

To debug the Mobile Access Gateway (MAG) application programming interface (API), information, or events, use the **debug ipv6 mobile mag** command in privileged EXEC mode. To disable display of the debugging output, use the **no** form of this command.

```
debug ipv6 mobile mag {api | events | info}
```

```
no debug ipv6 mobile mag {api | events | info}
```

Syntax Description	api	Enables API-specific debug events.
	events	Enables all events occurring within the Local Mobility Anchor (LMA) and the MAG.
	info	Provides debug information within the Proxy Mobile IPv6 (PMIP) module.

**Command Default** Debugging is not enabled.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Examples** The following sample output from the **debug ipv6 mobile mag api** command displays the APIs that are called during the call setup flow:

```
Router# debug ipv6 mobile mag api

07:52:08.051: MIP_PDL_API: pmipv6_pdl_get_att API Called
07:52:08.051: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
07:52:08.051: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
07:52:08.051: [PMIPV6_MAG_API]: mag_bul_do_state_transition API called
07:52:08.051: [PMIPV6_MAG_API]: pmipv6_mag_bul_null_state_hdlr API called
07:52:08.051: [PMIPV6_MAG_API]: pmipv6_mag_bul_null_state_exit API called
07:52:08.051: [PMIPV6_MAG_API]: pmipv6_mag_bul_init_state_entry API called
07:52:08.051: [PMIPV6_BINDING_API]: pmipv6_add_binding_entry API called
07:52:08.051: MIP_PDL_API: pmipv6_pdl_get_timestamp API Called
07:52:08.053: [PMIPV6_MAG_API]: pmipv6_mag_should_handle_pkt called
07:52:08.053: [PMIPV6_MAG_API]: pmipv6_mag_message_handler called
07:52:08.053: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
07:52:08.053: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
07:52:08.053: [PMIPV6_MAG_API]: mag_bul_do_state_transition API called
07:52:08.053: [PMIPV6_MAG_API]: pmipv6_mag_bul_init_state_hdlr API called
07:52:08.053: [PMIPV6_MAG_API]: pmipv6_mag_bul_init_state_exit API called
07:52:08.053: MIP_PDL_API: pmipv6_pdl_create_vintf API Called
16 07:52:08.054: MIP_PDL_API: pmipv6_pdl_set_ip4address API Called
16 07:52:08.054: MIP_PDL_API: pmipv6_pdl_set_macaddr API Called
16 07:52:08.054: MIP_PDL_API: mip_pdl_setupv4_route API Called
```

```

07:52:08.054: MIP_PDL_API: mip_pdl_setupv6_tunnel API Called
07:52:08.054: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to
down
07:52:08.054: MIP_PDL_API: mip_pdl_get_handle_for_tunnel API Called
07:52:08.054: MIP_PDL_API: mip_pdl_populate_rtunnel API Called
07:52:08.054: MIP_PDL_API: mip_pdl_get_handle_for_tunnel API Called
07:52:08.055: [PMIPV6_BINDING_API]: pmipv6_update_binding_key API called
07:52:08.055: [PMIPV6_MAG_API]: pmipv6_mag_bul_active_state_entry API called

```

The following example shows the output of the **debug ipv6 mobile mag events** command:

```
Router# debug ipv6 mobile mag events
```

```
PMIPv6 MAG Event debug is turned on
```

The following line shows that the DHCP Discover trigger is received from the mobile node (MN):

```
07:48:31.638: [PMIPV6_MAG_EVENT]: Trigger request received (DHCP Discover trigger) from
(MN3@cisco.com)
```

The following line shows the MAG machine state change. A new MN attaches to the MAG and the state changes from NULL to INIT:

```
07:48:31.638: [PMIPV6_MAG_EVENT]: Event received New MN intf attached in state: NULL, new
state: INIT
```

The following line shows that the Proxy Binding Update (PBU) message is sent from MAG for an MN:

```
07:48:31.638: [PMIPV6_MAG_EVENT]: PBU message sent
```

The following lines show that the Proxy Binding Acknowledgment (PBA) is received from the LMA for the MN. The incoming parameters are link layer identifier (lli) length, value, and access technology type (att). The status 0 indicates success.

```

07:48:31.639: [PMIPV6_MAG_EVENT]: message received: PBA
07:48:31.639: [PMIPV6_MAG_EVENT]: PBA: nai(MN3@cisco.com),nai len: 14, lli
(aabb.cc00.ce00), ll len: 16, att:3, status:0

```

The following line shows that the refresh timer has started:

```
07:48:31.639: [PMIPV6_MAG_EVENT]: Starting Refresh timer, period (300000)
```

The following lines show that a v4 route is added to the MN, which has a new address assigned. A new v6 tunnel is created and a reverse tunnel entry is added for the MN.

```

07:48:31.640: [PMIPV6_MAG_EVENT]: Adding V4 route, address (0x11110103), Prefix len (24),
handle: (GigabitEthernet0/0/0)
!
07:48:31.640: [PMIPV6_MAG_EVENT]: Adding V6 Tunnel, Handle (Tunnel1), mode: (IPV6_IN_IPV6)
07:48:31.641: [PMIPV6_MAG_EVENT]: Populating Reverse V4 Tunnel entry, l2 address
(0xaabb.cc00.ce00), ipv4 add: 0x11110103 phy handle: (GigabitEthernet0/0/0)

```

The following example shows the output of **debug ipv6 mobile mag info** command:

```
Router# debug ipv6 mobile mag info
```

```
PMIPv6 MAG INFO debug is turned on
```

The following lines show that the new binding is created and added to the AV tree:

```

07:50:31.714: [PMIPV6_PDB_INFO]: MN entry MN3@cisco.com found in hashset
07:50:31.714: [PMIPV6_BINDING_INFO]: binding added New NAI AVL node created

```

The following line provides more information about the PBUs that are sent:

```
07:50:31.714: [PMIPV6_MAG_INFO]: PBU message nai(MN3@cisco.com), nai len: 14, hoa(0),
att(3) llid(aabb.cc00.ce00) , ll len: 16
```

The following line shows that a binding for the MN using the Network Access Identifier (NAI) MN3@example.com is found:

```
07:50:31.717: [PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: MN3@example.com
07:50:31.717: [PMIPV6_BINDING_INFO]: binding found on NAI tree
```

The following line shows that a virtual interface is created in the MAG and assigned the MAC address aaaa.aaaa.aaaa:

```
07:50:31.717: [PMIPV6_MAG_EVENT]: Creating virtual interface handle (IFNAME_PMIP_VIF4)
07:50:31.717: [PMIPV6_MAG_INFO]: Setting Mac Address (aaaa.aaaa.aaaa) on
(IFNAME_PMIP_VIF4)
```

The following line shows that a route for the MN is added in the MAG:

```
07:50:31.717: MIP_PDL_INFO: Successfully added route 10.10.1.4/24 to GigabitEthernet0/0/0
07:50:31.717: MIP_PDL_INFO: Route via: GigabitEthernet0/1/0 (IPv6)
```

The following line shows that a tunnel is created with a source address and a destination address:

```
07:50:31.718: MIP_PDL_INFO: Tunnel0 (IPv6) created with src 2000::4 dst 2001::2
07:50:31.718: MIP_PDL_INFO: Rev. Tunnel acl entry added for subnet (10.10.0.0)
```

---

**Related Commands**

Command	Description
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

---

# debug ipv6 mobile packets

To debug the Proxy Mobile IPv4 or IPv6 packets, use the **debug ipv6 mobile packets** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

**debug ipv6 mobile packets**

**no debug ipv6 mobile packets**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Debugging is not enabled.

**Command Modes** Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Examples

The following example is sample output from the **debug ipv6 mobile packets** command:

```
Router# debug ipv6 mobile packets
```

```
PMIPv6 PKT debug is turned on
```

The following lines show the newly allocated packet size and the inner packet details:

```
07:51:17.693: [PMIPv6-MM]:Allocated packet of size 164 with tlv length 84
07:51:17.693: [PMIPV6_MM] Sending UDP Packet, src: 0x2020202, dst: 0x6060602, sport: 5436,
dport:5436
```

The following lines shows the mobility options, the value, and the length:

```
07:51:17.693: [PMIPV6_MM] NAI option included len 14
!
2A986107E0:          4D 4E334063 6973636F          MN3@abc
2A986107F0: 2E636F6D 1702          .com..
07:51:17.693:
07:51:17.693: [PMIPV6_MM] HI option included len 2 val 4
07:51:17.694: [PMIPV6_MM] ATT option included len 2 val 3
07:51:17.694: [PMIPV6_MM] TIMESTAMP option included len 8 value 3517199477
07:51:17.694: [PMIPV6_MM] LLI option included len 16
!
2A98610810: 61616262 2E636330 302E6365 30300100  aabb.cc00.ce00..
2A98610820: 24          $
07:51:17.694:
07:51:17.694: [PMIPV6_MM] V4HOAREQ option included len 6 val 0.0.0.0
07:51:17.694: [PMIPV6_MM] V4DFT_RTR option included len 6 val 0.0.0.0
07:51:17.694: **** Dumping the TLVs ****
!
```

```

2A986107E0: 01020000 080E014D 4E334063 6973636F .....MN3@cisco
2A986107F0: 2E636F6D 17020004 18020003 01001B08 .com.....
2A98610800: 00000000 D1A43475 01020000 19100000 ...Q$4u.....
2A98610810: 61616262 2E636330 302E6365 30300100 aabb.cc00.ce00..
2A98610820: 24060000 00000000 26060000 00000000 $.&.....
2A98610830: 01020000 .....
07:51:17.694:
07:51:17.695: [PMIPV6_MM] NAI option received len 14
!
2A97DBE560:          4D 4E334063 6973636F 2E636F6D      MN3@cisco.com
2A97DBE570: 0017              ..
07:51:17.696:
07:51:17.696: [PMIPV6_MM] HI option received len 2 val 4
07:51:17.696: [PMIPV6_MM] ATT option received len 2 val 3
07:51:17.696: [PMIPV6_MM] TIMESTAMP option received len 8 value 3517199477
07:51:17.696: [PMIPV6_MM] LLI option received len 16
!
2A97DBE580:                    61616262              aabb
2A97DBE590: 2E636330 302E6365 30300100 00          .cc00.ce00...
07:51:17.696:
07:51:17.696: [PMIPV6_MM] V4HOAREPLY option received len 6 val 10.10.1.5
07:51:17.696: [PMIPV6_MM] V4DFT_RTR option received len 6 val 10.10.1.1

```

The following lines show the dump of the packet with all the Type Length Values (TLVs):

```

07:51:17.696: **** Dumping the TLVs ****
!
2A97DBE550:                    01020000              ....
2A97DBE560: 080E014D 4E334063 6973636F 2E636F6D ...MN3@cisco.com
2A97DBE570: 00170200 04180200 03001B08 00000000 .....
2A97DBE580: D1A43475 01020000 19100000 61616262 Q$4u.....aabb
2A97DBE590: 2E636330 302E6365 30300100 00000000 .cc00.ce00.....
2A97DBE5A0: 00000000 00000000 00000000 00000000 .....
2A97DBE5B0: 25060060 11110105 26060000 11110101 %..`....&.....
2A97DBE5C0:
07:51:17.696:

```

#### Related Commands

Command	Description
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# description (mobile networks)

To add a description to a mobile router configuration, use the **description** command in mobile networks configuration mode. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

<b>Syntax Description</b>	<i>string</i>	Comment or description about the mobile router or its networks.
---------------------------	---------------	---

<b>Defaults</b>	No default behavior or values.	
-----------------	--------------------------------	--

<b>Command Modes</b>	Mobile networks configuration	
----------------------	-------------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(4)T	This command was introduced.

<b>Usage Guidelines</b>	The <b>description</b> command is meant solely as a comment to be put in the configuration to help you remember information about the configured mobile router or its mobile networks.	
-------------------------	--	--

<b>Examples</b>	The following example shows how to add a description for the mobile router:	
-----------------	---	--

```
ip mobile mobile-networks 10.2.0.1
description mobileunit
network 172.16.1.0 255.255.255.0
network 172.16.2.0 255.255.255.0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip mobile mobile-networks</b>	Displays a list of mobile networks associated with the mobile router.

# discover-mn-detach

To enable the periodic verification of the mobile node (MN) attachment with the Mobile Access Gateway (MAG)-enabled interface, use the **discover-mn-detach** command in MAG configuration mode. To disable the periodic verification, use the **no** form of this command.

**discover-mn-detach** *seconds timeout-seconds*

**no discover-mn-detach**

Syntax Description	seconds	Period for verifying the MN attachment, in seconds. The range is from 1 to 100.
	timeout-seconds	Timeout for response from the MN, in seconds. The timeout range is from 1 to 10, and should be less than the value for the period.

**Command Default** The periodic verification of the MN attachment is not enabled.

**Command Modes** MAG configuration (config-ipv6-pmipv6-mag)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** Use the **discover-mn-detach** command to enable periodic verification of the MN attachment with the MAG-enabled interface. When periodic verification is enabled, the MAG periodically verifies the MN attachment using the Address Resolution Protocol (ARP) request or the neighbor solicitation. When the mobile client responds with the ARP reply or the neighbor advertisement, a trigger attach is generated, thereby confirming that the MN is attached to the interface.

**Examples** The following example shows how to periodically verify the MN attachment with the MAG-enabled interface:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# discover-mn-detach 45 5
```

Related Commands	Command	Description
	<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
	<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# eigrp interface



## Note

Effective with Cisco IOS Release 15.0(1)M, the **eigrp interface** command is replaced by the **dampening-change** command and the **dampening-interval** command. See the **dampening-change** and **dampening-interval** commands for more information.

To set a threshold value to minimize hysteresis in a router-to-radio configuration, use the **eigrp interface** command in interface configuration mode. To reset the hysteresis threshold to the default value, use the **no** form of this command.

```
eigrp vmi-interface-number interface [dampening-change value] [dampening-interval value]
```

```
no eigrp vmi-interface-number interface [dampening-change value] [dampening-interval value]
```

## Syntax Description

<i>vmi-interface-number</i>	The number assigned to the VMI interface.
<b>dampening-change</b> <i>value</i>	(Optional) Value used to minimize the effect of frequent routing changes in router-to-radio configurations. Percent interface metric must change to cause update. Value range is 1 to 100.
<b>dampening-interval</b> <i>value</i>	(Optional) Specifies the time interval in seconds to check the interface metrics at which advertising of routing changes occurs. The default value is 30 seconds. Value range is 1 to 65535.

## Command Default

Default for change-based dampening is 50 percent of the computed metric.  
Default for interval-based dampening is 30 seconds.

## Command Modes

Interface configuration (config-if)

## Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.0(1)M	This command was replaced. This command was replaced by the <b>dampening-change</b> command and the <b>dampening-interval</b> command.

## Usage Guidelines

This command advertises routing changes for EIGRP traffic only.

The REPLY sent to any QUERY will always contain the latest metric information. Exceptions which will result in immediate UPDATE being sent:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

**Change-based Dampening**

The **default** value for the change tolerance will be 50% of the computed metric. It can be configured in the range from 0 to 100 percent. If the metric change of the interface is not greater (or less) than the current metric plus or minus the specified amount, the change will not result in a routing change, and no update will be sent to other adjacencies.

**Interval-based Dampening**

The default value for the update intervals is 30 seconds. It can be configured in the range from 0 to 64535 seconds. If this option is specified, changes in routes learned through this interface, or in the interface metrics, will not be advertised to adjacencies until the specified interval is met. When the timer expires, any changes detected in any routes learned through the interface, or the metric reported by the interfaces will be sent out.

**Examples****Change-based Dampening Example**

The following example sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-change 50
 physical-interface Ethernet0/0
```

**Interval-based Dampening Example**

The following example sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-interval 30
 physical-interface Ethernet0/0
```

**Related Commands**

Command	Description
<b>debug vmi</b>	Displays debugging output for virtual multipoint interfaces (VMIs)
<b>interface vmi</b>	Creates a virtual multipoint interface (VMI) that can be configured and applied dynamically.

# encap (Proxy Mobile IPv6)

To configure the tunnel encapsulation mode type between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA), use the **encap** command in PMIP domain or MAG-LMA configuration mode. To disable the tunnel encapsulation mode type, use the **no** form of this command.

```
encap {gre-ipv4 | ipv6-in-ipv6}
```

```
no encap {gre-ipv4 | ipv6-in-ipv6}
```

## Syntax Description

<b>gre-ipv4</b>	Sets the tunnel encapsulation mode type to generic routing encapsulation in IPv4.
<b>ipv6-in-ipv6</b>	Sets the tunnel encapsulation mode type to IPv6_in_IPv6.

## Command Default

The Proxy Mobile IPv6 (PMIP) tunnel encapsulation mode type is IPv6\_in\_IPv6.

## Command Modes

MAG-LMA configuration (config-ipv6-pmipv6mag-lma)  
PMIP domain configuration (config-ipv6-pmipv6-domain)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Usage Guidelines

Use the **encap** command in PMIP domain configuration mode to configure the tunnel encapsulation type for the PMIP domain. The LMAs and the MAGs within the PMIP domain use this configuration as the default.

Use the **encap** command in MAG-LMA configuration mode to configure the tunnel encapsulation type for the LMA within the MAG.



**Note** In Cisco IOS XE 3.4S, the only supported encapsulation type is IPv6\_in\_IPv6.

## Examples

The following example shows how to configure the encapsulation type as IPv6\_in\_IPv6 in MAG-LMA configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# lma lma1 dn1
Router(config-ipv6-pmipv6mag-lma)# encap ipv6-in-ipv6
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.
<b>lma</b>	Configures the LMA for the PMIP domain.

# fixed-link-layer-address

To configure the fixed link-layer address (Layer-2 address) for the Mobile Access Gateway (MAG)-enabled interface toward the mobile node (MN), use the **fixed-link-layer-address** command in PMIP domain or MAG configuration mode. To remove the fixed Layer-2 address for the MAG-enabled interface, use the **no** form of this command.

**fixed-link-layer-address** *hardware-address*

**no fixed-link-layer-address**

<b>Syntax Description</b>	<i>hardware-address</i>	The 48-bit hardware address.
<b>Command Default</b>	No fixed link-layer address is configured.	
<b>Command Modes</b>	MAG configuration (config-ipv6-pmipv6-mag) PMIP domain configuration (config-ipv6-pmipv6-domain)	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines**

Use the **fixed-link-layer-address** command in PMIP domain configuration mode to configure the fixed link-layer address for the MAG-enabled interface within the Proxy Mobile IPv6 (PMIP) domain. If the PMIP domain is configured using the **ipv6 mobile pmipv6-domain domain-name load-aaa** command, use the **fixed-link-layer-address** command to override the fixed link-layer address configuration.

Use the **fixed-link-layer-address** command in MAG configuration mode to configure the fixed link-layer address for the MAG-enabled interface.

**Examples**

The following example shows how to configure the fixed link-layer address for the MAG-enabled interface toward the MN in PMIP domain configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# fixed-link-layer-address aaaa.bbbb.cccc
```

The following example shows how to configure the fixed link-layer address for the MAG-enabled interface in MAG configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# fixed-link-layer-address aaaa.bbbb.cccc
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# fixed-link-local-address

To configure the fixed link-local address for the Mobile Access Gateway (MAG)-enabled interface toward the mobile node (MN), use the **fixed-link-local-address** command in PMIP domain or MAG configuration mode. To remove the fixed link-local address on the MAG-enabled interface, use the **no** form of this command.

**fixed-link-local-address** *ipv6-address*

**no fixed-link-local-address**

<b>Syntax Description</b>	<i>ipv6-address</i>	The IPv6 link-local address assigned to the MAG-enabled interface toward the MN.
---------------------------	---------------------	--

**Command Default** No fixed link-local address is configured for the MAG-enabled interface toward the MN.

**Command Modes** MAG configuration (config-ipv6-pmipv6-mag)  
PMIP domain configuration (config-ipv6-pmipv6-domain)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE Release 3.4S	This command was introduced.

**Usage Guidelines** Use the **fixed-link-local-address** command in the PMIP domain configuration mode to configure the fixed link-local address for the MAG-enabled interface within the Proxy Mobile IPv6 (PMIP) domain. If the PMIP domain is configured using **ipv6 mobile pmipv6-domain domain-name load-aaa** command, use the **fixed-link-local-address** command to override the fixed link-local address configuration.

Use the **fixed-link-local-address** command in MAG configuration mode to configure the fixed link-local address for the MAG-enabled interface.

**Examples** The following example shows how to configure the fixed link-local address for the MAG-enabled interface toward the MN in PMIP domain configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# fixed-link-local-address FE80:0DB8:3333:4::5
```

The following example shows how to configure the fixed link-local address for the MAG-enabled interface in MAG configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# fixed-link-local-address FE80:0DB8:3333:4::5
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# gre-encap-key

To configure the generic routing encapsulation (GRE) key for the mobile node (MN) within the Proxy Mobile IPv6 (PMIP) domain, use the **gre-encap-key** command in mobile node configuration mode. To remove the configuration, use the **no** form of this command.

**gre-encap-key** [**down** *key-value* | **up** *key-value*]

**no gre-encap-key** [**down** | **up**]

## Syntax Description

<b>down</b> <i>key-value</i>	(Optional) Specifies the encapsulation key as downstream, from the Local Mobility Anchor (LMA) to the Mobile Access Gateway (MAG). The range for the <i>key-value</i> argument is from 0 to 4294967295.
<b>up</b> <i>key-value</i>	(Optional) Specifies the encapsulation key as upstream, from the MAG to the LMA. The range for the <i>key-value</i> argument is from 0 to 4294967295.

## Command Default

No GRE key is configured.

## Command Modes

Mobile node configuration (config-ipv6-pmipv6-domain-mn)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Examples

The following example shows how to configure the GRE key from the LMA to the MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# nai example@example.com
Router(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 45
```

## Related Commands

Command	Description
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>nai</b>	Configures the NAI for the MN within the PMIP domain.

# home-agent

To specify the home agent that the mobile router uses during registration, use the **home-agent** command in mobile router configuration mode. To disable the home agent, use the **no** form of this command.

**home-agent** *ip-address* [**priority level**]

**no home-agent** *ip-address* [**priority level**]

## Syntax Description

<i>ip-address</i>	Home IP address.
<b>priority level</b>	(Optional) Priority level that prioritizes which home agent address is the best to use during registration. The range is from 0 to 255, where 0 denotes the lowest priority and 255 denotes the highest priority. The default is 100.

## Defaults

The default priority level is 100.

## Command Modes

Mobile router configuration

## Command History

Release	Modification
12.2(4)T	This command was introduced.

## Usage Guidelines

The **home-agent** command specifies which home agent the mobile router uses for registration and to detect when it is home. The priority level determines which home agent address to register with, although all addresses are on the same home agent. The mobile router registers with the home agent with the highest priority level.

The home agent address list is used to detect when the mobile router is home. The mobile router knows that it is at home when the source of the agent advertisements is an IP source address that exists on the home agent address list.

## Examples

The following example shows that the mobile router will use the home agent address 1.1.1.1 during registration and will detect when it is at home after receiving agent advertisements from either address 1.1.1.1 or 2.2.2.2:

```
router mobile
ip mobile router
address 10.1.0.1 255.255.0.0
home-agent 1.1.1.1 priority 101
home-agent 2.2.2.2 priority 100
```

## Related Commands

Command	Description
<b>show ip mobile router</b>	Displays configuration information and monitoring statistics about the mobile router.

# int att

To configure the access technology type (ATT), the interface, and the MAC address of the mobile node (MN) interface within the Proxy Mobile IPv6 (PMIP) domain, use the **int att** command in mobile node configuration mode. To remove the configuration of the MN, use the **no** form of this command.

**int att** *interface-access-type* **l2-addr** *mac-address*

**no int att** *interface-access-type* **l2-addr** *mac-address*

## Syntax Description

<i>interface-access-type</i>	MN interface access technology type. The type can be <b>ethernet</b> , <b>PPP</b> , <b>virtual</b> , <b>wimax</b> , or <b>wlan</b> .
<b>l2-addr</b>	Specifies the MAC address of the MN interface.
<i>mac-address</i>	MAC address of the MN interface.

## Command Default

The ATT, interface type, and MAC address are not configured for the MN.

## Command Modes

Mobile node configuration (config-ipv6-pmipv6-domain-mn)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Examples

The following example shows how to configure the ATT, interface type, and MAC address of the MN interface:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# nai example@example.com
Router(config-ipv6-pmipv6-domain-mn)# int att ETHERNET l2-addr 02c7.f800.0422
```

## Related Commands

Command	Description
<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
<b>nai</b>	Configures the NAI for the MN within the PMIP domain.

# interface (proxy mobile IPv6)

To configure the interface where Mobile Access Gateway (MAG) functionality is enabled, use the **interface** command in MAG configuration mode. To remove the interface configuration, use the **no** form of this command.

**interface** *type number*

**no interface** *type number*

Syntax Description	<i>type</i>	Type of interface to be configured.
	<i>number</i>	Port, connector, or interface card number.

**Command Default** MAG functionality for the interface is not configured.

**Command Modes** MAG configuration (config-ipv6-pmipv6-mag)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.

**Examples** The following example shows how to enable the GigabitEthernet interface for the MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# interface GigabitEthernet0/1/0
```

Related Commands	Command	Description
	<b>ipv6 mobile pmipv6-domain</b>	Configures the PMIP domain.
	<b>ipv6 mobile pmipv6-mag</b>	Configures the MAG for the PMIP domain.

# ip dampening-change eigrp

To set a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4, use the **ip dampening-change eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip dampening-change eigrp** *as-number* [*change-percentage*]

**no ip dampening-change eigrp** *as-number*

Syntax Description	
<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.
<i>change-percentage</i>	(Optional) The percentage a metric must change before the value is stored for future decisions on advertisements.  The range is from 1 to 100. If a change-percentage value is not specified, the default is 50 percent of the computed metric.

**Command Default** No threshold percentage is configured.

**Command Modes** Interface configuration (config-if)  
Virtual network interface (config-if-vnet)

Command History	Release	Modification
	15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
	Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

**Usage Guidelines** The **ip dampening-change eigrp** command is supported only for Mobile Ad Hoc Networking (MANET) router-to-radio links.

When a peer metric changes on an interface that is configured with the **ip dampening-change eigrp** command, EIGRP multiplies the dampening-change percentage with the old peer metric and compares the result (the threshold) to the difference between the old and new metrics. If the metric difference is greater than the calculated threshold, then the new metric is applied and the routes learned from that peer are updated and advertised to other peers. If the metric difference is less than the threshold, the new metric is discarded.

The following are the exceptions that will result in an immediate update of the routes regardless of the dampening-change setting:

- An interface is down.
- A route is down.
- A change in the metric that results in the router selecting a new next hop.

Peer metric changes that do not exceed a configured change percentage and that do not result in a routing change do not cause an update to be sent to other adjacencies. Peer metric changes are based on the stored last-update of the peer. Peer metric changes that exceed the threshold value are stored and used for future comparisons.

### Examples

The following example shows how to configure the EIGRP to accept a peer metric change if the change is greater than 75 percent of the last updated value:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip dampening-change eigrp 1 75
```

### Related Commands

Command	Description
<b>dampening-interval</b>	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
<b>dampening-change</b>	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
<b>ip dampening-interval</b>	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv4.
<b>ipv6 dampening-change</b>	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.
<b>ipv6 dampening-interval</b>	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.

# ip dampening-interval eigrp

To set a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4, use the **ip dampening-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip dampening-interval eigrp** *as-number* [*interval*]

**no ip dampening-interval eigrp** *as-number*

## Syntax Description

<i>as-number</i>	Autonomous system number. The range is from 1 to 65535.
<i>interval</i>	(Optional) Time interval, in seconds, that must elapse before a route change will cause an update to occur.  The range is from 1 to 65535. If an <i>interval</i> value is not specified, the default is 30 seconds.

## Command Default

A dampening interval is not enabled.

## Command Modes

Interface configuration (config-if)  
Virtual network interface (config-if-vnet)

## Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

## Usage Guidelines

The **ip dampening-interval eigrp** command is supported only for Mobile Ad Hoc Networking (MANET) Router-to-Radio links.

When a peer metric changes on an interface that is configured with a dampening interval, EIGRP for IPv4 will apply the metric change only if the time difference since the last metric change exceeds the specified interval. If the time difference is less than the specified interval, the update is discarded.

The following are the exceptions that result in an immediate update of the routes regardless of the dampening interval settings:

- An interface is down.
- A route is down.
- A change in the metric that results in the router selecting a new next hop.

**Examples**

The following example shows how to configure EIGRP for IPv4 on a FastEthernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip dampening-interval eigrp 1 45
```

**Related Commands**

Command	Description
<b>dampening-change</b>	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
<b>dampening-interval</b>	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
<b>ip dampening-change</b>	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv4.
<b>ipv6 dampening-change</b>	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.
<b>ipv6 dampening-interval</b>	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.

# ip dhcp client mobile renew

To configure the number of renewal attempts and the interval between attempts for renewing an IP address acquired by a Dynamic Host Configuration Protocol (DHCP) client, use the **ip dhcp client mobile renew** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

**ip dhcp client mobile renew count** *number interval ms*

**no ip dhcp client mobile renew count** *number interval ms*

## Syntax Description

<b>count</b> <i>number</i>	Number of attempts to renew a current IP address before starting the DHCP discovery process. The range is from 0 to 10 attempts. The default is 2 attempts.
<b>interval</b> <i>ms</i>	Interval to wait between renewal attempts. The range is from 1 to 1000 ms. The default is 50 ms.

## Defaults

**count** *number*: 2  
**interval** *ms*: 50

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(14)T	This command was introduced.

## Usage Guidelines

Mobile DHCP clients automatically attempt to renew an existing IP address in response to certain events, such as moving between wireless access points. The number of renewal attempts, and the interval between those attempts, depending on network conditions, can be modified by using the **ip dhcp client mobile renew** command.

## Examples

In the following example, the DHCP client will make four attempts to renew its current IP address with an interval of 30 milliseconds between attempts :

```
interface FastEthernet0
 ip dhcp client mobile renew count 4 interval 30
```

## Related Commands

Command	Description
<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.

# ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

**ip mobile arp** [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

**no ip mobile arp**

Syntax Description		
<b>timers</b>		(Optional) Sets local-area mobility timers.
<i>keepalive</i>		(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default value is 5.
<i>hold-time</i>		(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default value is 15.
<b>access-group</b>		(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
<i>access-list-number</i>		(Optional) Number of a standard IP access list. The range is from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
<i>name</i>		(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

**Command Default** Local-area mobility is disabled.

**Command Modes** Interface configuration (config-if)

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	XE 2.5.1	This command was integrated into Cisco IOS XE Release 2.5.1. VRF-awareness for local-area mobility is available in this release.

**Usage Guidelines**

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be mistaken for mobile nodes and disrupt normal operations.

**Examples**

The following example shows how to configure local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
interface ethernet 0
ip mobile arp access-group 10
```

**Related Commands**

Command	Description
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>default-metric (BGP)</b>	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
<b>default-metric (OSPF)</b>	Sets default metric values for OSPF.
<b>default-metric (RIP)</b>	Sets default metric values for RIP.
<b>network (BGP)</b>	Specifies the list of networks for the BGP routing process.
<b>network (IGRP)</b>	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
<b>network (RIP)</b>	Specifies a list of networks for the RIP routing process.
<b>redistribute (IP)</b>	Redistributes routes from one routing domain into another routing domain.
<b>router eigrp</b>	Configures the IP Enhanced IGRP routing process.
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
<b>router ospf</b>	Configures an OSPF routing process.

# ip mobile authentication ignore-spi

To enable the home agent or foreign agent to accept RFC-2002 based mobile nodes or foreign agents that don't include the security parameter index (SPI) in the authentication extension of the registration message, use the **ip mobile authentication ignore-spi** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile authentication ignore-spi**

**no ip mobile authentication ignore-spi**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Global configuration.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)BY	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**Usage Guidelines** Cisco IOS software supports the Mobile-Home Authentication Extension (MHAE). All registration messages between a mobile and a home agent include a mandatory authentication extension. In RFC 2002, the SPI field was not included to calculate the authenticator value in the authentication extension of the registration message. In RFC 3220 and 3344, the SPI field in the authentication extension is used as part of the data over which the authentication algorithm must be computed. The command turns off authentication and allows an RFC-2002 based mobile node and foreign agent to register with the home agent even though the SPI field is not included in the authentication extension of the registration message. The foreign agent will accept both RFC 2002 and RFC 3220/3344 based visitors and the home agent will accept both RFC 2002 and RFC 3220/3344 based mobile nodes and foreign agents.

**Examples** The following example allows the home agent to accept registration messages without the SPI in the authentication extension:

```
ip mobile authentication ignore-spi
```

# ip mobile bindupdate

To enable a home agent to send a binding update message to a foreign agent, use the **ip mobile bindupdate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile bindupdate** [**acknowledge**] [**maximum seconds**] [**minimum seconds**] [**retry number**]

**no ip mobile bindupdate** [**acknowledge**] [**maximum seconds**] [**minimum seconds**] [**retry number**]

## Syntax Description

<b>acknowledge</b>	(Optional). Indicates that the foreign agent must acknowledge receipt of a binding update message.
<b>maximum seconds</b>	(Optional) Maximum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 10 seconds.
<b>minimum seconds</b>	(Optional) Minimum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 1 second.
<b>retry number</b>	(Optional) Number of times to retry sending the binding update message. Retransmission stops after the maximum number of retries are attempted. The range is from 1 to 4; the default retry is 4.

## Defaults

**maximum seconds**: 10 seconds  
**minimum seconds**: 1 second  
**retry number**: 4 retries

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This command enables the home agent to send a binding update message to the previous foreign agent when the mobile node moves to a new care-of address. The binding update message informs the foreign agent that a mobile node has moved and it can reclaim resources associated with that mobile node such as a visitor entry or visitor route.

Typically, resources on the foreign agent are not reclaimed until the mobility binding lifetime expires for that mobile node. By using this command, the foreign agent does not have to wait to reclaim resources used by the mobile node when that mobile node is no longer associated with the foreign agent.

Without this command configured, when a mobile node moves from foreign agent 1 to foreign agent 2 or when the home agent removes the binding, foreign agent 1 does not know that the mobile node has moved and the resources on foreign agent 1 associated with the mobile node will not be cleared until the lifetime expires for the mobile node.

If the **acknowledge** keyword is specified, the home agent periodically retransmits a binding update message until it receives a binding acknowledgement from the foreign agent or until the number of retries is exceeded.

The home agent and foreign agent must share a security association. The binding update message from the home agent and the binding update acknowledgement from the foreign agent must contain a FHAE (Foreign-Home Authentication Extension). If the FHAE is not configured on the home agent with the **ip mobile secure** command, the home agent will not send a binding update message even if the **ip mobile bindupdate** command is configured.

---

### Examples

The following example configures the home agent to wait a maximum of 8 seconds before retransmitting a binding update message to a foreign agent. The foreign agent must send an acknowledgement of this binding update message upon receipt.

```
ip mobile bindupdate acknowledge maximum 8 retry 3
ip mobile secure foreign-agent 10.31.1.1 spi 100 key hex 23456781234567812345678123456781
```

The following example configures the security association on the foreign agent. Without the security association configured on the home agent and the foreign agent, the binding update message would not be sent or processed.

```
ip mobile secure home-agent 172.31.10.1 spi 100 key hex 23456781234567812345678123456781
```

# ip mobile cdma ha-chap send attribute

To include the Mobile Equipment Identifier (MEID) in the HA-CHAP access request, use the **ip mobile cdma ha-chap send attribute** command in global configuration mode. To disable this feature, use the **no** form of the command.

**ip mobile cdma ha-chap send attribute** [A1 | A2 | A3]

**no ip mobile cdma ha-chap send attribute** [A1 | A2 | A3]

## Syntax Description

<b>A1</b>	(Optional) Send A1 (Calling Station ID) in ha-chap.
<b>A2</b>	(Optional) Send A2 (ESN) in ha-chap.
<b>A3</b>	(Optional) Send A3 (MEID) in ha-chap.

## Defaults

There are no default values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX1	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. In the interim, both attributes are 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, then the MEID value is included in the HA-CHAP access request.

## Examples

The following example illustrates the **ip mobile cdma ha-chap send attribute A3** command:

```
ip mobile cdma ha-chap send attribute A3
```

# ip mobile debug include username

To display the username or International Mobile Subscriber Identity (IMSI) condition with each debug statement, use the **ip mobile debug include username** command. To remove the username or IMSI condition from the debug display, use the **no** form of the command.

**ip mobile debug include username**

**no ip mobile debug include username**

---

**Syntax Description**

This command has no arguments or keywords.

---

**Command Default**

The user name or IMSI condition is not displayed in the debug output.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

---

**Usage Guidelines**

In the following example, the user name or IMSI condition will be displayed in any Mobile IP debug output:

```
Router(config)# ip mobile debug include username
```

# ip mobile foreign-agent

To enable foreign agent service, use the **ip mobile foreign-agent** command in global configuration mode. To disable this service, use the **no** form of this command.

```
ip mobile foreign-agent [care-of interface {interface-only} [transmit-only] | reg-wait seconds | local-timezone | reverse-tunnel private-address }
```

```
no ip mobile foreign-agent {care-of interface [interface-only] [transmit-only] | reg-wait | local-timezone | reverse-tunnel private-address }
```

## Syntax Description

<b>care-of</b> <i>interface</i>	IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured. At least one care-of address must be configured for foreign agent service.
<b>interface-only</b>	(Optional) Enables the specified interface to advertise only its own address as the care-of address. Other interfaces configured for foreign agent service will not advertise this care-of address.
<b>transmit-only</b>	(Optional) Informs Mobile IP that the <i>interface</i> is being used on a unidirectional link and will transmit only. This interface will be used as the source interface for this care-of address for any registration request received on another interface. Only serial interfaces can be configured as transmit only.
<b>reg-wait</b> <i>seconds</i>	(Optional) Pending registration expires after <i>the specified number of seconds</i> if no reply is received. Range is from 5 to 600 seconds. Default is 15.
<b>local-timezone</b>	(Optional) Uses the local time zone to generate identification fields.
<b>reverse-tunnel private-address</b>	(Optional) Forces a mobile node with a private address to register with reverse tunneling.

## Defaults

**reg-wait** *seconds*: 15

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	The <b>interface-only</b> , <b>transmit-only</b> , and <b>reverse-tunnel private-address</b> keywords were added.
12.2(3)XC	The <b>local-timezone</b> keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

## Usage Guidelines

This command enables foreign agent service when at least one care-of address is configured. When no care-of address exists, foreign agent service is disabled.

The foreign agent is responsible for relaying the registration request to the home agent, setting up a tunnel to the home agent, and forwarding packets to the mobile node. The **show** commands used to display relevant information are shown in parentheses in the following paragraph.

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on an interface or when no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated. The registration bitflag is handled as described in [Table 1](#). The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending** command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in [Table 2](#)). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command).

When a registration reply comes in, the home agent is authenticated (**show ip mobile secure home-agent** command) if a security association exists for the home agent (IP source address or home agent address in reply). The reply is relayed to the mobile node.

When registration is accepted, the foreign agent creates or updates the visitor table, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the mobile node via the interface (of the incoming request) is added to the routing table (**show ip route mobile** command), and an ARP entry is added to avoid the sending of ARP requests for the visiting mobile node. Visitor binding is removed (along with its associated host route, tunnel, and ARP entry) when the registration lifetime expires or deregistration is accepted.

When registration is denied, the foreign agent will remove the request from the pending registration table. The table and timers of the visitor will be unaffected.

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent deencapsulates the packet and forwards it out its interface to the visiting mobile node, without sending ARP requests.

The care-of address must be advertised by the foreign agent. This address is used by the mobile node to register with the home agent. The foreign agent and home agent use this address as the source and destination point of tunnel, respectively. The foreign agent is not enabled until at least one care-of address is available. The foreign agent will advertise on interfaces configured with the **ip mobile foreign-service** command.

Only care-of addresses with interfaces that are up are considered available.

The **interface-only** and **transmit-only** keywords are used in an asymmetric link environment, such as satellite communications, where separate uplinks and downlinks exist. The **ip mobile foreign-agent care-of interface interface-only** command enables the specified interface to advertise only its own address as the care-of address. All other care-of addresses are not advertised. Other foreign agent interfaces configured for foreign-service will not advertise interface-only care-of addresses. The **ip mobile foreign-agent care-of interface transmit-only** command informs Mobile IP that the interface acts as an uplink. Registration requests and replies received for this care-of address are treated as transmit-only. This interface will not hear any solicitations. Any care-of address can be configured with the **interface-only** keyword, but only serial interfaces can be configured with the **transmit-only** keyword.

Use the **reverse-tunnel private-address** keywords to force a mobile node with a private address to register with reverse tunnel. Private addresses are IP addresses in the following ranges:

- 10.0.0.0 to 10.255.255.255 (10/8 prefix)
- 172.16.0.0 to 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Table 1 lists mobile node registration request service bitflags.

**Table 1** *Mobile Node Registration Request Service Bitflags*

Bit Set	Registration Request
S	No operation. Not applicable to foreign agent.
B	No operation. Not applicable to foreign agent.
D	Make sure source IP address belongs to the network of the interface.
M	Deny request. Minimum IP encapsulation is not supported.
G	No operation. GRE encapsulation is supported.
r	Sent as zero; ignored on reception. Do not allocate for any other uses.
V	Reserved.
T	Deny if reverse tunneling is disabled on the foreign agent.
reserved	Deny request. Reserved bit must not be set.

Table 2 lists foreign agent reply codes.

**Table 2** *Foreign Agent Reply Codes*

Code	Reason
64	Reason unspecified.
65	Administratively prohibited.
66	Insufficient resource.
67	Mobile node failed authentication.
68	Home agent failed authentication.
69	Requested lifetime is too long.
70	Poorly formed request.
71	Poorly formed reply.
72	Requested encapsulation is unavailable.
74	Reverse tunnel unsupported.
75	Reverse tunnel is mandatory and T bit is not set.
76	Mobile node too distant.
77	Invalid care-of address.
78	Registration timeout.
79	Delivery style not supported.
80	Home network unreachable (ICMP error received).
81	Home agent host unreachable (ICMP error received).
82	Home agent port unreachable (ICMP error received).
88	Home agent unreachable (other ICMP error received).
98	Missing home agent.
99	Missing home agent address.

**Table 2** Foreign Agent Reply Codes (continued)

Code	Reason
100	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the mobile node to the foreign agent.
101	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the home agent to the foreign agent.
104	Unknown challenge.
105	Missing challenge.
106	Stale challenge.

**Examples**

The following example enables foreign agent service on Ethernet interface 1, advertising 10.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

The following example enables foreign agent service on serial interface 4, advertising 10.0.0.2 as the only care-of address. The uplink interface is configured as a transmit-only interface.

```
ip mobile foreign-agent care-of Serial4 interface-only transmit-only
interface Serial4
 ! Uplink interface
 ip address 10.0.0.2 255.255.255.0
 ip irdp
 !
 ip mobile foreign-service
 !
```

**Related Commands**

Command	Description
<b>debug ip mobile advertise</b>	Displays advertisement information.
<b>ip mobile foreign-service</b>	Enables foreign agent service on an interface if care-of addresses are configured.
<b>show ip mobile globals</b>	Displays global information for mobile agents.
<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
<b>show ip mobile secure</b>	Displays mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.
<b>show ip mobile violation</b>	Displays information about security violations.
<b>show ip mobile visitor</b>	Displays the table containing the visitor list of the foreign agent.
<b>show ip route mobile</b>	Displays the current state of the routing table for mobile routes.

# ip mobile foreign-agent inject-mobile-networks

To enable direct routing to mobile networks via the foreign agent, use the **ip mobile foreign-agent inject-mobile-networks** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile foreign-agent inject-mobile-networks** [**mobnetacl** *access-list-identifier*]

**no ip mobile foreign-agent inject-mobile-networks** [**mobnetacl** *access-list-identifier*]

Syntax Description	Parameter	Description
	<b>mobnetacl</b>	(Optional) Specifies that the foreign agent can provide direct routing for only the mobile networks covered by the specified access list.
	<i>access-list-identifier</i>	(Optional) Name of an access list defined using the <b>ip access-list</b> command or number of an access list defined using the <b>access-list</b> command.

**Defaults** Direct routing via the foreign agent is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.

**Usage Guidelines** Configure the **ip mobile foreign-agent inject-mobile-networks** command on the foreign agent to enable direct routing.

The value entered for the *access-list-identifier* argument must match the name of an access list defined using the **ip access-list** command or the number of an access list defined using the **access-list** command.

**Examples** The following example configures the access list named mobile-net-list and enables direct routing via the foreign agent for mobile networks specified on that access list.

```
ip access-list standard mobile-net-list
 permit any
!
ip mobile foreign-agent inject-mobile-networks mobnetacl mobile-net-list
```

Related Commands	Command	Description
	<b>access-list (IP standard)</b>	Defines a standard IP access list.
	<b>ip access-list</b>	Defines an IP access list by name.
	<b>show ip mobile globals</b>	Displays global information for mobile agents.

# ip mobile foreign-agent nat traversal

To enable NAT traversal support for Mobile IP (MIP) foreign agents (FAs), use the **ip mobile foreign-agent nat traversal** command in global configuration mode. To disable NAT traversal support, use the **no** form of this command.

**ip mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**]

**no ip mobile foreign-agent nat traversal** [**keepalive** *keepalive-time*] [**force**]

## Syntax Description

<b>keepalive</b> <i>keepalive-time</i>	(Optional) Allows the FA to use a configured time for keepalive messages when the home agent (HA) keepalive time was not configured. The range is 0 to 65535 seconds. Default is 110 seconds.
<b>force</b>	(Optional) Allows the FA to force the HA to allocate a User Datagram Protocol (UDP) tunnel. The <b>force</b> keyword only sets the “force” bit in the message extension. The default is <i>not</i> to force UDP tunneling.

## Defaults

Network Address Translation (NAT) traversal support for FAs is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4T	The <b>keepalive</b> <i>keepalive-time</i> range changed.

## Usage Guidelines

You need to enable this command under the following circumstances:

- If you have a NAT box in your network.
- If you have a NAT box in your network, and you are using a private IP address for the care-of address (CoA) or source IP address in the registration request.

A likely scenario for using this command and when to set the force bit is when there is a firewall between an FA and HA. The firewall blocks IP-in-IP and GRE packets but permits UDP packets.

## Examples

The following example shows a FA configuration with a keepalive time of 45 and forced UDP tunneling.

```
ip mobile foreign-agent care-of Ethernet2/2
ip mobile foreign-agent nat traversal keepalive 45 force
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ip mobile</b>	Displays IP mobility activities.
<b>ip mobile home-agent nat traversal</b>	Enables NAT UDP traversal support for MIP HAs.
<b>show ip mobile bindings</b>	Displays the mobility binding table.
<b>show ip mobile globals</b>	Displays global information about MIP HAs, FAs, and MNs.
<b>show ip mobile visitor</b>	Displays information about UDP tunneling.
<b>show ip mobile tunnel</b>	Displays the table that contains a visitor list of FAs.

# ip mobile foreign-agent skip-aaa-reauthentication

To enable FA-CHAP during Mobile IP registration, and then to skip it in all subsequent re-registrations, use the **ip mobile foreign-agent skip-aaa-reauthentication** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
ip mobile foreign-agent skip-aaa-reauthentication
```

```
no ip mobile foreign-agent skip-aaa-reauthentication
```

## Syntax Description

There are no keywords or arguments for this command.

## Defaults

Disabled

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(11)T	This command was introduced.

## Usage Guidelines

FA-CHAP is a mechanism for authentication in Mobile IP. As per IS835, FA-CHAP is mandatory during Mobile IP call setup (registration), and requires access to a AAA server. A Mobile IP call has a parameter lifetime, so in order to continue a Mobile IP call, re-registration is required before the lifetime expires, and this re-registration leads to extending of lifetime.

Because FA-CHAP is mandatory, and the call is authenticated during registration, it may be undesirable to access AAA during re-registration of the Mobile IP call. The **ip mobile foreign-agent skip-aaa-reauthentication** command provides flexibility in this scenario.

When this command is configured, FA-CHAP is performed during Mobile IP registration, and is skipped in all subsequent re-registrations.

The default value is “false”, implying that AAA access is not skipped during Mobile IP re-registration.

## Examples

The following example shows that FA-CHAP is enabled during Mobile IP registration, but disabled for all subsequent re-registrations:

```
ip mobile foreign-agent skip-aaa-reauthentication
```

# ip mobile foreign-service

To enable foreign agent service on if care-of addresses are configured, use the **ip mobile foreign-service** command in interface or global configuration mode. To disable this service, use the **no** form of this command.

**ip mobile foreign-service** [**challenge** [**forward-mfce**] [**timeout** *value*] [**window** *number*] | [**home-access** *access-list*] [**limit** *number*] [**registration-required**] [**reverse-tunnel**] [**mandatory**]]

**no ip mobile foreign-service** [**challenge** [**forward-mfce**] [**timeout** *value*] [**window** *number*] | [**home-access** *access-list* | **limit** *number* | **registration-required** | **reverse-tunnel**]

Syntax Description	
<b>challenge</b>	(Optional) Configures the foreign agent challenge parameters. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>forward-mfce</b>	(Optional) Enables the foreign agent to forward mobile foreign challenge extensions (MFCEs) and mobile node-AAA extensions to the home agent.
<b>timeout</b> <i>value</i>	(Optional) Challenge timeout in seconds. Possible values are from 1 to 10.
<b>window</b> <i>number</i>	(Optional) Maximum number of valid challenge values to maintain. Possible values are from 1 to 10. The default is 2.
<b>home-access</b> <i>access-list</i>	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>limit</b> <i>number</i>	(Optional) Number of visitors allowed on the interface. The Busy (B) bit will be advertised when the number of registered visitors reaches this limit. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>registration-required</b>	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
<b>reverse-tunnel</b> [ <b>mandatory</b> ]	(Optional) Enables reverse tunneling on the foreign agent. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

## Defaults

Foreign agent service is not enabled.

There is no limit to the number of visitors allowed on an interface.

**window** *number*: 2

Foreign agent reverse tunneling is not enabled. When foreign agent reverse tunneling is enabled, it is not mandatory by default.

## Command Modes

Interface and global configuration

**Command History**

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)XS	The <b>challenge</b> keyword and associated parameters were added.
12.2(2)XC	The <b>reverse-tunnel [mandatory]</b> keywords were added.
12.2(13)T	The <b>challenge</b> keyword and associated parameters and the <b>reverse-tunnel [mandatory]</b> keywords were integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	Global configuration mode was added.

**Usage Guidelines**

This command enables foreign agent service on the interface or all interfaces (global configuration). The foreign agent (F) bit will be set in the agent advertisement, which is appended to the IRDP router advertisement whenever the foreign agent or home agent service is enabled on the interface.

**Note**

The Registration-required bit only tells the visiting mobile node to register even if the visiting mobile node is using a colocated care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from the interface of this foreign agent.

When you use the **reverse-tunnel** keyword to enable foreign agent reverse tunneling on an interface, the reverse tunneling support (T) bit is set in the agent advertisement.

Cisco Express Forwarding (CEF) switching is currently not supported on a foreign agent when reverse tunneling is enabled. If reverse tunneling is enabled at the foreign agent, disable CEF on the foreign agent, using the **no ip cef** global configuration command. If the foreign agent does not support reverse tunneling, then there is no need to disable CEF at the global configuration level.

[Table 3](#) lists the advertised bitflags.

**Table 3 Foreign Agent Advertisement Bitflags**

Bit Set	Service Advertisement
T	Set if the <b>reverse-tunnel</b> parameter is enabled.
R	Set if the <b>registration-required</b> parameter is enabled.
B	Set if the number of visitors reached the <b>limit</b> parameter.
H	Set if the interface is the home link to the mobile host (group).
F	Set if foreign-agent service is enabled.
M	Never set.
G	Always set.
V	Reserved.
reserved	Never set.

**Examples**

The following example shows how to enable foreign agent service for up to 100 visitors:

```
interface Ethernet 0
 ip mobile foreign-service limit 100 registration-required
```

The following example shows how to enable foreign agent reverse tunneling:

```
interface ethernet 0
 ip mobile foreign-service reverse-tunnel
```

The following example shows how to configure foreign agent challenge parameters:

```
interface ethernet 0
 ip mobile foreign-service challenge window 2
```

**Related Commands**

Command	Description
<b>ip cef</b>	Enables CEF on the RP card.
<b>ip mobile tunnel</b>	Specifies the settings of tunnels created by Mobile IP.
<b>show ip mobile interface</b>	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

# ip mobile home-agent

To enable and control home agent (HA) services, use the **ip mobile home-agent** command in global configuration mode. To disable these services, use the **no** form of this command.

**ip mobile home-agent** [**address** *ip-address*] [**broadcast**] [**care-of-access** *access-list*] [**lifetime** *seconds*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel** { **off** | **private-address** }] [**roam-access** *access-list*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown-ha** [**accept** | **reply**] | **deny**]] [**send-mn-address**]

**no ip mobile home-agent** [**address** *ip-address*] [**broadcast**] [**care-of-access** *access-list*] [**lifetime** *seconds*] [**nat-detect**] [**replay** *seconds*] [**reverse-tunnel** { **off** | **private-address** }] [**roam-access** *access-list*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown-ha** [**accept** | **reply**] | **deny**]] [**send-mn-address**]

## Syntax Description

<b>address</b> <i>ip-address</i>	(Optional) Specifies the IP address of the HA.  <b>Note</b> This option is only applicable when HA redundancy is used for virtual networks.
<b>broadcast</b>	(Optional) Enables forwarding of broadcast datagrams to the mobile node (MN). By default, broadcasting is disabled.
<b>care-of-access</b> <i>access-list</i>	(Optional) Controls which care-of addresses (CoAs) in registration requests are permitted by the HA. By default, all CoAs are permitted. The <i>access-list</i> argument can be a string or number from 1 to 99.
<b>lifetime</b> <i>seconds</i>	(Optional) Specifies the global registration lifetime for an MN in seconds. Range is from 3 to 65535 (infinity). Default is 36000 (10 hours).  <b>Note</b> This configuration can be overridden by the individual MN configuration. Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
<b>nat-detect</b>	(Optional) Allows the HA to detect registration requests from a MN traversing a Network Address Translation (NAT)-enabled device and apply a tunnel to reach the MN. By default, NAT detection is disabled.
<b>replay</b> <i>seconds</i>	(Optional) Sets the replay protection time-stamp value in seconds. A registration received within the router clock time plus or minus 7 is valid.
<b>reverse-tunnel</b> { <b>off</b>   <b>private-address</b> }	(Optional) Enables support of reverse tunnel by the HA. By default, reverse tunnel support is enabled. The keywords are as follows: <ul style="list-style-type: none"> <li><b>off</b>—Disables support of reverse tunnel.</li> <li><b>private-address</b>—Reverse tunnel mandatory for private Mobile IP addresses.</li> </ul>
<b>roam-access</b> <i>access-list</i>	(Optional) Controls which MNs are permitted or denied to roam. By default, all specified MNs can roam.
<b>strip-realm</b>	(Optional) Strips the realm part of the Network access identifier (NAI) before authentication is performed. This option is useful if the majority of MNs have the identical realm, for example, in the case of enterprise networks.
<b>suppress-unreachable</b>	(Optional) Disables sending Internet Control Message Protocol (ICMP) unreachable messages to the source when an MN on the virtual network is not registered. By default, ICMP unreachable messages are sent.

<b>local-timezone</b>	(Optional) Uses the local time zone to generate identification fields.
<b>unknown-ha [accept [reply]   deny]</b>	<p>Accepts or denies an unknown HA registration request. The keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>—(Optional) HA accepts the registration request with an HA address different from the IP destination of the registration request. The HA address set in the registration reply is that of the IP destination address.</li> <li>• <b>reply</b>—(Optional) HA uses the received HA address in reply.</li> <li>• <b>deny</b>—(Optional) HA denies the registration request with an HA address different from the IP destination of the registration request with error code Unknown HomeAgent. The HA address set in the reject registration reply is that of the IP destination address.</li> </ul> <p><b>Note</b> This command option can be used in a testing environment when the home agent is in private addressing space behind a NAT gateway.</p>
<b>send-mn-address</b>	<p>Sends the home address as received in the registration request and in the access request messages for the HA Challenge Handshake Authentication Protocol (CHAP).</p> <p><b>Note</b> You must configure this keyword in the HA to send <b>radius-server vsa send authentication 3gpp2</b> attributes. This keyword is available only on PDSN platforms running specific PDSN code images.</p>

**Defaults**

The command is disabled. Broadcasting is disabled. Reverse tunnel support is enabled. ICMP unreachable messages are sent. NAT detection is disabled.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>strip-nai-realm</b> and <b>local-timezone</b> keywords were added.
12.2(13)T	The <b>nat-detect</b> keyword was added.
12.3(4)T	The <b>unknown-ha</b> , <b>accept</b> , <b>reply</b> , <b>deny</b> and <b>send-mn-address</b> keywords were added.

**Usage Guidelines**

This command enables and controls HA services on a router. Changes to service take effect immediately; however, broadcast and lifetime settings for previously registered MNs are unaffected. Tunnels are shared by MNs registered with the same endpoints, so the **reverse-tunnel-off** keyword also affects registered MNs.

The HA processes registration requests from the MN and sets up tunnels and routes to the CoA. Packets to the MN are forwarded to the visited network.

The HA will forward broadcast packets to MNs if the MNs are registered with the service. However, heavy broadcast traffic uses the CPU of the router.

The HA can control where the MNs roam by the **care-of-access** keyword, and which MN is allowed to roam by the **roam-access** keyword.

When a registration request comes in, the HA ignores requests when HA service is not enabled or the security association of the MN is not configured. The latter condition occurs because the security association must be available for the MH authentication extension in the reply. If a security association exists for the FA (IP source address or CoA in the request), the FA is authenticated, and then the MN is authenticated. The Identification field is verified to protect against replay attack. The HA checks the validity of the request (see [Table 4](#)) and sends a reply. (Reply codes are listed in [Table 5](#).) A security violation is logged when FA authentication, MH authentication, or identification verification fails. (The violation reasons are listed in [Table 6](#).)

After registration is accepted, the HA creates or updates the mobility binding of the MN, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the MN via the care-of address is added to the routing table, and gratuitous ARPs are sent out. For deregistration, the host route is removed from the routing table, the virtual tunnel interface is removed (if no MNs are using it), and gratuitous ARP messages are sent out if the MN is back home. Mobility binding is removed (along with its associated host route and tunnel) when registration lifetime expires or deregistration is accepted.

By default, the HA uses the entire NAI string as the username for authentication (which may be with local security association or retrieved from the AAA server). The **strip-nai-realm** keyword instructs the HA to strip off the realm part of NAI (if it exists) before performing authentication. Basically, the MN is identified by only the user name part of the NAI. This option is useful if the majority of MNs belong to the same realm, for example, in the case of enterprise networks.

When the packet destined for the MN arrives on the HA, the HA encapsulates the packet and tunnels it to the care-of address. If the Don't Fragment (DF) bit is set in the packet via the **ip mobile tunnel path-mtu-discovery** global configuration command, the HA will copy the DF bit from the original packet to the new tunnel IP header. This allows the path MTU discovery to set the MTU of the tunnel. Subsequent packets greater than the MTU of the tunnel will be dropped and an ICMP datagram too big message will be sent to the source (correspondent node). If the HA loses the route to the tunnel endpoint, the host route to the MN will be removed from the routing table until the tunnel route is available. Packets destined for the MN without a host route will be sent out the interface (home network) or to the virtual network (see the description of the **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the HA will send a copy to all MNs registered with the broadcast routing option.

Some companies block ICMP datagram too big messages. If the message does not reach the original correspondent node sending the packet, the correspondent node will simply resend the same size packet. To work around this problem, turn off Path MTU Discovery with the **no ip mobile tunnel path-mtu-discovery** command. The DF bit will not be copied from the original packet and the tunnel packet can be fragmented.

The **ip mobile home-agent nat-detect** option is supported for MNs using a collocated care-of address and registering through the FA. The MN will use the NAT inside address as the collocated care-of address used in its registration requests. If a MN is using a FA CoA address, the MN can be detected behind a NAT gateway.

The **ip mobile home-agent unknown-ha** option can be useful in a testing environment when the HA is using a private address behind a NAT gateway. A MN would need to access the HA through the NAT box while it is on a public network domain. However, NAT will translate the destination IP address of the registration request to the private address of the HA. When the HA checks the HA field in the registration request, it does not match one of the interfaces. The packet can not be processed properly and the tunnels are not set up properly. The **ip mobile home-agent unknown-ha** command allows the HA to accept the unknown (translated) address and process the registration request.

The **send-mn-address** keyword is available only on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

The MN requests services from the HA by setting bits in the registration request. [Table 4](#) shows the services the MN can request.

**Table 4** HA Registration Bitflags

Bit Set	Definition
S	Accept with code 1 (no simultaneous binding).
B	Accept. Broadcast can be enabled or disabled.
D	Accept. Tunnel endpoint is a colocated care-of address.
M	Deny. Minimum IP encapsulation is not supported.
G	Accept. GRE encapsulation is supported.
V	Deny if this bit is set.
T	Accept if the <b>reverse-tunnel-off</b> parameter is not set.
reserved	Deny. Reserved bit must not be set.

[Table 5](#) lists the HA registration reply codes. The codes tell the MN whether the registration was accepted or denied. If registration is denied, the reply code gives the reason.

**Table 5** HA Registration Reply Codes

Code	Reason
0	Accept.
1	Accept. No simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	MN failed authentication.
132	FA failed authentication.
133	Registration identification mismatched (timestamp is off).
134	Poorly formed request.
136	Unknown HA address.
137	Reverse tunnel is unavailable.
138	Reverse tunnel is mandatory and T bit not set.
139	Unsupported encapsulation.
140	Unsupported vendor id or unable to interpret registration request extensions sent by the MN to the home agent.
141	Unsupported vendor id or unable to interpret registration request extensions sent by the FA to the home agent.
142	Active home agent failed authentication.

[Table 6](#) lists security violation codes.

**Table 6**      **Security Violation Codes**

Code	Reason
1	No mobility security association.
2	Bad authenticator.
3	Bad identifier.
4	Bad SPI.
5	Missing security extension.
6	Other.
7	Stale request.

**Examples**

The following example enables broadcast routing and specifies a global registration lifetime of 7200 seconds (2 hours):

```
ip mobile home-agent broadcast lifetime 7200
```

**Related Commands**

Command	Description
<b>ip mobile tunnel</b>	Specifies the setting of tunnels created by Mobile IP.
<b>show ip mobile binding</b>	Displays the mobility binding table.
<b>show ip mobile globals</b>	Displays global information for mobile agents.

# ip mobile home-agent aaa user-password

To configure an authentication password for the downloading of security associations from a AAA server, use the **ip mobile home-agent aaa user-password** command in global configuration mode. To remove the password requirement, use the **no** form of this command.

**ip mobile home-agent aaa user-password** {0 *password* | 7 *encrypted-password* | *password*}

**no ip mobile home-agent aaa user-password**

## Syntax Description

<b>0</b>	Specifies that an unencrypted password will follow.
<i>password</i>	The unencrypted (cleartext) password.
<b>7</b>	Specifies that an encrypted password will follow.
<i>encrypted-password</i>	The encrypted password.
<i>password</i>	The unencrypted (cleartext) password.

## Defaults

The default password is cisco.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3	This command was introduced.

## Usage Guidelines

When a mobile node sends a registration request packet to the home agent, Mobile IP requires a security association for registration authentication. Security associations for a mobile node can be configured on the home agent or retrieved by the home agent from a AAA server.

If security associations are retrieved from a AAA server, the AAA access-request packets used to retrieve the security associations require a challenge and response. If the registration request of the mobile node does not contain a challenge and response, the home agent auto-generates a challenge and creates a response using the default password “cisco” unless you specify a different password using the **ip mobile home-agent aaa user-password** command. In either case, a single password is used for all mobile nodes.

The AAA server will read the challenge in the access-request packet of the mobile node, and using the password of the mobile node that is stored on the AAA server, create the response to the challenge. It then authenticates the mobile node, identified by its IP address (or network access identifier), by comparing the two responses to ensure they are identical. For this reason, the password configured by the **ip mobile home-agent aaa user-password** command must match the user password in the user profile on the AAA server.

Mobile nodes that include a challenge and response in their registration request, such as in the case of dynamic security association and key distribution, do not use the defined password. Instead, the home agent copies the challenge/response from the registration request into the AAA access-request packet. Thus, a mobile node in this scenario can have a “unique” password.

You can enable or disable password encryption with the **service password-encryption** command. If this command is enabled, even if the **ip mobile home-agent aaa user-password 0** password is used, the password will be encrypted.

---

**Examples**

The following example enables the encrypted password “\$1\$i5Rkls3L0yxzS8t9” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password 7 $1$i5Rkls3L0yxzS8t9
```

The following example enables the unencrypted password “pswd2” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password 0 pswd2
```

The following example enables the unencrypted password “pswdmobile” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password pswdmobile
```

---

**Related Commands**

Command	Description
<b>service password-encryption</b>	Encrypts passwords.

# ip mobile home-agent accounting

To enable home agent accounting services on the router, use the **ip mobile home-agent accounting** command in global configuration mode. To disable these services, use the **no** form of this command.

**ip mobile home-agent accounting** { **default** | *list-name* }

**no ip mobile home-agent accounting** { **default** | *list-name* }

Syntax Description	default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
	<i>list-name</i>	Character string used to name the list of at least one of the accounting methods.

**Defaults** The command is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

**Usage Guidelines** This command enables and controls home agent accounting services on the router. First, use the **aaa accounting** global configuration command to define the accounting method list. Next, apply the same accounting method list on the home agent using the **ip mobile home-agent accounting** global configuration command.

**Examples** The following example enables home agent accounting for the list named mobile-list:

```
ip mobile home-agent accounting mobile-list
```

Related Commands	Command	Description
	<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes.

# ip mobile home-agent dynamic-address

To set the home agent address field in a Registration Response packet, use the **ip mobile home-agent dynamic-address** command in global configuration. To disable this functionality, or to reset the field use the **no** form of this command.

```
ip mobile home-agent dynamic-address ip-address
```

```
no ip mobile home-agent dynamic-address ip-address
```

---

**Syntax Description**

<i>ip-address</i>	The IP address of the Home Agent.
-------------------	-----------------------------------

---

---

**Defaults**

The Home Agent Address field will be set to the values specified by the *ip-address* argument.

---

**Command Modes**

Global configuration

---

**Command History**

Release	Modification
12.3(11)YF	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

---

---

**Examples**

In the following example, the dynamic home-agent address is set to 10.1.1.1:

```
Router(config)# ip mobile home-agent dynamic-address 10.1.1.1
```

# ip mobile home-agent multi-path

To enable the home agent to process registration requests with multiple path support for all mobile routers, use the **ip mobile home-agent multi-path** command in global configuration mode. To disable multipath support on the home agent, use the **no** form of this command.

```
ip mobile home-agent multi-path [metric {bandwidth | hopcount}]
```

```
no ip mobile home-agent multi-path [metric {bandwidth | hopcount}]
```

## Related Commands

<b>metric</b>	(Optional) Metric for multipath load balancing.
<b>bandwidth</b>	(Optional ) Specifies that bandwidth is used as the metric. Bandwidth is the default metric.
<b>hopcount</b>	(Optional) Specifies that hop count is used as the metric.

## Command Default

Multiple path support is enabled by default on the mobile router.

## Command Modes

Global configuration.

## Command History

Release	Modification
12.4(9)T	This command was introduced.

## Usage Guidelines

Multiple path support is enabled by default on the mobile router but disabled by default on the home agent. The **multi-path** command in mobile networks configuration mode overrides the global setting.

## Examples

The following example shows how to configure the home agent to globally process registration requests for all mobile routers:

```
!
router mobile
exit
ip mobile home-agent multi-path
```

## Related Commands

Command	Description
<b>multi-path (mobile networks)</b>	Overrides the global default setting and enables the home agent to process requests with multiple path support for a specific mobile router.
<b>multi-path (mobile router)</b>	Enables the mobile router to request multiple path support.

# ip mobile home-agent nat traversal

To enable NAT traversal support for Mobile IP home agents (HAs), use the **ip mobile home-agent nat traversal** command in global configuration mode. To disable Network Address Translation (NAT) traversal support for Mobile IP for the HA, use the **no** form of this command.

```
ip mobile home-agent nat traversal [keepalive keepalive-time] [forced {accept | reject}]
```

```
no ip mobile home-agent nat traversal [keepalive keepalive-time] [forced {accept | reject}]
```

## Syntax Description

<b>keepalive</b> <i>keepalive-time</i>	(Optional) Configures the keepalive interval in seconds the HA uses in registration replies. When the HA replies with a keepalive interval other than zero, it forces the FA or MN to use this interval. If it replies with an interval of zero, the FA or MN should use its default configured interval. The range is 0 to 65535 seconds. The default is 110 seconds.
<b>forced</b>	(Optional) Enables the HA to accept or reject forced UDP tunneling from the mobile node (MN) regardless of the NAT-detection outcome. <ul style="list-style-type: none"> <li><b>accept</b>—Accepts UDP tunneling.</li> <li><b>reject</b>—Rejects UDP tunneling.</li> </ul> <p><b>Note</b> If the <b>forced</b> keyword is not specified, the command defaults to rejecting registration requests where the “force” bit is set in the UDP tunnel extension. MN registration attempts will fail until the MN retries without the “forced” bit set in the UDP tunnel extension. The registration will fail until the MN retries the registration.</p>

## Defaults

NAT traversal support for Mobile IP is disabled for the HA.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4T	the <b>keepalive</b> <i>keepalive-time</i> range changed.

## Usage Guidelines

Enable this command if your MNs will roam behind a NAT-enabled router or firewall.

## Examples

The following example shows an HA configured with a keepalive timer set to 56 seconds and forced to accept UDP tunneling.

```
ip mobile home-agent nat traversal 56 forced accept
ip mobile home-agent replay 255
ip mobile home-agent redundancy Phyl virtual-network
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug ip mobile</b>	Displays IP mobility activities.
<b>ip mobile foreign-agent nat traversal</b>	Enables NAT UDP traversal support for MIP FAs.
<b>show ip mobile binding</b>	Displays the mobility binding table.
<b>show ip mobile globals</b>	Displays global information about MIP HAs, FAs, and MNs.
<b>show ip mobile tunnel</b>	Displays information about UDP tunneling.
<b>show ip mobile visitor</b>	Displays the table that contains a visitor list of FAs.

## ip mobile home-agent redundancy

To configure the home agent for redundancy by using the Hot Standby Router Protocol (HSRP) group name, use the **ip mobile home-agent redundancy** command in global configuration mode. To remove the address, use the **no** form of this command.

```
ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address] [mode active-standby] [swact-notification]
```

```
no ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address] [mode active-standby] [swact-notification]
```

### Syntax Description

<i>hsrp-group-name</i>	Specifies the HSRP group name.
<b>virtual-network</b>	(Optional) Specifies that the HSRP group is used to support virtual networks.
<b>address</b> <i>address</i>	(Optional) Home agent address.
<b>mode active-standby</b>	(Optional) Allows the bindings to come up (with local pool addressing for virtual-networks) with the home agent IP address specified under the loopback interface.
<b>swact-notification</b>	(Optional) Notifies the RADIUS server of a home agent failover.

### Defaults

No global home agent addresses are specified.

### Command Modes

Global configuration

### Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(8)T	The command changed from <b>ip mobile home-agent standby</b> to <b>ip mobile home-agent redundancy</b> .
12.4(11)T	The <b>mode active-standby</b> and <b>swact-notification</b> keywords were added.

### Usage Guidelines

The **virtual-network** keyword specifies that the HSRP group supports virtual networks.



#### Note

Redundant home agents must have identical Mobile IP configurations. You can use a standby group to provide HA redundancy for either physical or virtual networks, but not both at the same time.

When Mobile IP standby is configured, the home agent can request mobility bindings from the peer home agent. When Mobile IP standby is deconfigured, the home agent can remove mobility bindings. Operation of home agent redundancy on physical and virtual networks is described as follows:

- **Physical network**—Only the active home agent will receive registrations on a physical network. It updates the standby home agent. The standby home agent requests the mobility binding table from the active home agent. When Mobile IP standby is deconfigured, the standby home agent removes all bindings, but the active home agent keeps all bindings.
- **Virtual network**—Both active and standby home agents receive registrations if the loopback interface is used; each will update the peer after accepting a registration. Otherwise, the active home agent receives registrations. Both active and standby home agents request mobility binding tables from each other. When Mobile IP standby is deconfigured, the standby or active home agent removes all bindings.

**Note**

The **swact-notification** option notifies the RADIUS server of a home agent failover. This is achieved by including the `cisco-avpair radius attribute "mobileip-rfswat=1"` in RADIUS accounting records. This attribute is included only in the first accounting record of a binding generated after a failover, and if that binding was created before the failover.

**Examples**

The following example specifies an HSRP group named SanJoseHA:

```
ip mobile home-agent redundancy SanJoseHA
```

**Related Commands**

Command	Description
<b>show ip mobile globals</b>	Displays global information for mobile agents.

# ip mobile home-agent redundancy periodic-sync

To synchronize the byte and packet counters for each binding to the standby unit using an accounting update event, use the **ip mobile home-agent redundancy periodic-sync** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address]
periodic-sync
```

```
no ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address]
periodic-sync
```

## Syntax Description

<i>hsrp-group-name</i>	The HSRP group name.
<b>virtual-network</b>	(Optional) Specifies that the HSRP group is used to support virtual networks.
<b>address</b> <i>address</i>	(Optional) Home agent address.

## Defaults

There are no default values for this command.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Usage Guidelines

The byte and packet counters for each binding are synchronized to the standby unit using an accounting update event only if the byte counts have changed since the last synchronization.

## Examples

In the following example, the byte and packet counters for each binding will be periodically synchronized between the active and standby unit:

```
Router(config)# ip mobile home-agent redundancy group1 periodic-sync
```

# ip mobile home-agent reject-static-addr

To configure the HA to reject Registration Requests from MNs under certain conditions, use the **ip mobile home-agent reject-static-addr** sub-command under the **ip mobile home-agent** global configuration command.

**ip mobile home-agent reject-static-addr**

**Syntax Description** This command has not arguments or keywords

**Command Modes** Subcommand of the **ip mobile home-agent** global configuration command.

Command History	Release	Modification
	12.2(8)BY	This command was introduced.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

**Usage Guidelines** You must first configure the **ip mobile home-agent** command to use this sub-command.

If an MN that has a binding to the HA with a static address tries to register with the same static address again, then the HA rejects the second RRQ from the MN.

**Examples** The following example illustrates the **ip mobile home-agent reject-static-addr** command:

```
Router(config)# ip mobile home-agent reject-static-addr
```

## ip mobile home-agent resync-sa

To configure the home agent to clear out the old cached security associations and requery the AAA server for a new security association when the mobile node fails authentication, use the **ip mobile home-agent resync-sa** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip mobile home-agent resync-sa** *seconds*

**no ip mobile home-agent resync-sa** *seconds*

### Syntax Description

<i>seconds</i>	Specifies the time in which the home agent will wait to initiate a resynchronization.
----------------	---

### Defaults

This command is off by default. The normal behavior of the home agent is to never requery the AAA server for a new security association.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2	This command was introduced.

### Usage Guidelines

You must enable security association caching for the **ip mobile home-agent resync-sa** command to work. Use the **ip mobile host aaa load-sa** global configuration command to enable caching of security associations retrieved from a AAA server.

When a security association is downloaded for a mobile node from a AAA server, the security association is time stamped. If the mobile node fails reregistration and the time interval since the security association was cached is greater than *sec* seconds, the home agent will clear out the old security association and requery the AAA server. If the time period is less than the *sec* value, the home agent will not requery the AAA server for the security association of the mobile node.

The *sec* value represents the number of seconds the home agent will consider the downloaded security association synchronized with the AAA server. After that time period, it is considered old and can be replaced by a new security association from the AAA server.

This time-based resynchronization process helps prevent denial-of-service attacks on the AAA server and provides a way to synchronize the home agent's cached security association entry when a change to the security association for the mobile node is made at the AAA server and on the mobile node. By using this process, once the mobile node fails reregistration with the old cached security association, the home agent will clear the cache for that mobile node, and resynchronize with the AAA server.

---

**Examples**

In the following example, if a registration fails authentication, the home agent retrieves a new security association from the AAA server if the existing security association was downloaded more than 10 seconds ago:

```
ip mobile home-agent resync-sa 10
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip mobile host</b>	Configures the mobile node or mobile host group.

---

# ip mobile home-agent revocation

To enable support for MIPv4 registration revocation on the home agent, use the **ip mobile home-agent revocation** command in global configuration mode. To disable support for registration revocation, use the **no** form of the command.

**ip mobile home-agent revocation** [*timeout seconds*] [*retransmit retries*] [*timestamp msec*]

**no ip mobile home-agent revocation** [*timeout seconds*] [*retransmit retries*] [*timestamp msec*]

## Syntax Description

<b>timeout</b> <i>seconds</i>	(Optional) Configures the time interval (in seconds) between retransmission of MIPv4 registration revocation message. The <b>no</b> version restores the time interval between retransmission of MIPv4 registration revocation Message to the default value. The default is 3 seconds. The range is from 1 to 100 seconds
<b>retransmit</b> <i>retries</i>	(Optional) Configures the number of times MIPv4 registration revocation messages are retransmitted. The <b>no</b> version of this command restores the retransmit number to the default value. The default is 3 retransmissions. The range is from 1 to 100 retransmissions.
<b>timestamp</b> <i>msec</i>	(Optional) Configures the units in which the timestamp value in the revocation support extension and revocation message should be encoded. By default the timestamp value will be sent as seconds. If the <b>msec</b> option is specified, the values will be encoded in milliseconds.

## Command Default

The home agent does not support registration revocation.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(7)XJ	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

In the following example, the MIPv4 registration message will be retransmitted a maximum of 5 times with a time interval of 4 seconds in between retransmissions:

```
Router(config)# ip mobile home-agent revocation timeout 4 retransmit 5
```

# ip mobile home-agent template tunnel

To configure a home agent to use the template tunnel, use the **ip mobile home-agent template tunnel** command in global configuration. To disable the use of the template tunnel, use the **no** form of the command.

**ip mobile home-agent template tunnel** *interface-id* **address** *ha-address*

**no ip mobile home-agent template tunnel** *interface-id* **address** *ha-address*

## Syntax Description

<i>interface-id</i>	The template tunnel interface ID from which to apply ACLs.
<b>address</b> <i>ha-address</i>	Specifies the home agent address. ACLs will be applied to tunnels with <i>ha-address</i> as the local end point.

## Command Default

The home agent does not use a template tunnel.

## Command Modes

Global configuration

## Command History

Release	Modification
12.3(8)XJW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

## Examples

In the following example, the home agent is configured to use the template tunnel:

```
Router(config)# interface tunnel 10
!
Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1
```

# ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** command in global configuration mode. To disable these services, use the **no** form of this command.

```
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} [aaa [load-sa
[permanent]]] [authorized-pool name] [skip-aaa-reauthentication][care-of-access
access-list] [lifetime seconds]
```

```
no 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} [aaa
[load-sa [permanent]]] [authorized-pool name] [skip-aaa-reauthentication] [care-of-access
access-list] [lifetime seconds]
```

## Syntax Description

<i>lower</i> [ <i>upper</i> ]	One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional.
<b>nai string</b>	Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (@realm).
<b>static-address</b>	(Optional) Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm.
<i>addr1</i> , <i>addr2</i> , ...	(Optional) One to a maximum of five IP addresses to be assigned using the <b>static-address</b> keyword.
<b>local-pool name</b>	(Optional) Name of the local pool of addresses to use for assigning a static IP address to this NAI.
<b>address</b>	(Optional) Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
<i>addr</i>	(Optional) IP address to be assigned using the <b>address</b> keyword.
<b>pool</b>	(Optional) Indicates that a pool of addresses is to be used in assigning a dynamic IP address.
<b>local name</b>	(Optional) The name of the local pool to use in assigning addresses.
<b>dhcp-proxy-client</b>	(Optional) Indicates that the DHCP request should be sent to a DHCP server on behalf of the mobile node.
<b>dhcp-server</b> <i>addr</i>	(Optional) IP address of the DHCP server.
<b>interface name</b>	When used with DHCP, specifies the gateway address from which the DHCP server should select the address.
<b>virtual-network</b> <i>network-address mask</i>	Indicates that the mobile station resides in the specified virtual network, which was created using the <b>ip mobile virtual-network</b> command.
<b>aaa</b>	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server. Allows the home agent to download address configuration details from the AAA server.
<b>load-sa</b>	(Optional) Caches security associations after retrieval by loading the security association into RAM. See <a href="#">Table 8</a> for details on how security associations are cached for NAI hosts and non-NAI hosts.

<b>permanent</b>	(Optional) Caches security associations in memory after retrieval permanently. Use this optional keyword only for NAI hosts.
<b>authorized-pool</b> <i>name</i>	(Optional) Verifies the IP address assigned to the mobile node if it is within the pool specified by the <i>name</i> argument.
<b>skip-aaa-reauthentication</b>	(Optional) When configured, the home agent does not send an access request for authentication for mobile IP re-registration requests. When disabled, the home agent sends an access request for all Mobile IP registration requests.
<b>care-of-access</b> <i>access-list</i>	(Optional) Access list. This can be a named access list or standard access list. The range is from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
<b>lifetime</b> <i>seconds</i>	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. The range is from 3 to 65535 (infinite).

**Defaults**

No host is configured.

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The <b>nai</b> keyword and associated parameters were added.
12.2(13)T	The <b>permanent</b> keyword was added and the command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The <b>authorized-pool</b> and <b>skip-aaa-reauthentication</b> keywords were added.

**Usage Guidelines**

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from a AAA server.

All hosts must have security associations for registration authentication. Mobile nodes can have more than one security association. The memory consumption calculations shown in [Table 7](#) are based on the assumption of one security association per mobile node. Caching behavior of security associations differs between NAI and non-NAI hosts as described in [Table 8](#).

The **nai** keyword allows you to specify a particular mobile node or range of mobile nodes. The mobile node can request a static IP address (**static-address** keyword), which is configured using the *addr1* variable (for a specific address) or the **local-pool** keyword (for an IP address from an address pool; the requested address must be in the pool). Or, the mobile node can request a dynamic address (**address** keyword), which is configured using the *addr* variable (for a specific address) or the **pool** keyword (for an IP address from a pool or DHCP server). If this command is used with the Packet Data Serving Node (PDSN) proxy Mobile IP feature and a realm is specified in the **ip mobile proxy-host nai** command, then only a pool of addresses can be specified in this command.

The address pool can be defined by a local pool or by use of a DHCP proxy client. For DHCP, the **interface name** keyword and argument combination specifies the gateway address from which the DHCP server should select the address and the **dhcp-server** keyword specifies the DHCP server address. The NAI is sent in the client-id option of the DHCP packet and can be used to provide dynamic DNS services.

You can also use this command to configure the static IP address or address pool for multiple flows with the same NAI. A flow is a set of {NAI, IP address}.

Security associations can be stored by using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in (**aaa optional** keyword)
- On the AAA server, retrieve and cache security association (**aaa load-sa** option)

Each method has advantages and disadvantages, which are described in [Table 7](#).

**Table 7**      **Methods for Storing Security Associations**

Storage Method	Advantage	Disadvantage
On the router	<ul style="list-style-type: none"> <li>• Security association is in router memory, resulting in fast lookup.</li> <li>• For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router).</li> </ul>	<ul style="list-style-type: none"> <li>• NVRAM of router is limited, cannot store many security associations. Each security association configuration takes about 80 bytes. For 125 KB NVRAM, you can store about 1500 security associations on a home agent.</li> </ul>
On the AAA server, retrieve security association each time registration comes in	<ul style="list-style-type: none"> <li>• Central administration and storage of security association on AAA server.</li> <li>• If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration.</li> <li>• Router memory (DRAM) is conserved. Router will need memory only to load in a security association, and then release the memory when done.</li> </ul>	<ul style="list-style-type: none"> <li>• Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance.</li> <li>• Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response.</li> <li>• Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).</li> </ul>

**Table 7** *Methods for Storing Security Associations (continued)*

Storage Method	Advantage	Disadvantage
On the AAA server, retrieve and store security association	<ul style="list-style-type: none"> <li>• AAA acts as an offload configuration server, security associations are loaded into router DRAM, which is more abundant (for example, 16 MB, 32 MB, 64 MB) when the first registration comes in. Each security association takes only about 50 bytes of DRAM, so 10,000 mobile nodes will use up 0.5 MB.</li> <li>• If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router.</li> <li>• Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory.</li> </ul>	<ul style="list-style-type: none"> <li>• If keys change on the AAA server after the mobile node registered, then you need to use <b>clear ip mobile secure</b> command to clear and load in new security association from AAA, otherwise the security association of the router is stale.</li> </ul>

The caching behavior of security associations for NAI hosts and non-NAI hosts is described in [Table 8](#).

**Table 8** *Caching Behavior for Security Associations*

Keyword Option	NAI Hosts	Non-NAI Hosts
<b>aaa</b>	Security associations are deleted after authentication and are not cached.	Security associations are deleted after authentication and are not cached.
<b>aaa load-sa</b>	The security association is cached while the mobile node is registered. If the mobile node's registration is deleted, the security association is removed.	Security associations are cached permanently.
<b>aaa load-sa permanent</b>	Security associations are cached permanently after being retrieved from the AAA server.	—

**Note**

On the Mobile Wireless Home Agent, the following conditions apply:

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.

**Examples**

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and retrieve mobile node security associations from a AAA server every time the mobile node registers:

```
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 aaa
```

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:

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 9.0.0.0  
255.0.0.0 aaa lifetime 180
```

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 as long as the binding is present and are deleted on the home agent when the binding is removed (due to manual clearing of the binding or lifetime expiration).

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

The following example configures a local pool of static addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
ip mobile host nai @cisco.com static-address local-pool mobilenodes
```

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
```

The following example configures the DHCP proxy client to use a DHCP server located at 10.1.2.3 to allocate a dynamic home address:

```
ip mobile host nai @dhcppool.com address pool dhcp-proxy-client dhcp-server 10.1.2.3  
interface FastEthernet 0/0
```

Related Commands	Command	Description
	<b>aaa authorization ipmobile</b>	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.
	<b>clear ip mobile secure</b>	Clears and retrieves remote security associations.
	<b>ip mobile proxy-host</b>	Locally configures the proxy Mobile IP attributes
	<b>ip mobile secure</b>	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.
	<b>show ip mobile host</b>	Displays mobile node counters and information.