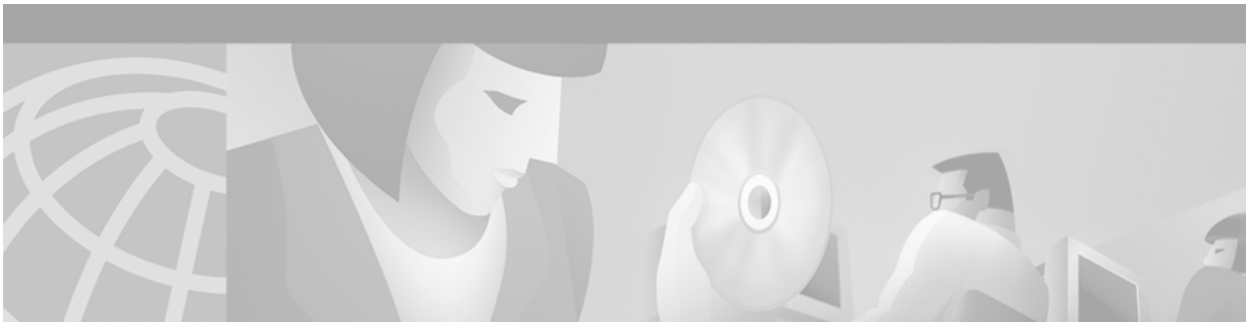

Mobile IP Commands

Use the commands in this chapter to configure and monitor Mobile IP. For Mobile IP configuration information and examples, refer to the "Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide*.

aaa authorization ipmobile

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

aaa authorization ipmobile {[**radius** | **tacacs+**] | **default**} [**group** *server-groupname*]

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

Syntax Description

radius	Authorization list named radius.
tacacs+	Authorization list named tacacs+.
default	Default authorization list.
group *server-groupname*	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 suppported.

The **aaa authorization ipmobile default group** *server-groupname* 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
aaa new-model	Enables the AAA access control model.
ip mobile host	Configures the mobile host or mobile node group.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
show ip mobile host	Displays mobile node information.
tacacs-server host	Specifies a TACACS host.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

clear ip mobile binding

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

clear ip mobile binding {**all** [**load** *standby-group-name*] | [*ip-address*]}

Syntax Description

all	Clears all mobility bindings.
load	(Optional) Downloads mobility bindings for a standby group after clear.
standby-group-name	(Optional) Name of the standby group.
ip-address	(Optional) IP address of a mobile node.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The following keywords and argument were added: • **all** • **load** • *standby-group-name*

Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. The mobility binding allows the mobile node to exchange packets with the correspondent 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. There should be no need to clear the binding because it expires after lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed, 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.

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

Examples

The following example administratively stops mobile node 10.0.0.1 from roaming:

```
Router# clear ip mobile binding 10.0.0.1

Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.

clear ip mobile secure

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

clear ip mobile secure {**host** *lower* [*upper*] | **empty** | **all**} [**load**]

Syntax Description

host	Mobile node host.
lower	IP address of mobile node. Can be used alone, or as lower end of a range of addresses.
upper	(Optional) Upper end of range of IP addresses.
empty	Load in only mobile nodes without security associations. Must be used with the **load** keyword.
all	Clears all mobile nodes.
load	(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.

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 10.0.0.1 after registration:

```
Router# show ip mobile secure host 10.0.0.1

Security Associations (algorithm,mode,replay protection,key):
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

The security association of the AAA server changes as follows:

```
Router# clear ip mobile secure host 10.0.0.1 load

Router# show ip mobile secure host 10.0.0.1
```

```
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

Related Commands

Command	Description
ip mobile secure aaa-download	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** EXEC command.

clear ip mobile traffic [**undo**]

Syntax Description

undo	Restores the previously cleared counters.

Command Modes

EXEC

Command History

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 (this is useful for debugging). See the **show ip mobile traffic** command for a description of all counters.

Examples

The following example shows how the 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
show ip mobile traffic	Displays protocol counters.

clear ip mobile visitor

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

clear ip mobile visitor [*ip-address*]

Syntax Description

ip-address	(Optional) IP address. If not specified, visitor information will be removed for all addresses.

Command Modes

EXEC

Command History

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

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 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.

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

Examples

The following example administratively stops visitor 10.0.0.1 from visiting:

```
Router# clear ip mobile visitor 10.0.0.1
```

Related Commands

Command	Description
show ip mobile visitor	Displays the table containing the visitor list of the foreign agent.

ip mobile foreign-agent

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

ip mobile foreign-agent [**care-of** *interface* | **reg-wait** *seconds*]

no ip mobile foreign-agent [**care-of** *interface* | **reg-wait** *seconds*]

Syntax Description

care-of *interface*	(Optional) IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured.
reg-wait *seconds*	(Optional) Pending registration expires after the specified number of seconds if no reply is received. Range is from 5 to 600. Default is 15.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

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 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 interface or no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated (**show ip mobile secure visitor** command). The registration bitflag is handled as described in Table 38 (**show ip mobile interface** command). 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 39). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation** command). (Violation reasons are listed in Table 43.)

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 sending 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 will 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 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.

Table 38 lists foreign agent registration bitflags.

Table 38 Foreign Agent Registration 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.
V	Deny request. Van Jacobson Header compression is not supported.
T	Deny request. Reverse tunnel is not supported.
reserved	Deny request. Reserved bit must not be set.

Table 39 lists foreign agent reply codes.

Table 39 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.

Table 39 Foreign Agent Reply Codes (continued)

Code	Reason
72	Requested encapsulation is unavailable.
73	Requested Van Jacobson Header compression is unavailable.
74	Reverse tunnel unsupported.
80-95	ICMP Unreachable message code 0 to 15.

Examples

The following example enables foreign agent service on interface Ethernet1, advertising 1.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 1.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

Related Commands

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

ip mobile foreign-service

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

ip mobile foreign-service [**home-access** *acl*] [**limit** *number*] [**registration-required**]

no ip mobile foreign-service [**home-access** *acl*] [**limit** *number*] [**registration-required**]

Syntax Description

home-access *acl*	(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. You cannot use this keyword when you enable foreign agent service on a subinterface.
limit *number*	(Optional) Number of visitors allowed on interface. The Busy (B) bit will be advertised when the number of registered visitors reach this limit. Range is from 1 to 1000. Default is no limit. You cannot use this keyword when you enable foreign agent service on a subinterface.
registration-required	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. You cannot use this keyword when you enable foreign agent service on a subinterface.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command enables foreign agent service on the interface. 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.

Table 40 lists the advertised bitflags.

Table 40 Foreign Agent Advertisement Bitflags

Bit Set	Service Advertisement
R	Set if the **registration-required** parameter is enabled.
B	Set if the number of visitors reached the **limit** 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	Never set.
reserved	Never set.

Examples

The following example enables foreign agent service for up to 100 visitors:

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

Related Commands

Command	Description
show ip mobile interface	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 services on the router, use the **ip mobile home-agent** global configuration command. To disable these services, use the **no** form of this command.

ip mobile home-agent [**address** *ip-address*][**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]

no ip mobile home-agent [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**suppress-unreachable**]

Syntax Description

address *ip-address*	(Optional) Specifies the IP address of the home agent. This option is only applicable when home agent redundancy is used for virtual networks.
broadcast	(Optional) Enables broadcast datagram routing. By default, broadcasting is disabled.
care-of-access *acl*	(Optional) Controls which care-of addresses (in registration request) are permitted by the home agent. By default, all care-of addresses are permitted. The access control list can be a string or number from 1 to 99.
lifetime *number*	(Optional) Specifies the global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Range is from 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
replay *seconds*	(Optional) Sets the replay protection time-stamp value. Registration received within this time is valid.
reverse-tunnel-off	(Optional) Disables support of reverse tunnel by the home agent. By default, reverse tunnel support is enabled.
roam-access *acl*	(Optional) Controls which mobile nodes are permitted or denied to roam. By default, all specified mobile nodes can roam.
suppress-unreachable	(Optional) Disables sending ICMP unreachable messages to the source when a mobile node on the virtual network is not registered, or when a packet came in from a tunnel interface created by the home agent (in the case of a reverse tunnel). By default, ICMP unreachable messages are sent.

Defaults

Disabled. Broadcasting is disabled by default. Reverse tunnel support is enabled by default. ICMP Unreachable messages are sent by default.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

The home agent is responsible for processing registration requests from the mobile node and setting up tunnels and routes to the care-of address. Packets to the mobile node are forwarded to the visited network.

The home agent will forward broadcast packets to mobile nodes if they registered with the service. However, heavy broadcast traffic utilizes the CPU of the router. The home agent can control where the mobile nodes roam by the **care-of-access** parameter, and which mobile node is allowed to roam by the **roam-access** parameter.

When a registration request comes in, the home agent will ignore requests when home agent service is not enabled or the security association of the mobile node 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 foreign agent (IP source address or care-of address in request), the foreign agent is authenticated, and then the mobile node is authenticated. The Identification field is verified to protect against replay attack. The home agent checks the validity of the request (see Table 41) and sends a reply. (Replay codes are listed in Table 42.) A security violation is logged when foreign agent authentication, MH authentication, or Identification verification fails. (The violation reasons are listed in Table 43.)

After registration is accepted, the home agent creates or updates the mobility binding of the mobile node, 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 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 mobile nodes are using it), and gratuitous ARPs are sent out if the mobile node is back home. Mobility binding is removed (along with its associated host route and tunnel) when registration lifetime expires or deregistration is accepted.

When the packet destined for the mobile node arrives on the home agent, the home agent encapsulates the packet and tunnels it to the care-of address. If the Don't fragment bit is set in the packet, the outer bit of the IP header is also set. 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 sent to the source. If the home agent loses the route to the tunnel endpoint, the host route to the mobile node will be removed from the routing table until tunnel route is available. Packets destined for the mobile node without a host route will be sent out the interface (home link) or to the virtual network (see the description of **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the home agent will send a copy to all mobile nodes registered with the broadcast routing option.

Table 41 describes how the home agent treats registrations with various bits set when authentication and identification are passed.

Table 41 Home Agent Registration Bitflags

Bit Set	Registration Reply
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	Ignore. Van Jacobsen Header compression is not supported.

Table 41 Home Agent Registration Bitflags (continued)

Bit Set	Registration Reply
T	Accept if **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

Table 42 lists the home agent registration reply codes.

Table 42 Home Agent Registration Reply Codes

Code	Reason
0	Accept.
1	Accept, no simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	Mobile node failed authentication.
132	Foreign agent failed authentication.
133	Registration identification mismatched.
134	Poorly formed request.
136	Unknown home agent address.
137	Reverse tunnel is unavailable.
139	Unsupported encapsulation.

Table 43 lists security violation codes.

Table 43 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.

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
show ip mobile globals	Displays global information for mobile agents.

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 *sec*

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

Syntax Description

sec	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

Command	Description
ip mobile host	Configures the mobile node or mobile host group.

ip mobile home-agent standby

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

ip mobile home-agent standby *hsrp-group-name* [[**virtual-network**] **address** *address*]

no ip mobile home-agent standby *hsrp-group-name* [[**virtual-network**] **address** *address*]

Syntax Description

hsrp-group-name	Specifies the HSRP group name.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address *address*	(Optional) Home agent address.

Defaults

No global home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.

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.

Examples

The following example specifies an HSRP group named SanJoseHA:

```
ip mobile home-agent standby SanJoseHA
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command.

ip mobile host *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

no ip mobile host *lower* [*upper*] {**interface** *name* | **virtual-network** *net mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

Syntax Description

lower [*upper*]	Range of mobile host or mobile node group IP addresses.
interface *name*	Mobile node that belongs to the specified interface.
virtual-network *net mask*	The wireless mobile node resides in the virtual network created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations froma AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Stores security associations in memory after retrieval.
care-of-access *acl*	(Optional) Access list. This can be a string or number from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
lifetime *number*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. Range is from 3 to 65535.

Defaults

No host is configured.

Command Modes

Global configuration

Command History

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

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 an AAA server. When using an AAA server, the router will attempt to download all security associations when the command is entered. If no security associations are retrieved, retrieval will be attempted when a registration request arrives or the **clear ip mobile secure** command is entered.

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 44 are based on the assumption of one security association per mobile node.

Security associations can be stored using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in
- On the AAA server, retrieve and store security association

Each method has advantages and disadvantages, which are described in Table 44.

Table 44 Methods for Storing Security Associations

Storage Method	Advantage	Disadvantage
On the router	• Security association is in router memory, resulting in fast lookup. • For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router).	• 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.
On the AAA server, retrieve security association each time registration comes in	• Central administration and storage of security association on AAA server. • If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration. • Router memory (DRAM) is conserved. Router will only need memory to load in a security association, and then release the memory when done. Router can support unlimited number of mobile nodes.	• Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance. • Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response. • Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).

Table 44 Methods for Storing Security Associations (continued)

Storage Method	Advantage	Disadvantage
On the AAA server, retrieve and store security association	• 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. • If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router. • Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory.	• If keys change on the AAA server after the mobile node registered, then you need to use **clear ip mobile secure** command to clear and load in new security association from AAA, otherwise the security association of the router is stale.

Examples

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and store its security associations on the AAA server:

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

Related Commands

Command	Description
aaa authorization ipmobile	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.
ip mobile secure aaa-download	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.
show ip mobile host	Displays mobile node information.

ip mobile prefix-length

To append the prefix-length extension to the advertisement, use the **ip mobile prefix-length** interface configuration command. To restore the default, use the **no** form of this command.

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

This command has no arguments or keywords.

Defaults

The prefix-length extension is not appended.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The prefix-length extension is used for movement detection. When a mobile node registered with one foreign agent receives an agent advertisement from another foreign agent, the mobile node uses the prefix-length extension to determine whether the advertisements arrived on the same network. The mobile node needs to register with the second foreign agent if it is on a different network. If the second foreign agent is on the same network, reregistration is not necessary.

Examples

The following example appends the prefix-length extension to agent advertisements sent by a foreign agent:

```
ip mobile prefix-length
```

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile registration-lifetime

To set the registration lifetime value advertised, use the **ip mobile registration-lifetime** interface configuration command.

ip mobile registration-lifetime *seconds*

Syntax Description

seconds	Lifetime in seconds. Range is from 3 to 65535 (infinity).

Defaults

36000 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command allows an administrator to control the advertised lifetime on the interface. The foreign agent uses this command to control duration of registration. Visitors requesting longer lifetimes will be denied.

Examples

The following example sets the registration lifetime to 10 minutes on interface Ethernet 1 and 1 hour on interface Ethernet 2:

```
interface e1
 ip mobile registration-lifetime 600
interface e2
 ip mobile registration-lifetime 3600
```

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile secure aaa-download

To specify that authentication, authorization, and accounting (AAA) mobility security associations (SAs) are downloaded from the AAA server and at what rate the information is downloaded, use the **ip mobile secure aaa-download** command in global configuration mode. To delete the AAA download rate, use the **no** form of this command.

ip mobile secure aaa-download rate *seconds*

no ip mobile secure aaa-download rate *seconds*

Syntax Description

rate	Rate at which the AAA SA is downloaded. • *seconds*—Download rate, in seconds. The range is from 1 to 100.

Defaults

No AAA SAs are downloaded.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SAs are downloaded from a AAA server on the first use. This command allows the home agent (HA) to prepopulate an SA table.

Examples

The following example shows a download rate of 35 seconds:

```
ip mobile secure aaa-download rate 35
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.

Command	Description
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure foreign-agent

To specify the mobility security associations (SAs) for a foreign agent (FA), use the **ip mobile secure foreign-agent** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a FA or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple FAs are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for FAs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

On a FA, the SA of the visiting mobile host and the SA of the home agent (HA) are optional. Multiple SAs for each entity can be configured.

The SA of a visiting mobile host on the MFAE and the SA of the HA on the FHAE are optional on the FA as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of SAs for an FA with an IP address of 209.165.200/254:

```
ip mobile secure foreign-agent 209.165.200/254 inbound-spi 203 outbound-spi 150 key
hex ffffffff
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure home-agent

To specify the mobility security associations (SAs) for a home agent (HA), use the **ip mobile secure home-agent** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of an HA or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple HAs are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for HAs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HA may have multiple SAs for each peer. The SPI specifies which SA to use for the peer and selects the specific security parameters to be used to authenticate the peer.

On an HA, the SA of the mobile host is mandatory for mobile host authentication and allows the HA to compute the MHAE for mobile host authentication. If desired, configure a foreign agent (FA) SA on your HA.

The mobile IP protocol automatically synchronizes the time stamp used by the mobile node (MN) in its registration requests. If the MN registration request time stamp is outside the HA permitted replay protection time interval, the HA will respond with the number of seconds by which the MN time stamp is off relative to the HA clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always falls within the HA replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and HA.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for an HA with an IP address of 10.0.0.4:

```
ip mobile secure home-agent 10.0.0.4 spi 100 key hex ffffffff
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure host

To specify the mobility security associations (SAs) for a mobile host, use the **ip mobile secure host** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a host or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple hosts are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for mobile hosts.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for a host:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.

ip mobile secure mn-aaa

To specify non-standard security parameter index (SPI) values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent, use the **ip mobile secure mn-aaa** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile secure mn-aaa spi {*hex-value* | **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

no ip mobile secure mn-aaa spi {*hex-value* | **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

Syntax Description

spi	Bidirectional security parameter index (SPI). The index can be a hexadecimal or decimal value. The arguments and keyword are as follows: • *hex-value*—SPI expressed in hexadecimal digits. The range is from 100 to ffffffff. No spaces are allowed. The maximum is 32 characters. • **decimal** *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295. No spaces are allowed. The maximum is 32 characters.
algorithm md5 mode ppp-chap-style	Message Digest 5 (MD5) authentication algorithm used during authentication by the Challenge-Handshake Authentication Protocol (CHAP).

Defaults

The home agent or foreign agent only accept the standard SPI value in the MN-AAA authentication extension that specifes CHAP-style authentication using MD5. The standard value for the SPI is 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode.

A mobile node configured to be authenticated via an MN-AAA authentication extension is required to use an SPI value of 2 to indicate CHAP-style authentication using MD5 as specified by RFC 3012, *Mobile IPv4 Challenge/Response Extensions.*

Some network implementations need the flexibility to allow an SPI value other than 2 even though the mobile node is authenticated using CHAP. The **ip mobile secure mn-aaa** command maps new SPI values in the MN-AAA extension of the registration message to the SPI value pre-defined by RFC 3012. When a registration request arrives at the foreign agent or home agent with the MN-AAA extension containing an SPI value specified by the **ip mobile secure mn-aaa** command, the foreign agent or home agent will process it as if the value was 2 instead of rejecting the request.

Use this command with caution because it is non-standard behavior. For example, different vendors might use the same non-standard SPI to denote different authentication methods and this could affect interoperability. In general, Cisco recommends the use of standard SPI values to be used in the MN-AAA authentication extension by the mobile node.

Examples

In the following example, the foreign agent or home agent will process the registration request even though the CHAP SPI value is not 2:

```
ip mobile secure mn-aaa spi 1234 algorithm md5 mode ppp-chap-style
```

ip mobile secure proxy-host

To specify the mobility security associations (SAs) for a proxy host, use the **ip mobile secure proxy-host** command in global configuration mode. To remove the mobility SAs, use the **no** form of this command.

ip mobile secure proxy-host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure proxy-host {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a proxy host or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple proxy hosts are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time that a router uses for replay protection. The range is from plus or minus 255 seconds. The default is plus or minus 7 seconds. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for proxy hosts.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.
12.3(4)T	The **proxy-host** keyword was added for Packet Data Serving Node (PDSN) platforms only.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note The **proxy-host** keyword is available only on PDSN platforms that are running specific PDSN code images; consult Cisco Feature Navigator for your Cisco IOS software release.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for a proxy host:

```
ip mobile secure proxy-host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure visitor

To specify the mobility security associations (SAs) for a visitor, use the **ip mobile secure visitor** command in global configuration mode. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure visitor {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

no ip mobile secure visitor {*lower-address* [*upper-address*] | **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix** | **hmac-md5**}]

Syntax Description

lower-address	IP address of a visitor or lower range of IP address pool. • *upper-address*—(Optional) Upper range of IP address pool. If specified, SAs for multiple visitors are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string*—NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *spi-in*—Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *spi-out*—Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value*—SPI expressed as a hexadecimal. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal**—Decimal SPI. The argument is as follows: – *decimal-value*—SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string*—Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string*—Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.

replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*—Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **md5 mode**—Message Digest 5 (MD5) mode used to authenticate packets during registration. • **prefix-suffix**—Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. • **hmac-md5**—Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Defaults

No SA is specified for visitors.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The Mobile IP protocol automatically synchronizes the time stamp used by the MN in its registration requests. If the MN registration request time stamp is outside the visitor permitted replay protection time interval, the visitor will respond with the number of seconds the MN time stamp is off relative to the visitor clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always fall within the visitor replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and visitor.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for a visitor:

```
ip mobile secure visitor 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** global configuration command.

ip mobile tunnel {**route-cache** | **path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] | **nat** {**inside** | **outside**}}

Syntax Description

route-cache	Sets tunnels to default or process switching mode.
path-mtu-discovery	Specifies when the tunnel MTU should expire if set by Path MTU Discovery.
age-timer *minutes*	(Optional) Time interval in minutes after which the tunnel reestimates the path MTU.
infinite	(Optional) Turns off the age timer.
nat	Applies Network Address Translation (NAT) on the tunnel interface.
inside	Sets the dynamic tunnel as the inside interface for NAT.
outside	Sets the dynamic tunnel as the outside interface for NAT.

Defaults

Disabled.

If enabled, default value for the *minutes* argument is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	The following keywords were added: • **nat** • **inside** • **outside**

Usage Guidelines

Path MTU Discovery is used by end stations to find a packet size that does not need fragmentation between them. Tunnels must adjust their MTU to the smallest MTU interior to achieve this condition, as described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from a case where suboptimum MTU existed at time of discovery. It is reset to the outgoing MTU of the interface.

Examples

The following example sets the discovered tunnel MTU to expire in 10 minutes (600 seconds):

```
ip mobile tunnel path-mtu-discovery age-timer 600
```

Related Commands

Command	Description
show ip mobile tunnel	Displays active tunnels.

ip mobile virtual-network

To define a virtual network, use the **ip mobile virtual-network** global configuration command. To remove the virtual network, use the **no** form of this command.

ip mobile virtual-network *net mask* [**address** *address*]

no ip mobile virtual-network *net mask*

Syntax Description

net	Network associated with the IP address of the virtual network.
mask	Mask associated with the IP address of the virtual network.
address *address*	(Optional) IP address of a home agent on a virtual network.

Defaults

No home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **address** • *address*

Usage Guidelines

This command inserts the virtual network into the routing table to allow mobile nodes to use the virtual network as their home network. The network is propagated when redistributed to other routing protocols.

Note You may need to include virtual networks when configuring the routing protocols. If this is the case, use the **redistribute mobile** router configuration command to redistribute routes from one routing domain to another.

Examples

The following example adds the virtual network 20.0.0.0 to the routing table and specifies that the home agent IP address is configured on the loopback interface for that virtual network:

```
interface ethernet 0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

interface loopback 0
 ip address 20.0.0.1 255.255.255.255
```

```
ip mobile home-agent
 ip mobile virtual-network 20.0.0.0 255.255.0.0 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 hex 00112233445566778899001122334455
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
redistribute mobile	Redistributes routes from one routing domain into another routing domain.

router mobile

To enable Mobile IP on the router, use the **router mobile** global configuration command. To disable Mobile IP, use the **no** form of this command.

router mobile

no router mobile

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command must be used in order to run Mobile IP on the router, as either a home agent or a foreign agent. The process is started, and counters begin. Disabling Mobile IP removes all related configuration commands, both global and interface.

Examples

The following example enables Mobile IP:

```
router mobile
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.
show ip protocols	Displays the parameters and current state of the active routing protocol process.
show processes	Displays information about the active processes.

show ip mobile binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

show ip mobile binding [**home-agent** *address* | **summary**]

Syntax Description

home-agent *address*	(Optional) IP address of mobile node.
summary	(Optional) Total number of bindings in the table.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** • *address*
12.1(2)T	The **summary** keyword was added.

Usage Guidelines

The home agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

Examples

The following is sample output from the **show ip mobile binding** command:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
20.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Table 45 describes the significant fields shown in the display.

Table 45 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
<IP address>	Home IP address of the mobile node.
Care-of Addr	Care-of address of the mobile node.

Table 45 show ip mobile binding Field Descriptions (continued)

Field	Description
Src Addr	IP source address of the Registration Request as received by the home agent. Will be either the colocated care-of address of a mobile node or an address of the foreign agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the home agent.
Flags	Registration flags sent by mobile node. Uppercase characters denote bit set. See Table 41 for a description of each bit.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request, and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all home agent-accepted services. For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the home agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).

show ip mobile globals

To display global information for mobile agents, use the **show ip mobile globals** EXEC command.

show ip mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

This command shows the services provided by the home agent or foreign agent. Note the deviation from RFC 2006: the foreign agent will not display busy or registration required information. Both are handled on a per-interface basis (see the **show ip mobile interface** command in this chapter), not at the global foreign agent level.

Examples

The following is sample output from the **show ip mobile globals** command:

```
Router# show ip mobile globals

IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Virtual networks
        20.0.0.0/8

Foreign Agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled
Discovered tunnel MTU aged out after 1:00:00
```

Table 46 describes the significant fields shown in the display.

Table 46 show ip mobile globals Field Descriptions

Field	Description
Home Agent	
Registration lifetime	Default lifetime for all mobile nodes. Number of seconds given in parentheses.
Roaming access list	Determines which mobile nodes are allowed to roam. Displayed if defined.
Care-of access list	Determines which care-of addresses are allowed to be accepted. Displayed if defined.
Broadcast	Broadcast enabled or disabled.
Reverse tunnel	Reverse tunnel enabled or disabled.
ICMP Unreachable	Sends ICMP unreachable messages, which are enabled or disabled for virtual network.
Virtual networks	Lists virtual networks serviced by the home agent. Displayed if defined.
Foreign Agent	
Care-of addresses advertised	Lists care-of addresses (interface is up or down). Displayed if defined.
Mobility Agent	
Number of interfaces providing service	See the **show ip mobile interface** command for more information on advertising. Agent advertisements are sent when IRDP is enabled.
Encapsulations supported	IPIP and GRE.
Tunnel fast switching	Tunnel fast switching is enabled or disabled.
Discovered tunnel MTU	Aged out after amount of time.

show ip mobile host

To display mobile node information, use the **show ip mobile host** EXEC command.

show ip mobile host [*address* | **interface** *interface* | **network** *address* | **group** | **summary**]

Syntax Description

address	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
interface *interface*	(Optional) All mobile nodes whose home network is on this interface.
network *address*	(Optional) All mobile nodes residing on this network or virtual network.
group	(Optional) All mobile node groups configured using the **ip mobile host** command.
summary	(Optional) All values in the table.

Command Modes

EXEC

Command History

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

Examples

The following is sample output from the **show ip mobile host** command:

```
Router# show ip mobile host

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    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
```

Table 47 describes the significant fields shown in the display.

Table 47 show ip mobile host Field Descriptions

Field	Description
<IP address>	Home IP address of the mobile node.
Allowed lifetime	Allowed lifetime of the mobile node. By default, it is set to the global lifetime (**ip mobile home-agent lifetime** command). Setting this lifetime will override global value.
Roaming status	When the mobile node is registered, the roaming status is - Registered - ; otherwise, it is - Unregistered -. Use the **show ip mobile binding** command for more information when the user is registered.

Table 47 show ip mobile host Field Descriptions (continued)

Field	Description
Home link	Interface or virtual network.
Accepted	Total number of service requests for the mobile node accepted by the home agent (Code 0 + Code 1).
Last time	The time at which the most recent Registration Request was accepted by the home agent for this mobile node.
Overall service time	Overall service time that has accumulated for the mobile node since the home agent last rebooted.
Denied	Total number of service requests for the mobile node denied by the home agent (sum of all registrations denied with Code 128 through Code 159). See Table 41 for a list of codes.
Last time	The time at which the most recent Registration Request was denied by the home agent for this mobile node.
Last code	The code indicating the reason why the most recent Registration Request for this mobile node was rejected by the home agent.
Total violations	Total number of security violations.
Tunnel to MN	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from MN	Number of packets and bytes reverse tunneled from mobile node.

The following is sample output from the **show ip mobile host group** command for groups configured with the **ip mobile host** command:

```
Router# show ip mobile host group

20.0.0.1 - 20.0.0.20:
    Home link on virtual network 20.0.0.0 /8, Care-of ACL -none-
    Security associations on router, Allowed lifetime 10:00:00 (36000/default)
```

Table 48 describes the significant fields shown in the display.

Table 48 show ip mobile host group Field Descriptions

Field	Description
<IP address>	Mobile host IP address or grouping of addresses.
Home link	Interface or virtual network.
Care-of ACL	Care-of address access list.
Security association	Router or AAA server.
Allowed lifetime	Allowed lifetime for mobile host or group.

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.

show ip mobile interface

To display advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes, use the **show ip mobile interface** EXEC command.

show ip mobile interface [*interface*]

Syntax Description

interface	(Optional) IP address of mobile node. If not specified, all interfaces are shown.

Command Modes

EXEC

Command History

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

Examples

The following is sample output from the **show ip mobile interface** command:

```
Router# show ip mobile interface

IP Mobility interface information:
IRDP disabled
Interface Ethernet3:
    Prefix Length not advertised
    Lifetime is 36000 seconds
    Home Agent service provided
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip mobile interface Field Descriptions

Field	Description
Interface	Name of the interface.
IRDP	IRDP (includes agent advertisement) enabled or disabled. IRDP must be enabled for an advertisement to be sent out. Use the **ip irdp** command to enable IRDP.
Prefix Length	Prefix-length extension to be included or not in the advertisement.
Lifetime	Advertised registration lifetime.
Home Agent service provided	Displayed if home agent service is enabled on the interface.
Foreign Agent service provided	Displayed if foreign agent service is enabled on the interface.
Registration required	Foreign agent requires registration even from those mobile nodes that have acquired their own, colocated care-of address.
Busy	Foreign agent is busy for this interface.
Home Agent access list	Which home agent is allowed.

Table 49 show ip mobile interface Field Descriptions (continued)

Field	Description
Maximum number of visitors allowed	Displayed if defined.
Current number of visitors	Number of visitors on interface.

Related Commands

Command	Description
ip mobile foreign-agent	Enables foreign agent service.
ip mobile host	Configures the mobile host or mobile node group.
ip mobile prefix-length	Appends the prefix-length extension to the advertisement.
show ip irdp	Displays IRDP values.

show ip mobile secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, or home agent, use the **show ip mobile secure** EXEC command.

show ip mobile secure {**host** | **visitor** | **foreign-agent** | **home-agent** | **summary**} *address*

Syntax Description

host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile visitor on the foreign agent.
foreign-agent	Security association of the remote foreign agents on the home agent.
home-agent	Security association of the remote home agent on the foreign agent.
summary	All values in the table.
address	IP address.

Command Modes

EXEC

Command History

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

Usage Guidelines

Multiple security associations can exist for each entity.

Examples

The following is sample output from the **show ip mobile secure** command:

```
Router# show ip mobile secure

Security Associations (algorithm,mode,replay protection,key):
20.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip mobile secure Field Descriptions

Field	Description
20.0.0.6	IP address.
In/Out SPI	The SPI is the 4-byte opaque index within the Mobility Security Association that selects the specific security parameters to be used to authenticate the peer. Allows either “SPI” or “In/Out SPI.” The latter specifies an inbound and outbound SPI pair. If an inbound SPI is received, then outbound SPI will be used when a response is sent.
MD5	Message Digest 5 authentication algorithm.

Table 50 show ip mobile secure Field Descriptions (continued)

Field	Description
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

show ip mobile traffic

To display protocol counters, use the **show ip mobile traffic** EXEC command.

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

Counters can be reset to zero using the **clear ip mobile traffic** command, which also allows you to undo the reset.

Examples

The following is sample output from the **show ip mobile traffic** command:

```
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
    Unavailable encap 0, reverse tunnel 0
    Binding updates received 0, sent 0 total 0 fail 0
    Binding update acks received 0, sent 0
    Binding info request received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Replies in 0
    Forwarded 0, Bad 0, Ignored 0
    Authentication failed MN 0, HA 0
```

Table 51 describes the significant fields shown in the display.

Table 51 show ip mobile traffic Field Descriptions

Field	Description
Solicitations received	Total number of solicitations received by the mobility agent.
Advertisements sent	Total number of advertisements sent by the mobility agent.
response to solicitation	Total number of advertisements sent by the mobility agent in response to mobile node solicitations.
Home Agent	
Register requests	Total number of Registration Requests received by the home agent.
Deregister requests	Total number of Registration Requests received by the home agent with a lifetime of zero (requests to deregister).
Register replied	Total number of Registration Replies sent by the home agent.
Deregister replied	Total number of Registration Replies sent by the home agent in response to requests to deregister.
Accepted	Total number of Registration Requests accepted by the home agent (Code 0).
No simultaneous bindings	Total number of Registration Requests accepted by the home agent—simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of Registration Requests denied by the home agent.
Ignored	Total number of Registration Requests ignored by the home agent.
Unspecified	Total number of Registration Requests denied by the home agent—reason unspecified (Code 128).
Unknown HA	Total number of Registration Requests denied by the home agent—unknown home agent address (Code 136).
Administrative prohibited	Total number of Registration Requests denied by the home agent—administratively prohibited (Code 129).
No resource	Total number of Registration Requests denied by the home agent—insufficient resources (Code 130).
Authentication failed MN	Total number of Registration Requests denied by the home agent—mobile node failed authentication (Code 131).
Authentication failed FA	Total number of Registration Requests denied by the home agent—foreign agent failed authentication (Code 132).
Bad identification	Total number of Registration Requests denied by the home agent—identification mismatch (Code 133).
Bad request form	Total number of Registration Requests denied by the home agent—poorly formed request (Code 134).
Unavailable encap	Total number of Registration Requests denied by the home agent—unavailable encapsulation (Code 139).
Unavailable reverse tunnel	Total number of Registration Requests denied by the home agent—reverse tunnel unavailable (Code 137).

Table 51 show ip mobile traffic Field Descriptions (continued)

Field	Description
Binding updates	A Mobile IP standby message sent from the active router to the standby router when a registration request comes into the active router.
Binding update acks	A Mobile IP standby message sent from the standby router to the active router to acknowledge the reception of a binding update.
Binding info request	A Mobile IP standby message sent from a router coming up from reboot/or a down interface. The message is a request to the current active router to send the entire Mobile IP binding table.
Binding info reply	A reply from the active router to the standby router that has part or all of the binding table (depending on size).
Binding info reply acks	An acknowledge message from the standby router to the active router that it has received the binding info reply.
Gratuitous ARP	Total number of gratuitous ARPs sent by the home agent on behalf of mobile nodes.
Proxy ARPs sent	Total number of proxy ARPs sent by the home agent on behalf of mobile nodes.
Foreign Agent	
Request in	Total number of Registration Requests received by the foreign agent.
Forwarded	Total number of Registration Requests relayed to home agent by the foreign agent.
Denied	Total number of Registration Requests denied by the foreign agent.
Ignored	Total number of Registration Requests ignored by the foreign agent.
Unspecified	Total number of Registration Requests denied by the foreign agent—reason unspecified (Code 64).
HA unreachable	Total number of Registration Requests denied by the foreign agent—home agent unreachable (Codes 80-95).
Administrative prohibited	Total number of Registration Requests denied by the foreign agent—administratively prohibited (Code 65).
No resource	Total number of Registration Requests denied by the home agent— insufficient resources (Code 66).
Bad lifetime	Total number of Registration Requests denied by the foreign agent— requested lifetime too long (Code 69).
Bad request form	Total number of Registration Requests denied by the home agent—poorly formed request (Code 70).
Unavailable encapsulation	Total number of Registration Requests denied by the home agent— unavailable encapsulation (Code 72).
Unavailable compression	Total number of Registration Requests denied by the foreign agent— requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of Registration Requests denied by the home agent—reverse tunnel unavailable (Code 74).
Replies in	Total number of well-formed Registration Replies received by the foreign agent.
Forwarded	Total number of valid Registration Replies relayed to the mobile node by the foreign agent.

Table 51 show ip mobile traffic Field Descriptions (continued)

Field	Description
Bad	Total number of Registration Replies denied by the foreign agent—poorly formed reply (Code 71).
Ignored	Total number of Registration Replies ignored by the foreign agent.
Authentication failed MN	Total number of Registration Requests denied by the home agent—mobile node failed authentication (Code 67).
Authentication failed HA	Total number of Registration Replies denied by the foreign agent—home agent failed authentication (Code 68).

show ip mobile tunnel

To display active tunnels, use the **show ip mobile tunnel** EXEC command.

show ip mobile tunnel [*interface*]

Syntax Description

interface	(Optional) Displays a particular tunnel interface. The *interface* argument is tunnel *x*.

Command Modes

EXEC

Command History

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

Usage Guidelines

This command displays active tunnels created by Mobile IP. When no more users are on the tunnel, the tunnel is released.

Examples

The following is sample output from the **show ip mobile tunnel** command:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Tunnel0:
    src 68.0.0.32, dest 68.0.0.48
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    HA created, fast switching enabled, ICMP unreachable enabled
    0 packets input, 0 bytes, 0 drops
    1591241 packets output, 1209738478 bytes
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip mobile tunnel Field Descriptions

Field	Description
src	Tunnel source IP address.
dest	Tunnel destination IP address.
encap	Tunnel encapsulation type.
mode	Either reverse-allowed or reverse-off for reverse tunnel mode.
tunnel-users	Number of users on tunnel.
HA created	Home agent created.
fast switching	Enabled or disabled.

Table 52 show ip mobile tunnel Field Descriptions (continued)

Field	Description
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.
0 drops	Number of packets dropped. Packets are dropped when there are no visitors to send to after the foreign agent deencapsulates incoming packets. This prevents loops because the foreign agent will otherwise route the deencapsulated packets back to the home agent.
packets output	Number of packets output.
bytes	Number of bytes output.

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.
show ip mobile host	Displays mobile node information.
show ip mobile visitor	Displays the table of the visitor list of the foreign agent.

show ip mobile violation

To display information about security violations, use the **show ip mobile violation** EXEC command.

show ip mobile violation [*address*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.

Command Modes

EXEC

Command History

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

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the **logging** global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the **show logging** command.

Examples

The following is sample output from the **show ip mobile violation** command:

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1:
    Violations: 1, Last time: 06/18/97 01:16:47
    SPI: 300, Identification: B751B581.77FD0E40
    Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

Table 53 describes significant fields shown in the display.

Table 53 show ip mobile violation Field Descriptions

Field	Description
20.0.0.1	IP address of the violator.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.
SPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the Mobile-Home Authentication Extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.

Table 53 show ip mobile violation Field Descriptions (continued)

Field	Description
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply. See Table 51 for list of error codes.
Reason	Reason for the most recent security violation for this peer. Possible reasons are: • No mobility security association • Bad authenticator • Bad identifier • Bad SPI • Missing security extension • Other

show ip mobile visitor

To display the table containing the visitor list of the foreign agent, use the **show ip mobile visitor** EXEC command.

show ip mobile visitor [**pending**] [*address* | **summary**]

Syntax Description

pending	(Optional) Pending registration table.
address	(Optional) IP address.
summary	(Optional) All values in the table.

Command Modes

EXEC

Command History

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

Usage Guidelines

The foreign agent updates the table containing the visitor list of the foreign agent in response to registration events from mobile nodes.

Examples

The following is sample output from the **show ip mobile visitor** command:

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
20.0.0.1:
    Interface Ethernet1/2, MAC addr 0060.837b.95ec
    IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
    HA addr 66.0.0.5, Identification B7510E60.64436B38
    Lifetime 08:20:00 (30000) Remaining 08:19:16
    Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
    Routing Options - (T)Reverse-tunnel
```

Table 54 describes the significant fields shown in the display.

Table 54 show ip mobile visitor Field Descriptions

Field	Description
Total	1
20.0.0.1	Home IP address of a visitor.
Interface	Name of the interface.
MAC addr	MAC address of the visitor.
IP src	Source IP address the Registration Request of a visitor.

Table 54 show ip mobile visitor Field Descriptions (continued)

Field	Description
IP dest	Destination IP address of Registration Request of a visitor. When a foreign agent sends a reply to a visitor, the IP source address is set to this address, unless it is multicast or broadcast, in which case it is set to IP address of the output interface.
UDP src port	Source UDP port of Registration Request of the visitor.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime granted to the mobile node for this registration.
Remaining	The number of seconds remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Possible options are: • (S) Mult-binding • (B) Broadcast • (D) Direct-to-MN • (M) MinIP • (G) GRE • (V) VJH-compress • (T) Reverse-tunnel