

Mobile IP

Feature Summary

As PDAs and the next generation of data-ready cellular phones become more widely deployed, a greater degree of connectivity is almost becoming a necessity for the business user on the go. Data connectivity solutions for this group of users is a very different requirement than it is for the fixed dialup user or the stationary wired LAN user. Solutions here need to deal with the challenge of movement during a data session or conversation. Cellular service providers and network administrators wanting to deploy wireless LAN technologies need to have a solution which will grant this greater freedom.

Cisco IOS has integrated new technology into our routing platforms to meet these new networking challenges. Mobile IP is a tunneling-based solution which takes advantage of the Cisco-created GRE tunneling technology, as well as simpler IP-in-IP tunneling protocol. This tunneling enables a router on a user's home subnet to intercept and transparently forward IP packets to users while they roam beyond traditional network boundaries. This solution is a key enabler of wireless mobility, both in the wireless LAN arena, such as the 802.11 standard, and in the cellular environment for packet-based data offerings which offer connectivity to a user's home network and the Internet.

Mobile IP provides users the freedom to roam beyond their home subnet while consistently maintaining their home IP address. This enables transparent routing of IP datagrams to mobile users during their movement, so that data sessions can be initiated to them while they roam; it also enables sessions to be maintained in spite of physical movement between points of attachment to the Internet or other networks. Cisco's implementation of Mobile IP is fully compliant with the Internet Engineering Task Force's (IETF's) proposed standard defined in Request for Comments (RFC) 2002.

Benefits

Mobile IP is most useful in environments where mobility is desired and the traditional land line dial-in model or DHCP do not provide adequate solutions for the needs of the users. If it is necessary or desirable for a user to maintain a single address while they transition between networks and network media, Mobile IP can provide them with this ability. Generally, Mobile IP is most useful in environments where a wireless technology is being utilized. This includes cellular environments as well as wireless LAN situations that may require roaming. Mobile IP can go hand in hand with many different cellular technologies like CDMA, TDMA, GSM, AMPS, NAMPS, as well as other proprietary solutions, to provide a mobile system which will scale for many users.

Each mobile node is always identified by its home address, no matter what its current point of attachment to the Internet, allowing for transparent mobility with respect to the network and all other devices. The only devices which need to be aware of the movement of this node are the mobile device and a router serving the user's topologically correct subnet.

List of Terms

agent discovery—The method by which a mobile node determines whether it is currently connected to its home network or a foreign network and detects whether it has moved and the way it has moved. It is the mechanism by which mobile nodes query and discover mobility agents. This is done through an extension of the ICMP router discovery protocol, IRDP (RFC 1256), which includes a mechanism to advertise mobility services to potential users.

care-of address—The termination point of the tunnel to a mobile node. This can be a collocated care-of address, where the mobile node acquires a local address and detunnels its own packets, or a foreign agent care-of address, where a foreign agent detunnels packets and forwards them to the mobile node.

correspondent node—A peer with which a mobile node is communicating. A correspondent node may be either stationary or mobile.

foreign agent—A router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

home address—An IP address that is assigned for an extended time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

home agent—A router on a mobile node's home network which tunnels packets to the mobile node while it is away from home. It keeps current location information for registered mobile nodes called a *mobility binding*.

home network—The network or virtual network which matches the subnet address of the mobile node.

mobile node—A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming link-layer connectivity to a point of attachment is available.

mobility agent—A home agent or a foreign agent.

mobility binding—The association of a home address with a care-of address and the remaining lifetime.

mobility security association—A collection of security contexts between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode, a secret (a shared key or appropriate public/private key pair), and a style of replay protection in use.

MTU—Maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

node—A host or router.

registration—The process by which the mobile node is associated with a care-of address on the home agent while it is away from home. This may happen directly from the mobile node to the home agent or through a foreign agent.

security parameter index (SPI)—The index identifying a security context between a pair of nodes.

tunnel—The path followed by a datagram while it is encapsulated from the home agent to the mobile node.

virtual network—A network with no physical instantiation beyond a router (with a physical network interface on another network). The router (a home agent, for example) generally advertises reachability to the virtual network using conventional routing protocols.

visited network—A network other than a mobile node's home network, to which the mobile node is currently connected.

visitor list—The list of mobile nodes visiting a foreign agent.

Platforms

This feature is supported on these platforms:

- Cisco 2500 Series
- Cisco 2600 Series
- Cisco 3600 Series
- Cisco 4000 Series
- Cisco 4500 Series
- Cisco 4700 Series
- Cisco 7200 Series
- Cisco 7500 Series

Prerequisites

To configure home agent functionality on your router, you need to determine IP addresses or subnets for which you would like to allow roaming service. If you intend to support roaming without having a physical home location for the roaming devices, you need to identify the subnets for which you will allow this service and place these virtual networks appropriately within your network on the home agent. It is possible to enable home agent functionality for a homed or non-homed subnet. In the case of non-homed addresses, it is necessary to define virtual networks on the router. Mobile IP Home Agent and Foreign agent services can be configured on the same router or on separate routers to enable Mobile IP service to users.

Since Mobile IP requires support on the host device, it is necessary that each mobile node is appropriately configured for the desired Mobile IP service. Please refer to the manual entries in your mobile aware IP stack vendor's documentation for details on this.

Supported MIBs and RFCs

This feature supports the following MIBs:

- RFC2006-MIB.my

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB website on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

This feature supports the following RFCs:

- RFC 2002

- RFC 2003
- RFC 2006

Configuration Tasks

To enable Mobile IP services on your network, you need to determine not only which home agents will facilitate the tunneling for selected IP address, but also where these devices or hosts will be allowed to roam. The areas, or subnets, into which the hosts will be allowed to roam will determine where Foreign Agent services need to be set up.

To configure Mobile IP, complete the following tasks as related to the functions you intend to support.

Enabling Home Agent Services

Home Agent functionality is useful within an enterprise network to allow users to retain an IP address while they move their laptop PCs from their desktops into conference rooms or labs or common areas. It is especially beneficial in environments where wireless LANs are used, since it allows seamless transition between base stations, since the tunneling of datagrams hides the movement of the host. To support the mobility of users beyond the bounds of the enterprise network, home agent functionality can be enabled for virtual subnets on the DMZ or periphery of the network also, to communicate with external foreign agents.

To enable Home Agent service for users having homed or virtually homed IP addresses on the router, use the following commands in global configuration mode:

Step	Command	Purpose
1	router mobile	Enable Mobile IP on the router.
2	ip mobile home-agent	Enable home agent service.
3	ip mobile virtual-network <i>addr mask</i>	Add virtual network to routing table. If not using a virtual network, skip to step 6.
4	router protocol redistribute mobile	Enable redistribution of virtual network into routing protocol(s).
5	ip mobile host <i>lower [upper] virtual-network addr mask [aaa [load-sa]]</i>	Specify mobile nodes (on virtual network) and where their security associations are stored. ¹
6	ip mobile host <i>lower [upper] {interface name}</i>	Specify mobile nodes on interface and where their security associations are stored. Skip this step if there are no mobile nodes on the interface.
7	ip mobile secure host <i>addr {inbound-spi spi-in outbound-spi spi-out spi spi} key hex string</i>	Set up mobile hosts' security associations. Skip this step if using AAA.
8	ip mobile secure foreign-agent <i>addr {inbound-spi spi-in outbound-spi spi-out spi spi} key hex string</i>	(Optional) Set up foreign agents' security associations. Skip this step unless you have security association with remote foreign agents.

¹ By default, security associations are expected to be configured locally; however, the security association configuration can be offloaded to an AAA server.

Enabling Foreign Agent Services

Foreign Agent services need to be enabled on a router attached to any subnet into which a mobile node may be roaming. Therefore, you need to configure Foreign Agent functionality on routers connected to conference room or lab subnets, for example. For administrators wanting to utilize roaming between wireless LANs, Foreign Agent functionality would be configured on routers connected to each base station. In this case it is conceivable that both Home Agent and Foreign Agent functionality will be enabled on some of the routers connected to these wireless LANs.

To start a foreign agent providing default services, use the following commands in global configuration mode:

Step	Command	Purpose
1	router mobile	Enable Mobile IP on the router.
2	ip mobile foreign-agent care-of <i>interface</i>	Set up care-of address(es) advertised to all foreign agent-enabled interfaces.
3	ip mobile foreign-service	Enable foreign agent service on the interface.
4	ip mobile secure home-agent <i>addr</i> { inbound-spi <i>spi-in</i> outbound-spi <i>spi-out</i> spi <i>spi</i> } key <i>hex string</i>	(Optional) Set up home agent security association (optional). Skip steps 4 and 5 unless you have security association with remote home agents or visitors.
5	ip mobile secure visitor <i>addr</i> { inbound-spi <i>spi-in</i> outbound-spi <i>spi-out</i> spi <i>spi</i> } key <i>hex string</i> [replay timestamp]	(Optional) Set up visitor security association.

Verify Setup

To make sure Mobile IP is set up correctly, use any of the following commands in EXEC mode:

Command	Purpose
show ip mobile globals	Check home agent and foreign agent global settings.
show ip mobile host group	Check mobile node groups.
show ip mobile secure { host visitor foreign-agent home-agent } <i>addr</i>	Check security associations.
show ip mobile interface	Check advertisements on interfaces.

Monitor and Maintain Mobile IP

To monitor and maintain Mobile IP, use any of the following commands :

Command	Purpose
show ip mobile host	Check mobile node counters (home agent only).
show ip mobile binding	Check mobility bindings (home agent only).
show ip mobile tunnel	Check active tunnels.
show ip mobile visitor	Check visitor bindings (foreign agent only).
show ip route mobile	Check Mobile IP routes.
show ip mobile traffic	Check protocol statistics.
clear ip mobile traffic	Clear counters.
show ip mobile violation	Check security violations.

Command	Purpose
<code>debug ip mobile advertise</code>	Display advertisement information. ¹
<code>debug ip mobile host</code>	Display mobility events.

¹ Make sure ICMP Router Discovery Protocol (IRDP) is running on the interface.

Shutting Down Mobile IP

To shut down Mobile IP, use all of the following commands in global configuration mode:

Command	Purpose
<code>no ip mobile home-agent</code>	Disable home agent services.
<code>no ip mobile foreign-agent</code>	Disable foreign agent services.
<code>no router mobile</code>	Stop Mobile IP process.

Configuration Examples

This section contains the following configuration examples:

- Home Agent Configuration Example
- Home Agent Using AAA Server Example
- Foreign Agent Configuration Example

Home Agent Configuration Example

In the following example, the home agent has five mobile hosts on interface Ethernet1 (network 11.0.0.0) and ten on virtual network 10.0.0.0. There are two mobile node groups. Each mobile host has one security association. The home agent has an access-list to disable roaming capability by mobile host 11.0.0.5. The 11.0.0.0 group has a lifetime of 1 hour (3600 secs). The 10.0.0.0 group cannot roam in areas where the network is 13.0.0.0.

```
router mobile
!
! Define which hosts are permitted to roam
ip mobile home-agent broadcast roam-access 1
!
! Define a virtual network
ip mobile network 10.0.0.0 255.0.0.0
!
! Define which hosts are on the virtual network, and the care-of access list
ip mobile host 10.0.0.1 10.0.0.10 virtual-network 10.0.0.0 255.0.0.0 care-of-access 2
!
! Define which hosts are on Ethernet 1, with lifetime of one hour
ip mobile host 11.0.0.1 11.0.0.5 interface Ethernet1 lifetime 3600
```

```

!
! The next ten lines specify security associations for mobile hosts
! on virtual network 10.0.0.0
!
ip mobile secure host 10.0.0.1 spi 100 key hex 12345678123456781234567812345678
ip mobile secure host 10.0.0.2 spi 200 key hex 87654321876543218765432187654321
ip mobile secure host 10.0.0.3 spi 300 key hex 31323334353637383930313233343536
ip mobile secure host 10.0.0.4 spi 100 key hex 45678332353637383930313233343536
ip mobile secure host 10.0.0.5 spi 200 key hex 33343536313233343536373839303132
ip mobile secure host 10.0.0.6 spi 300 key hex 73839303313233343536313233343536
ip mobile secure host 10.0.0.7 spi 100 key hex 83930313233343536313233343536373
ip mobile secure host 10.0.0.8 spi 200 key hex 43536373839313233330313233343536
ip mobile secure host 10.0.0.9 spi 300 key hex 23334353631323334353637383930313
ip mobile secure host 10.0.0.10 spi 100 key hex 63738393132333435330313233343536
!
! The next five lines specify security associations for mobile hosts
! on Ethernet1
!
ip mobile secure host 11.0.0.1 spi 100 key hex 73839303313233343536313233343536
ip mobile secure host 11.0.0.2 spi 200 key hex 83930313233343536313233343536373
ip mobile secure host 11.0.0.3 spi 300 key hex 43536373839313233330313233343536
ip mobile secure host 11.0.0.4 spi 100 key hex 23334353631323334353637383930313
ip mobile secure host 11.0.0.5 spi 200 key hex 63738393132333435330313233343536
!
! Deny access for this host
access-list 1 deny 11.0.0.5
!
! Deny access to anyone on network 13.0.0.0 trying to register
access-list 2 deny 13.0.0.0

```

Home Agent Using AAA Server Example

In the following AAA server configuration, the home agent can use an AAA server for storing security associations. Mobile IP has been authorized using TACACS+ server to retrieve the security association information, which is used by the home agent to authenticate registrations. This format can be imported into a CiscoSecure server.

```

user = 20.0.0.1 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}

user = 20.0.0.2 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}

user = 20.0.0.3 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}

```

In the example above, user is the mobile node's IP address. The syntax for the security association is **spi#num = "string"**, where *string* is the rest of the **ip mobile secure {host | visitor | home-agent | foreign-agent} key hex string** command.

The following example shows how the home agent is configured to use the AAA server:

```
aaa new-model
aaa authorization ipmobile tacacs+
!
ip mobile home-agent
ip mobile network 20.0.0.0 255.0.0.0
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 255.0.0.0 aaa
!
tacacs-server host 1.2.3.4
tacacs-server key cisco
```

Foreign Agent Configuration Example

In the following example, the foreign agent is providing service on interface Ethernet1, advertising care-of address 68.0.0.31 and a lifetime of one hour.

```
interface Ethernet0
 ip address 68.0.0.31 255.0.0.0
interface Ethernet1
 ip address 67.0.0.31 255.0.0.0
 ip irdp
 ip irdp maxadvertinterval 10
 ip irdp minadvertinterval 7
 ip mobile foreign-service
 ip mobile registration-lifetime 3600
!
router mobile
!
 ip mobile foreign-agent care-of Ethernet0
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **aaa authorization ipmobile**
- **clear ip mobile binding**
- **clear ip mobile secure**
- **clear ip mobile traffic**
- **clear ip mobile visitor**
- **ip mobile foreign-agent**
- **ip mobile foreign-service**
- **ip mobile home-agent**
- **ip mobile host**
- **ip mobile virtual-network**
- **ip mobile prefix-length**
- **ip mobile registration-lifetime**
- **ip mobile secure**
- **ip mobile tunnel**

- **router mobile**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile host**
- **show ip mobile interface**
- **show ip mobile secure**
- **show ip mobile traffic**
- **show ip mobile tunnel**
- **show ip mobile violation**
- **show ip mobile visitor**
- **debug ip mobile advertise**
- **debug ip mobile host**

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. Use the **no** form of this command to remove authorization.

```
aaa authorization ipmobile {tacacs+ | radius}
no aaa authorization ipmobile {tacacs+ | radius}
```

Syntax Description

tacacs+	Use TACACS+.
radius	Use RADIUS.

Default

AAA is not used to retrieve security associations for authentication.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

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

Example

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
```

Related Commands

```
aaa new-model
ip mobile host
radius-server host
radius-server key
```

```
show ip mobile host
tacacs-server host
tacacs-server key
```

clear ip mobile binding

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

clear ip mobile binding [*addr*]

Syntax Description

addr (Optional) IP address. If not specified, mobility bindings will be removed for all addresses.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 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, since it can terminate any sessions used by the mobile node. The mobile node will need to be reregistered to continue roaming.

Example

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

show ip mobile binding

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

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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. It is possible that the security association on the router becomes 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.

Example

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 AAA server's security association changes:

```
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

ip mobile secure

clear ip mobile traffic

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

clear ip mobile traffic

Syntax Description

This command has no keywords or arguments.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 list and description of all counters.

Example

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

show ip mobile traffic

clear ip mobile visitor

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

```
clear ip mobile visitor [addr]
```

Syntax Description

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 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 since it can break any sessions the mobile node has.

After using this command, the visitor will need to reregister to continue roaming.

Example

The following example administratively stops visitor 10.0.0.1 from visiting:

```
clear ip mobile visitor 10.0.0.1
```

Related Commands

show ip mobile visitor

ip mobile foreign-agent

To enable foreign agent service, use the **ip mobile foreign-agent** global configuration command.

```
ip mobile foreign-agent [care-of interface | reg-wait secs]  
no ip mobile foreign-agent [care-of interface | reg-wait secs]
```

Syntax Description

care-of <i>interface</i>	IP address of interface. Sets the care-of address on the foreign agent. Multiple care-of addresses may be configured.
reg-wait <i>secs</i>	Pending registration expires after <i>secs</i> seconds if no reply is received. Range is 5 to 600. Default is 15.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 to display relevant information are shown in parentheses.

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, visitor is authenticated (**show ip mobile secure visitor**). The registration bitflag handling is described in Table 1 (**show ip mobile interface**). The foreign agent checks validity of the request. If successful, the foreign agent relays 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**). At most, five outstanding pending requests per mobile node are allowed. If the validity check fails, the foreign agent sends a reply with error code to the mobile node. Reply codes are listed in Table 2. Security violation is logged when visiting mobile node authentication fails (**show ip mobile violation**). The violation reasons are listed in Table 6.

When a registration reply comes in, the home agent is authenticated (**show ip mobile secure home-agent**) 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 will create or update 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 interface (of incoming request) is added to the routing table

(**show ip route mobile**), and an ARP entry added to avoid ARPing for the visiting mobile node. Visitor binding is removed (along with its associated host route, tunnel, and ARP entry) when registration lifetime expires or deregistration accepted.

When registration is denied, the foreign agent will remove request from pending registration table. The visitors table and timers are unaffected.

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent will deencapsulate the packet and forward it out its interface to the visiting mobile node, without ARPing.

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 **ip mobile foreign-service**.

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

Table 1 lists foreign agent registration bitflags.

Table 1 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 interface's network
M	Deny request. Minimum IP encapsulation not supported.
G	No operation. GRE encapsulation supported.
V	Deny request. Van Jacobson Header compression not supported.
T	Deny request. Reverse tunnel not supported.
reserved	Deny request. Reserved bit must not be set.

Table 2 lists foreign agent reply codes.

Table 2 Foreign Agent Reply Codes

Code	Reason
64	Reason unspecified.
65	Administratively prohibited.
66	Insufficient resource.
67	Mobile node failed authentication.
68	Home agent failed authentication.
69	Requested lifetime too long.
70	Poorly formed request.
71	Poorly formed reply.
72	Requested encapsulation unavailable.
73	Requested Van Jacobson Header compression unavailable.
74	Reverse tunnel unsupported.
80-95	ICMP Unreachable message code 0 - 15.

Example

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

debug ip mobile advertise
ip mobile foreign-service
show ip mobile globals

ip mobile foreign-service

To enable foreign agent service on an interface if care-of address(es) is configured, use the **ip mobile foreign-service** interface configuration command.

```
ip mobile foreign-service [home-access acl] [limit num] [registration-required]
no ip mobile foreign-service [home-access acl] [limit num] [registration-required]
```

Syntax Description

home-access <i>acl</i>	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99. You cannot use this keyword when you enable foreign agent service on a subinterface.
limit <i>num</i>	(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 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 co-located 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 using a co-located care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from this foreign agent's interface.

Table 3 lists the advertised bitflags.

Table 3 Foreign Agent Advertisement Bitflags

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

Example

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

show ip mobile interface

ip mobile home-agent

To enable and control home agent services on the router, use the **ip mobile home-agent** global configuration command. Use the **no** form of this command to disable these services.

```
ip mobile home-agent [broadcast] [care-of-access acl] [lifetime num] [replay sec]
[reverse-tunnel-off]
[roam-access acl] [suppress-unreachable]
no ip mobile home-agent [broadcast] [care-of-access acl] [lifetime num]
[replay sec] [reverse-tunnel-off] [roam-access acl] [suppress-unreachable]
```

Syntax Description

broadcast	Enables broadcast datagram routing. By default, broadcasting is disabled.
care-of-access <i>acl</i>	Controls which care-of addresses (in registration request) are permitted by the home agent. By default, all care-of addresses are permitted. The access list can be a string or number from 1 to 99.
lifetime <i>num</i>	(Optional) Specifies the global registration lifetime for mobile node. Note that this can be overridden by the individual mobile node configuration. Range is 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting lifetime greater than this value will still be accepted, but using this lifetime value.
replay <i>sec</i>	(Optional) Sets replay protection timestamp 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	(Optional) Controls which mobile nodes are permitted/denied to roam. By default, all specified mobile nodes can roam.
suppress-unreachable	(Optional) Disables sending ICMP Unreachable to source when mobile node on 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 is sent.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 **reverse-tunnel-off** affects registered mobile nodes too.

The home agent is responsible for processing registration requests from the mobile node and setting up tunnel and route to 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 router’s CPU. 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 mobile node’s security association is not configured. The latter occurs because the security association must be available for the MH authentication extension in the reply. If an security association exists for the foreign agent (IP source address or care-of address in request), foreign agent is authenticated, then 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 4) and sends a reply. Replay codes are listed in Table 5. A security violation is logged when foreign agent authentication, MH authentication or Identification verification fail. The violation reasons are listed in Table 6.

After registration is accepted, the home agent creates or updates the mobile node’s mobility binding, 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 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 ARP 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 IP header’s bit is also set. This allows Path MTU Discovery to set the tunnel’s MTU. Subsequent packets greater than tunnel’s MTU will be dropped and ICMP Datagram Too Big message sent to the source. If the home agent loses the route to the tunnel endpoint, the host route to mobile node will be removed from routing table until tunnel route is available. Packets destined for mobile node without a host route will be sent out the interface (home link) or to the virtual network (see suppress-unreachable parameter below). 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 4 describes how the home agent treats registrations with various bits set when authentication and identification passed.

Table 4 Home Agent Registration Bitflags

Bit Set	Registration Reply
S	Accept with code 1 (no simultaneous binding).
B	Accept. Broadcast may be enabled or disabled.
D	Accept. Tunnel endpoint is co-located care-of address.
M	Deny. Minimum IP encapsulation not supported.
G	Accept. GRE encapsulation supported.
V	Ignore. Van Jacobsen Header compression not supported.

Table 4 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 5 lists the home agent registration reply codes.

Table 5 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 unavailable.
139	Unsupported encapsulation.

Table 6 lists security violation codes.

Table 6 Security Violations

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

Example

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

show ip mobile globals

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

Syntax Description

<i>lower</i> [<i>upper</i>]	Range of mobile host or mobile node group IP addresses.
interface <i>name</i>	Mobile node belongs to specified <i>interface</i> .
virtual-network <i>net mask</i>	The wireless mobile node resides in the virtual network created using the ip mobile network command.
aaa	(Optional) Retrieve security associations from AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Store security associations in memory after retrieval.
care-of-access <i>acl</i>	(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 <i>num</i>	(Optional) Lifetime in seconds. The lifetime for each mobile node (group) can be set to override the global value. Range is 3 to 65535.

Default

No host is configured.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

This 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 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 registration request arrives or the **clear ip mobile secure** command is entered.

All host must have security associations for registration authentication. Mobile nodes may have more than one security association. The calculations below for memory consumption are based on the assumption of one security association per mobile node.

Security associations can be stored three ways:

- 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 has advantages and disadvantages, which are described in Table 7.

Table 7 Methods for Storing Security Associations

Storage Method	Advantage	Disadvantage
On the router.	<ul style="list-style-type: none"> • Security association is in router memory, resulting in fast lookup • For home agents supporting less than ~1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router). 	<ul style="list-style-type: none"> • Router's NVRAM 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.	<ul style="list-style-type: none"> • Central admin/storage of security association on AAA server. • If keys changes constantly, admin 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. 	<ul style="list-style-type: none"> • Require network to retrieve security association, slower, 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 is not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).
On the AAA server, retrieve and store security association.	<ul style="list-style-type: none"> • 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 1/2 MB. • If keys remains fairly constant, once security associations are loaded, home agent authenticates as fast as the first method. • Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory. 	<ul style="list-style-type: none"> • If keys change on the AAA server after mobile node registered, then need to clear ip mobile secure to clear and load in new security association from AAA, else router's security association is stale.

Example

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

aaa authorization ipmobile
ip mobile secure
show ip mobile host

ip mobile virtual-network

To insert a virtual network for non-homed mobile nodes in the routing table, use the **ip mobile virtual-network** global configuration command. To remove a virtual network from the routing table, use the **no** form of this command.

```
ip mobile virtual-network addr mask  
no ip mobile virtual-network addr mask
```

Syntax Description

<i>addr</i>	IP address of virtual network.
<i>mask</i>	Network mask associated with the IP address of the virtual network.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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.

This command is unnecessary for mobile nodes that reside on the network of the home agent's interface. The connected network already exists.

Example

The following example adds the virtual network 20.0.0.0 to the routing table:

```
ip mobile virtual-network 20.0.0.0 255.255.0.0
```

Related Commands

```
ip mobile host  
redistribute mobile
```

ip mobile prefix-length

To append the prefix-lengths 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 keywords or arguments.

Default

The prefix-lengths extension is not appended

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

The prefix-lengths 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-lengths extension to determine whether or not 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.

Example

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

```
ip mobile prefix-length
```

Related Commands

show ip mobile interface

ip mobile registration-lifetime

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

```
ip mobile registration-lifetime sec
```

Syntax Description

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

Default

36000 seconds

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

Example

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

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

Related Commands

show ip mobile interface

ip mobile secure

To specify the mobility security associations for mobile host, visitor, home agent, and foreign agent, use the **ip mobile secure** global configuration command.

```
ip mobile secure {host | visitor | home-agent | foreign-agent} addr {inbound-spi spi-in
outbound-spi spi-out | spi spi} key hex string [replay timestamp [num] algorithm md5
mode prefix-suffix]
```

```
no ip mobile secure {host | visitor | home-agent | foreign-agent} addr {inbound-spi spi-in
outbound-spi spi-out | spi spi} key hex string [replay timestamp [num] algorithm md5
mode prefix-suffix]
```

Syntax Description

host	Mobile host's security association on the home agent.
visitor	Mobile visitor's security association on the foreign agent.
home-agent	Remote home agent's security association on the foreign agent.
foreign-agent	Remote foreign agent's security association on the home agent.
<i>addr</i>	IP address of host, visitor or mobility agent.
inbound-spi <i>spi-in</i>	Security parameter index used for authenticating inbound registration packets. Range is 0x100 to 0xffffffff.
outbound-spi <i>spi-out</i>	Security parameter index used for calculating the authenticator in outbound registration packets. Range is 0x100 to 0xffffffff.
spi <i>spi</i>	Bidirectional SPI. Range is 0x100 to 0xffffffff.
key <i>hex string</i>	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Replay protection used on registration packets.
timestamp	(Optional) Used to validate incoming packets to ensure that they are not being "replayed" by a spoofer using timestamp method.
<i>num</i>	(Optional) Number of seconds. Registration is valid if received within the specified time. This means sender and receiver are in time sync (NTP may be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
mode	(Optional) Mode used to authenticate during registration.
prefix-suffix	(Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest.

Default

No security association is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

The security association consists of the entity address, SPI, key, replay protection method, authentication algorithm and mode.

The security parameter index (SPI) is the 4-byte index which selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout and IP address.

On a home agent, the mobile host's security association is mandatory for mobile host authentication. If desired, configure a foreign agent security association on your home agent. On a foreign agent, the visiting mobile host's security association and home agent's security association are optional. Multiple security associations for each entity may be configured.

If registration fails because the **timestamp** value is out of bounds, the home agent's timestamp is returned so the mobile node can reregister with the timestamp value closer to the home agent's, if desired.

Note NTP may be used to sync time for all parties.

Example

The following example shows mobile node 20.0.0.1 which has a key that is generated by MD5 hash of the string 'mykey':

```
ip mobile secure host 20.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

ip mobile host
ntp server
show ip mobile secure

ip mobile tunnel

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

```
ip mobile tunnel {route-cache | path-mtu-discovery [age-timer {minutes | infinite}]}
```

Syntax Description

route-cache	Sets tunnels to default or process switching mode.
path-mtu-discovery	Specifies when to expire the tunnel MTU if set by Path MTU Discovery.
age-timer <i>minutes</i>	(Optional) Time interval (in minutes) after which the tunnel re-estimates the Path MTU.
infinite	Turns off the age timer.

Default

Disabled.

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

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

The discovered tunnel MTU should be aged out periodically to possibly recover from case where sub-optimum MTU existed at time of discovery. It is reset to the outgoing interface's MTU.

Example

The following example sets the discovered tunnel MTU to expire in ten minutes:

```
ip mobile tunnel reset-mtu-time 600
```

Related Commands

show ip mobile tunnel

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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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 will remove all related configuration commands, both global and interface.

Example

The following example enables Mobile IP:

```
router mobile
```

Related Commands

show ip mobile globals
show ip protocol
show process

show ip mobile binding

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

show ip mobile binding [*addr*]

Syntax Description

addr (Optional) IP address of mobile node.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

Sample Display

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 8 describes significant fields shown in the display.

Table 8 Show IP Mobile Binding Display Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Mobile node's home IP address.
Care-of Addr	Mobile node's care-of-address.
Src Addr	IP source address of the Registration Request as received by the home agent. Will be either a mobile node's co-located care-of address 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. Upper case characters denote bit set. See Table 4 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.

Table 8 Show IP Mobile Binding Display Field Descriptions (continued)

Field	Description
Tunnel	The tunnel used by mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. Default is IPIP encapsulation, otherwise GRE will be displayed in Routing Options.
Routing Options	Routing options list all home agent-accepted services. For example, V bit may have been request by mobile node (shown in Flags field), but 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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

This command shows which services are provided by the home agent and/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), not at the global foreign agent level.

Sample Display

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 9 describes significant fields shown in the display.

Table 9 Show IP Mobile Globals Display 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.

Table 9 Show IP Mobile Globals Display Field Descriptions (continued)

Field	Description
Broadcast	Broadcast enabled or disabled.
Reverse tunnel	Reverse tunnel enabled or disabled.
ICMP Unreachable	Send ICMP Unreachable enabled or disabled for virtual network.
Virtual networks	List virtual networks serviced by home agent. Displayed if defined.
Foreign Agent	
Care-of addresses advertised	List care-of addresses (interface is up or down). Displayed if defined.
Mobility Agent	
Number of interfaces providing service	See the ip mobile interface command for more information on advertising. Agent advertisements are sent when IRDP is enabled.
Encapsulation supported	IPIP and GRE.
Tunnel fast switching	Tunnel fast switching 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 [*addr* | **interface** *int* | **network** *addr* | **group**]

Syntax Description

<i>addr</i>	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
interface <i>int</i>	(Optional) All mobile nodes whose home network is on this interface.
network <i>addr</i>	(Optional) All mobile nodes residing on this network or virtual network.
group	(Optional) All mobile node groups configured using the ip mobile host command.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

Sample Displays

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)'
```

Table 10 describes significant fields shown in the display.

Table 10 Show IP Mobile Host Display Field Descriptions

Field	Description
IP address	mobile node's home IP address
Allowed lifetime	mobile node's allowed lifetime. By default, it is set to the global lifetime (ip mobile home-agent lifetime). Setting this lifetime will override global value.
Roaming status	When the mobile node is registered, the roaming status is '- Registered -', otherwise, '- Unregistered -'. Use show ip mobile binding for more information when user is registered.
Home link	Either on an interface or virtual network.

Table 10 Show IP Mobile Host Display Field Descriptions (continued)

Field	Description
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 4 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 tunnelled to mobile node.
Reverse tunnel from MN	Number of packets and bytes reverse tunnelled 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 11 describes significant fields shown in the display.

Table 11 Show IP Mobile Host Group Display Field Descriptions

Field	Description
IP address	Mobile host IP address or grouping of addresses.
Home link	Either on interface or virtual network.
Care-of ACL	Care-of address access-list.
Security association	Either on router or AAA server.
Allowed lifetime	Allowed lifetime for mobile host or group.

Related Commands

show ip mobile binding

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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

Sample Display

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 12 describes significant fields shown in the display.

Table 12 Show IP Mobile Interface Display Field Descriptions

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

Related Commands

ip mobile foreign-agent
ip mobile host
ip mobile prefix-length
show ip irdp

show ip mobile secure

To display the mobility security associations for 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} addr
```

Syntax Description

addr IP address.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

Multiple security associations may exist for each entity.

Sample Display

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 13 describes significant fields shown in the display.

Table 13 Show IP Mobile Secure Display Field Descriptions

Field	Description
20.0.0.1	IP address.
In/Out SPI	The SPI is the 4-byte opaque index within the Mobility Security Association which 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 sending a response.
MD5	Authentication algorithm.
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 Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

Sample Display

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
  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 14 describes significant fields shown in the display.

Table 14 Show IP Mobile Traffic Display 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 mobility agent in response to mobile node solicitations.
Home Agent	
Register requests	Total number of Registration Requests received by 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 home agent (Code 0).
No simultaneous binding	Total number of Registration Requests accepted by home agent—simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of Registration Requests denied by home agent.
Ignored	Total number of Registration Requests ignored by home agent.
Unspecified	Total number of Registration Requests denied by home agent—reason unspecified (Code 128).
Unknown HA	Total number of Registration Requests denied by home agent—unknown home agent address (Code 136).
Administrative prohibited	Total number of Registration Requests denied by home agent—administratively prohibited (Code 129).
No resource	Total number of Registration Requests denied by home agent—insufficient resources (Code 130).
Authentication failed MN	Total number of Registration Requests denied by home agent—mobile node failed authentication (Code 131).
Authentication failed FA	Total number of Registration Requests denied by home agent—foreign agent failed authentication (Code 132).
Bad identification	Total number of Registration Requests denied by home agent—identification mismatch (Code 133).
Bad request form	Total number of Registration Requests denied by home agent—poorly formed request (Code 134).
Unavailable encapsulation	Total number of Registration Requests denied by home agent—unavailable encapsulation (Code 139).
Unavailable reverse tunnel	Total number of Registration Requests denied by home agent—reverse tunnel unavailable (Code 137).
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 foreign agent.
Forwarded	Total number of Registration Requests relayed to home agent by foreign agent.

Table 14 Show IP Mobile Traffic Display Field Descriptions (continued)

Field	Description
Denied	Total number of Registration Request denied by foreign agent.
Ignored	Total number of Registration Request ignored by foreign agent.
Unspecified	Total number of Registration Requests denied by foreign agent—reason unspecified (Code 64).
HA unreachable	Total number of Registration Requests denied by foreign agent—home agent unreachable (Codes 80-95).
Administrative prohibited	Total number of Registration Requests denied by foreign agent— administratively prohibited (Code 65)
No resource	Total number of Registration Requests denied by home agent— insufficient resources (Code 66).
Bad lifetime	Total number of Registration Requests denied by foreign agent— requested lifetime too long (Code 69).
Bad request form	Total number of Registration Requests denied by home agent—poorly formed request (Code 70).
Unavailable encapsulation	Total number of Registration Requests denied by home agent— unavailable encapsulation (Code 72).
Unavailable compression	Total number of Registration Requests denied by foreign agent— requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of Registration Requests denied by home agent—reverse tunnel unavailable (Code 74).
Replies in	Total number of well-formed Registration Replies received by foreign agent.
Forwarded	Total number of valid Registration Replies relayed to the mobile node by foreign agent.
Bad	Total number of Registration Replies denied by foreign agent—poorly formed reply (Code 71).
Ignored	Total number of Registration Replies ignored by foreign agent.
Authentication failed MN	Total number of Registration Requests denied by home agent—mobile node failed authentication (Code 67).
Authentication failed HA	Total number of Registration Replies denied by 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 Descriptio

interface (Optional) Display a particular tunnel interface. The argument *interface* is Tunnelx.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

Sample Display

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 15 describes significant fields shown in the display.

Table 15 Show IP Mobile Tunnel Display 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.
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.

Table 15 Show IP Mobile Tunnel Display Field Descriptions (continued)

Field	Description
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

show ip mobile binding
show ip mobile host
show ip mobile visitor

show ip mobile violation

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

show ip mobile violation [*addr*]

Syntax Description

addr (Optional) Display violations from a specific IP address.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

The most recent violation is saved for all mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. 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.

Sample Display

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 16 describes significant fields shown in the display.

Table 16 Show IP Mobile Violation Display Field Descriptions

Field	Description
20.0.0.1	Violator's IP address.
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 16 Show IP Mobile Violation Display 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 14 for list of error codes.
Reason	Reason for the most recent security violation for this peer. Possible reasons are: <ul style="list-style-type: none">• No mobility security association• Bad authenticator• Bad identifier• Bad SPI• Missing security extension• Other

show ip mobile visitor

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

```
show ip mobile visitor [pending] [addr]
```

Syntax Description

pending (Optional) Pending registration table.

addr (Optional) IP address.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

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

Sample Display

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

```
Router# show ip mobile visitor
Mobile Visitor List:

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 17 describes significant fields shown in the display.

Table 17 Show IP Mobile Visitor Display Field Descriptions

Field	Description
20.0.0.1	Visitor’s home IP address.
Interface	Name of interface.
MAC addr	Visitor’s MAC address.
IP src	Source IP address of visitor’s Registration Request.
IP dest	Destination IP address of visitor’s Registration Request. When foreign agent sends a reply to visitor, the IP source address is set to this address, unless multicast or broadcast. In this case it is set to output interface’s IP address.
UDP src port	Source UDP port of visitor’s Registration Request.
HA addr	Home agent IP address for that visiting mobile node.

Table 17 Show IP Mobile Visitor Display Field Descriptions (continued)

Field	Description
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 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. Default is IPIP encapsulation, otherwise GRE will be displayed in Routing Options.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by mobile node. Possible options are: <ul style="list-style-type: none">• (S) Mult-binding• (B) Broadcast• (D) Direct-to-MN• (M) MinIP• (G) GRE• (V) VJH-compress• (T) Reverse-tunnel

Debug Commands

debug ip mobile advertise

Use the **debug ip mobile advertise EXEC** command to display advertisement information.

debug ip mobile advertise

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

Sample Display

The following is sample output from the **debug ip mobile advertise** command:

```
Router# debug ip mobile advertise
MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400 (rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8 )
```

Table 18 describes significant fields shown in the display.

Table 18 Debug IP Mobile Advertise Field Descriptions

Field	Description
type	Type of advertisement.
len	Length of extension in bytes.
seq	Sequence number of this advertisement.
lifetime	Lifetime in seconds.
flags	Capital letters represent bits that are set, lower case letters represent unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.

debug ip mobile host

Use the **debug ip mobile host** EXEC command to display IP mobility events.

debug ip mobile host *acl*

Syntax Description

acl (Optional) Access list.

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0(1)T.

Sample Display

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

```
Router# debug ip mobile host
MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA
68.0.0.31 HA 66.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6

MobileIP: HA sent reply to MN 20.0.0.6
```

