Cisco Mobile Wireless Home Agent

Feature History

Release	Modification
12.2(8)BY	This feature was introduced on the Cisco 7200 Series Router.
12.2(8)ZB	This feature was introduced on the Cisco Catalyst 6500 Switch.

This feature module describes the Cisco Mobile Wireless Home Agent. It includes information on the features and functions of the product, supported platforms, related documents, and configuration tasks.

This document includes the following sections:

Feature Overview

Cisco's Mobile Wireless Packet Data Solution includes the Packet Data Serving Node (PDSN) with foreign agent functionality (FA), the Cisco Mobile Wireless Home Agent (HA), AAA servers, and several other security products and features. The solution is standards compliant, and is designed to meet the needs of mobile wireless industry as it transitions towards third-generation cellular data services.

The Home Agent is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic sent to the terminal is routed via the Home Agent. With reverse tunneling, traffic from the terminal is also routed via the Home Agent.

A PDSN provides access to the Internet, intranets, and Wireless Application Protocol (WAP) servers for mobile stations using a Code Division Multiple Access 2000 (CDMA2000) Radio Access Network (RAN). The Cisco PDSN is a Cisco IOS software feature that runs on Cisco 7200 routers and Catalyst 6500 switches, and acts as an access gateway for Simple IP and Mobile IP stations. It provides foreign agent (FA) support and packet transport for virtual private networking (VPN). It also acts as an Authentication, Authorization, and Accounting (AAA) client.

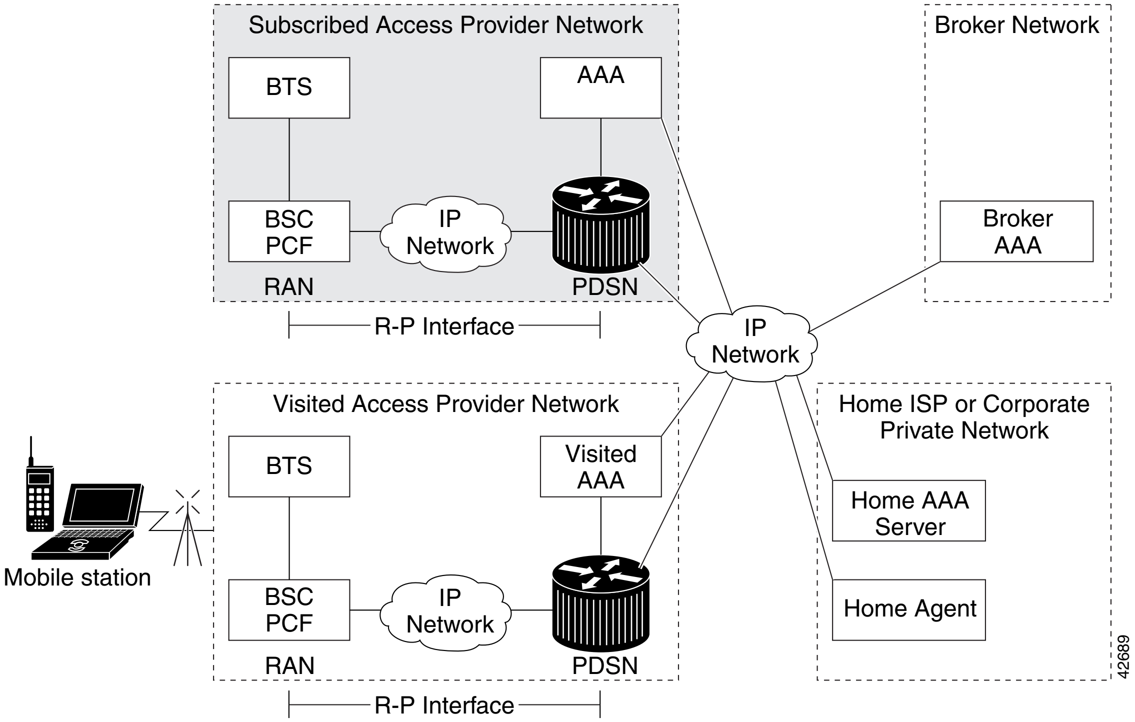
The Cisco PDSN, and the Cisco Home Agent support all relevant 3GPP2 standards, including those that define the overall structure of a CDMA2000 network, and the interfaces between radio components, the Home Agent, and the PDSN.

System Overview

CDMA is one of the standards for mobile communication. A typical CDMA2000 network includes terminal equipment, mobile termination, base transceiver stations (BTSs), base station controllers (BSCs), PDSNs, and other CDMA network and data network entities. The PDSN is the interface between a BSC and a network router.

Figure 1 illustrates the relationship of the components of a typical CDMA2000 network, including a PDSN and a Home Agent. In this illustration, a roaming mobile station user is receiving data services from a visited access provider network, rather than from the mobile station user's subscribed access provider network.

Figure 1 The CDMA Network



As the illustration shows, the mobile station, which must support either Simple IP or Mobile IP, connects to a radio tower and BTS. The BTS connects to a BSC, which contains a component called the Packet Control Function (PCF). The PCF communicates with the Cisco PDSN through an A10/A11 interface. The A10 interface is for user data and the A11 interface is for control messages. This interface is also known as the RAN-to-PDSN (R-P) interface. For the Cisco Home Agent Release 1.2, you must use a Fast Ethernet (FE) interface as the R-P interface on the 7200 platform, and a Giga Ethernet (GE) interface on the MWAM platform.

The IP networking between the PDSN and external data networks is through the PDSN-to-intranet/Internet (P_i) interface. For the Cisco Home Agent Release 1.2, you can use either an FE or GE interface as the P_i interface.

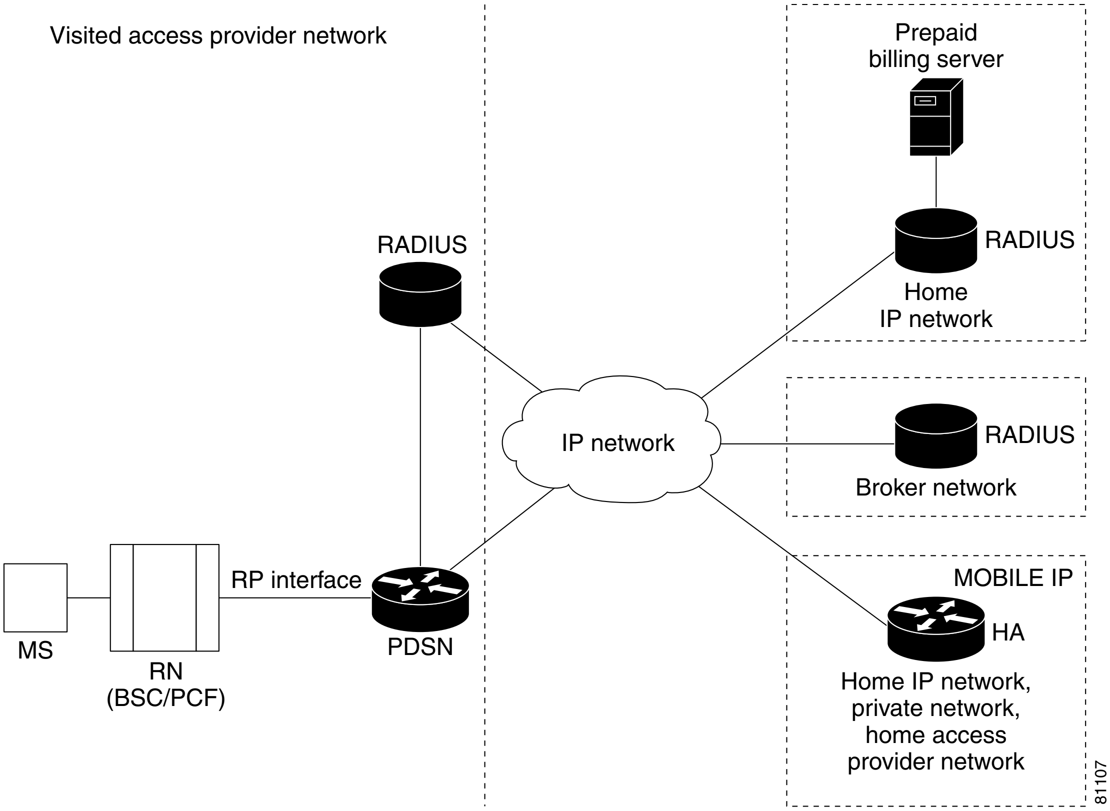
For “back office” connectivity, such as connections to a AAA server, the interface is media independent. Any of the interfaces supported on the Cisco 7206 can be used to connect to these types of services, but Cisco recommends that you use either an FE or GE interface as the P_i interface.

Cisco Home Agent Network

Figure 2 illustrates the functional elements in a typical CDMA2000 packet data system, and Cisco products that are currently available to support this solution. The Home Agent, in conjunction with the PDSN/Foreign Agent, allows a mobile station with Mobile IP client function, to access the internet or corporate intranet using Mobile IP-based service access. Mobile IP extends user mobility beyond the coverage area of the current, serving PDSN/Foreign Agent. If another PDSN is allocated to the call(following a handoff), the target PDSN performs a Mobile IP registration with the Home Agent; this ensures that the same home address is allocated to the mobile. Additionally, clients without a Mobile IP client can also make use of these services by using the Proxy Mobile IP capability provided by the PDSN

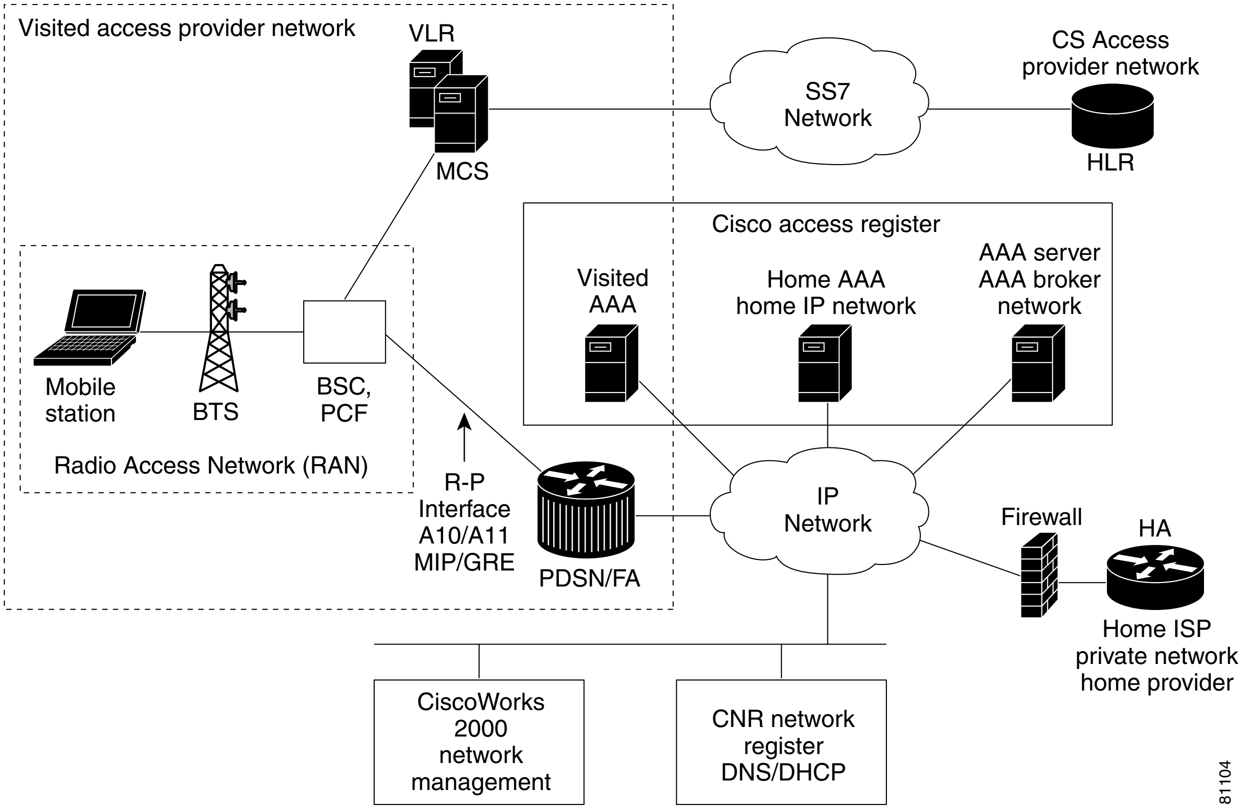
The Home Agent, then, is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic is routed via the home agent, and the home agent also provides Proxy ARP services. In the case of reverse tunneling, traffic from the terminal is also routed via the Home Agent.

Figure 2 Cisco Products for CDMA2000 Packet Data Services Solution



For Mobile IP services, the Home Agent would typically be located within an ISP network, or within a corporate domain. However, many ISPs and/or corporate entities may not be ready to provision Home Agents by the time service providers begin rollout of third-generation packet data services. As a remedy, Access service providers could provision Home Agents within their own domains, and then forward packets to ISPs or corporate domains via VPDN services. Figure 3 illustrates the functional elements that are necessary to support Mobile IP-based service access when the Home Agent is located in the service provider domain.

Figure 3 Cisco Mobile IP Based Service Access With Home Agent in Service Provider Network


Visited access provider network
VLR
MCS
SS7 Network
CS Access provider network
HLR
Cisco access register
Visited AAA
Home AAA home IP network
AAA server AAA broker network
Mobile station
BTS
BSC, PCF
Radio Access Network (RAN)
R-P Interface A10/A11 MIP/GRE
PDSN/FA
IP Network
Firewall
HA
Home ISP private network home provider
CiscoWorks 2000 network management
CNR network register DNS/DHCP
81104

For Mobile IP and Proxy-Mobile IP types of access, these solutions allow a mobile user to roam within and beyond it's service provider boundaries, while always being reachable and addressable via the IP address assigned on initial session establishment. Details of Mobile IP and Proxy Mobile IP Services can be found in Packet Data Services.

Packet Data Services

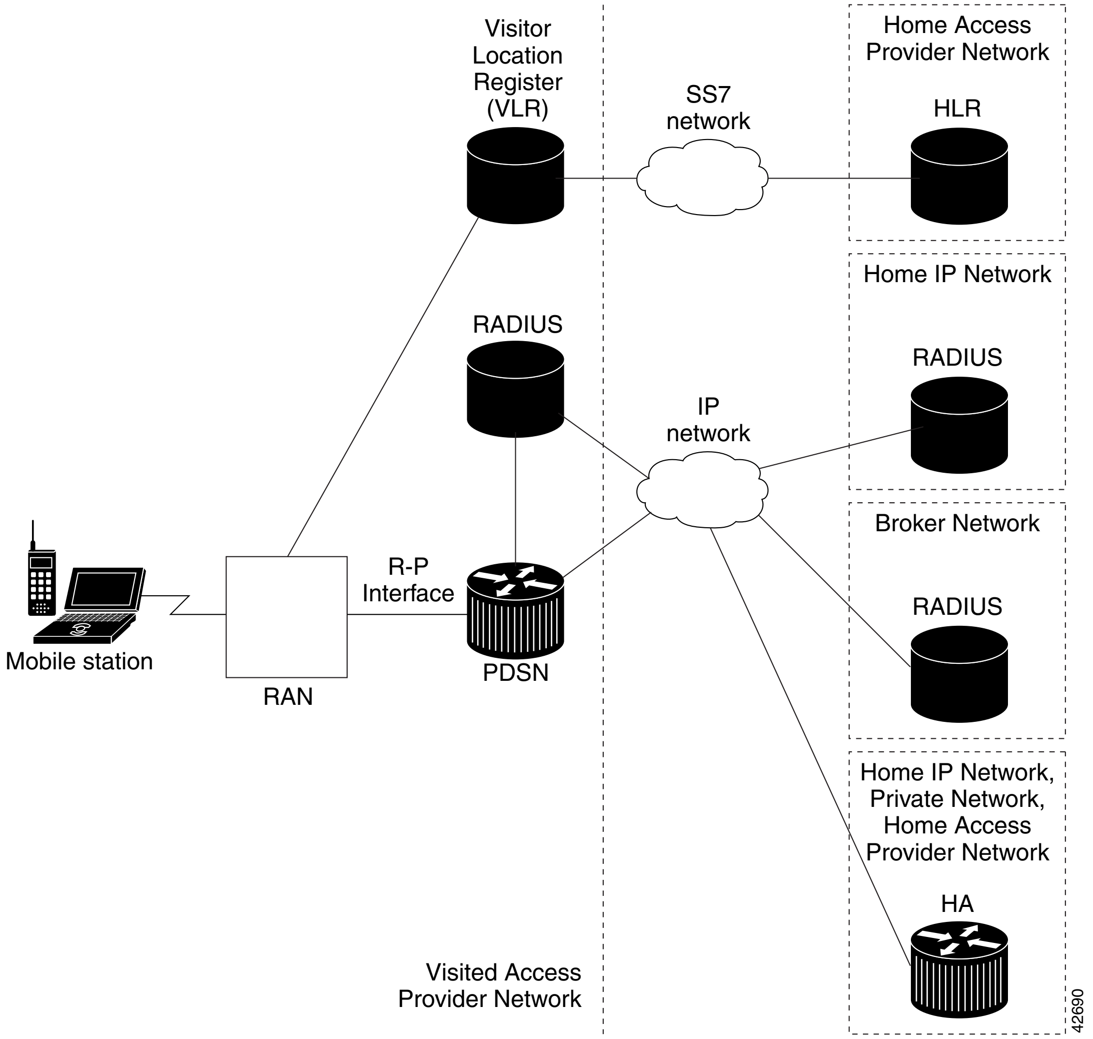
In the context of a CDMA2000 network, the Cisco Home Agent supports two types of packet data services: Mobile-IP and Proxy Mobile-IP services. From the perspective of the Cisco Home Agent, these services are identical.

Cisco Mobile IP Service

With Mobile IP, the mobile station can roam beyond the coverage area of a given PDSN and still maintain the same IP address and application-level connections.

Figure 4 shows the placement of the Cisco Home Agent in a Mobile IP scenario.

Figure 4 CDMA Network —Mobile IP Scenario


Visitor Location Register (VLR)
SS7 network
Home Access Provider Network
HLR
Home IP Network
RADIUS
RADIUS
IP network
Broker Network
RADIUS
R-P Interface
Mobile station
RAN
PDSN
Home IP Network, Private Network, Home Access Provider Network
HA
Visited Access Provider Network
42690

The communication process occurs in the following order:

1. The mobile station registers with its Home Agent (HA) through a FA. In the context of the CDMA2000 network, the FA is the Cisco PDSN.
2. The Cisco HA accepts the registration, assigns an IP address to the mobile station, and creates a tunnel to the FA. The resulting configuration is a PPP link between the mobile station and the FA (or PDSN), and an IP-in-IP or GRE tunnel between the FA and the HA.

   As part of the registration process, the Cisco HA creates a binding table entry to associate the mobile station's home address with its *care of* address.

Note While away from home (from the HA's perspective), the mobile station is associated with a care-of address. This address identifies the mobile station's current, topological point of attachment to the Internet, and is used to route packets to the mobile station. Either a foreign agent's address, or an address obtained by the mobile station for use while it is present on a particular network, is used as the care-of address. In the case of the Cisco Home Agent, the Care-of-Address is always an address of the Foreign Agent

3. The HA advertises network reachability to the mobile station, and tunnels datagrams to the mobile station at its current location.
4. The mobile station sends packets with its home address as the source IP address.
5. Packets destined for the mobile station go through the HA, which tunnels them to the PDSN. From there they are sent to the mobile station using the care-of address. This scenario also applies to reverse tunneling, which allows traffic moving from the mobile to the network to pass through the Home Agent.
6. When the PPP link is handed off to a new PDSN, the link is re-negotiated and the Mobile IP registration is renewed.
7. The HA updates its binding table with the new care-of address.

Note For more information about Mobile IP, refer to the Cisco IOS Release 12.2 documentation modules *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command Reference.* RFC2002 describes the specification in detail. TIA/EIA/IS-835-B also defines how Mobile IP is realized in the Home Agent.

Cisco Proxy Mobile IP Service

Currently, there is a lack of commercially-available Mobile IP client software. Conversely, PPP, which is widely used to connect to an Internet Service Provider (ISP), is ubiquitous in IP devices. As an alternative to Mobile IP, you can use Cisco's proxy Mobile IP feature. This capability of the Cisco PDSN, which is integrated with PPP, enables the PDSN, functioning as a Foreign Agent, and a Mobile IP client, to provide mobility to authenticated PPP users.

The communication process occurs in the following order:

1. The Cisco PDSN (acting as an FA) collects and sends mobile station authentication information to the AAA server (specifically, PPP authentication information).
2. If the mobile station is successfully authorized to use Cisco PDSN Proxy Mobile IP service, the AAA server returns the registration data and an HA address.
3. The FA uses this information, and other data, to generate a Registration Request (RRQ) on behalf of the mobile station, and sends it to the Cisco HA.
4. If the registration is successful, the Cisco HA sends a registration reply (RRP) that contains an IP address to the FA.
5. The FA assigns the IP address (received in the RRP) to the mobile station, using IPCP.
6. A tunnel is established between the Cisco HA and the FA/PDSN. If reverse tunneling is enabled, the tunnel carries traffic to and from the mobile station.

Note The PDSN takes care of all Mobile IP re-registrations on behalf of the Proxy-MIP client.

Features

This section describes the following key features of the Cisco PDSN/HA:

Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7200 router, or 6500 switch configured as a Home Agent, supports the following Home Agent-specific features:

- Support for static IP Addresses assignment
  - Public IP addresses
  - Private IP addresses
- Support for dynamic IP Addresses assignment
  - Public IP addresses
  - Private IP addresses
- Multiple flows for different NAIs using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge extensions in RFC 3012 - bis 03
  - Mobile IP Agent Advertisement Challenge Extension
  - MN-FA Challenge Extension
  - Generalized Mobile IP Authentication Extension, which specifies the format for the MN-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
  - MN-HA Authentication Extension
  - FA-HA Authentication Extension
- Reverse Tunneling, RFC 2344
- Mobile NAI Extension, RFC 2794

- Multiple tunneling Modes between FA and HA
  - IP-in-IP Encapsulation, RFC 2003
  - Generic Route Encapsulation, RFC 2784
- Binding Update message for managing stale bindings
- Home Agent redundancy support
- Mobile IP Extensions specified in RFC 3220
  - Authentication requiring the use of SPI. section 3.2
- Support for Packet Filtering
  - Input access lists
  - Output access lists
- Support for proxy and gratuitous ARP
- Mobile IP registration replay protection using timestamps. Nonce-based replay protection is not supported

Benefits

The following list identifies some of the key benefits that the Cisco Home Agent provides:

- Supports static and dynamic IP address allocation.
- Attracts, intercepts and tunnels datagrams for delivery to the MS.
- Receives tunneled datagrams from the MS (through the FA), un-encapsulates them, and delivers them to the Corresponding Node (CN).

Note Depending on the configuration, reverse tunneling may, or may not, be used by the MS, and may or may not be accepted by the HA.

- Presents a unique routable address to the network.
- Supports ingress and egress filtering.
- Maintains binding information for each registered MS containing an association of CoA with home address, NAI, and security key(s) together with the lifetime of that association.
- Receives and processes registration renewal requests within the bounds of the Mobile IP registration lifetime timer, either from the MS (via the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Receives and processes de-registration requests either from the MS (via the FA in the Mobile IP case), or from the FA (in the Proxy Mobile IP case).
- Maintains a subscriber database that is stored locally or retrieved from an external source.
- Sends a binding update to the source PDSN under hand-off conditions when suitably configured.
- Supports dynamic HA assignment.

The Home Agent

The Home Agent (HA) maintains mobile user registrations and tunnels packets destined for the mobile to the PDSN/FA. It supports reverse tunneling, and can securely tunnel packets to the PDSN using IPSec. Broadcast packets are not tunneled. Additionally, the HA performs dynamic home address assignment for the mobile. Home address assignment can be from address pools configured locally, through either DHCP server access, or from the AAA server.

The Cisco HA supports proxy Mobile IP functionality, and is available on the 7200 and 6500 series platforms. A 7200-based Cisco HA supports up to 262,000 mobile bindings, can process 100 bindings per second, and is RFC 2002, 2003, 2005 and 2006 compliant.

A 6500-based Cisco HA with 2 MWAM cards housing 5 active HA images and 5 standby images, would support the above figures multiplied by 5.

For more information on Mobile IP as it relates to Home Agent configuration tasks, please refer to the following url:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm.

Dynamic Home Agent Assignment

The Home Agent can be dynamically assigned in a CDMA2000 network when the following qualifications exist.

The first qualification is that the Home Agent receives a mobile IP Registration Request with a value of **0.0.0.0** in the “Home Agent” field. Upon authentication/authorization, the PDSN retrieves the HA’s IP address. The PDSN then uses this address to forward the Registration Request to the HA, but does not update the actual HA address field in the Registration Request.

The Home Agent sends a Registration Reply, and places it’s own IP address in the “Home Agent” field. At this point, any re-registration request that are received would contain the Home Agent’s IP address in the “Home Agent” field.

The second qualification is a function of the PDSN/Foreign Agent, and is included here for completeness. In this case, a AAA server is used to perform the dynamic Home Agent assignment function. Depending on network topology, either the local-AAA, or the home-AAA server would perform this function. When an access service provider is also serving as an ISP, Home Agents would be located in the access provider network. In this service scenario, a local-AAA server would perform Home Agent assignment function. Based on the user NAI received in the access request message, the AAA server would return a elected Home Agent’s address in an access reply message to the PDSN.

A pool of Home Agent addresses is typically configured at the AAA server. For the access provider serving as an ISP, multiple pools of Home Agents could be configured at the local AAA server; however, this depends on SLAs with the domains for which Mobile IP, or proxy-Mobile IP services are supported. You can configure the Home Agent selection procedure at the AAA server, using either a round-robin or a hashing algorithm over user NAI selection criteria.

The PDSN/Foreign Agent sends the Registration Request to the Home Agent; however, there is no IP address in the HA field of the MIP RRQ (it is 0.0.0.0). When the PDSN retrieves the IP address from AAA, it does not update the MIP RRQ; instead, it forwards the RRQ to the HA address retrieved. The PDSN cannot alter the MIP RRQ because it does not know the MN-HA SPI, and key value (which contains the IP address of the Home Agent in the “Home Agent” field). Depending on network topology, either the local-AAA, or the home-AAA server would perform this function. In situations where the Home Agents are located in the access provider network, the local-AAA server would perform Home

Agent assignment function. Additionally, multiple pools of Home Agents could be configured at the local-AAA server, depending on SLAs with the domains for which Mobile IP or proxy-Mobile IP services are supported.

Home Agent Redundancy

Cisco Home Agents can be configured to provide 1:1 redundancy. Two Home Agents are configured in hot-standby mode, based on Cisco Hot Standby Routing Protocol (HSRP in RFC 2281).[1] This enables the active Home Agent to continually copy mobile session-related information to the standby Home Agent, and maintains synchronized state information at both Home Agents. In case an active Home Agent fails, the standby home agent takes over without service disruption.

During the Mobile IP registration process, an HA creates a mobility binding table that maps the home IP address of an MN to the current care-of address of the MN. If the HA fails, the mobility binding table will be lost and all MNs registered with the HA will lose their connectivity. To reduce the impact of an HA failure, Cisco IOS software supports the HA redundancy feature.

Note On 6500-based configurations, the backup Home Agent image is configured on a different MWAM card to the primary.

The functionality of HA redundancy runs on top of the Hot Standby Router Protocol (HSRP). HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic will immediately and transparently recover from failures.

HSRP Groups

Before configuring HA redundancy, you must understand the concept of HSRP groups.

An HSRP group is composed of two or more routers that share an IP address and a MAC (Layer 2) address and act as a single virtual router. For example, your Mobile IP topology can include one active HA and one or more standby HAs that the rest of the topology view as a single virtual HA.

You must define certain HSRP group attributes on the interfaces of the HAs so that Mobile IP can implement the redundancy. You can use the groups to provide redundancy for MNs with a home link on either the interface of the group (a physical network) or on virtual networks. Virtual networks are logical circuits that are programmed and share a common physical infrastructure.

How HA Redundancy Works

The HA redundancy feature enables you to configure an active HA and one or more standby HAs. The HAs in a redundancy group may be configured in an Active HA-Standby HA role if the HAs are supporting physical networks, or in a Peer HA-Peer HA role if they are supporting virtual networks.

In the first case, the Active HA assumes the lead HA role, and synchronizes the Standby HA. In the case of virtual network support, Peer HAs share the lead HA role and “update” each other. The Peer HA configuration allows for load balancing of the incoming RRQs, as either HA may receive RRQs. In either scenario, the HAs participating in the redundancy group should be configured similarly. The current support structure is 1 to1 to provide the maximum robustness and transparency in failover.

[1] *NAI support in Mobile IP HA Redundancy* feature provides CDMA2000 specific capabilities for Home Agent redundancy. The CDMA2000 framework requires address assignment based on NAI, and support of multiple static IP addresses per user NAI.

HA functionality is a service provided by the router and is not interface specific. Therefore, the HA and the MN must agree on which HA interface the MN should send its registration requests, and conversely, on which HA interface the HA should receive the registration requests. This agreement must factor in the following two scenarios:

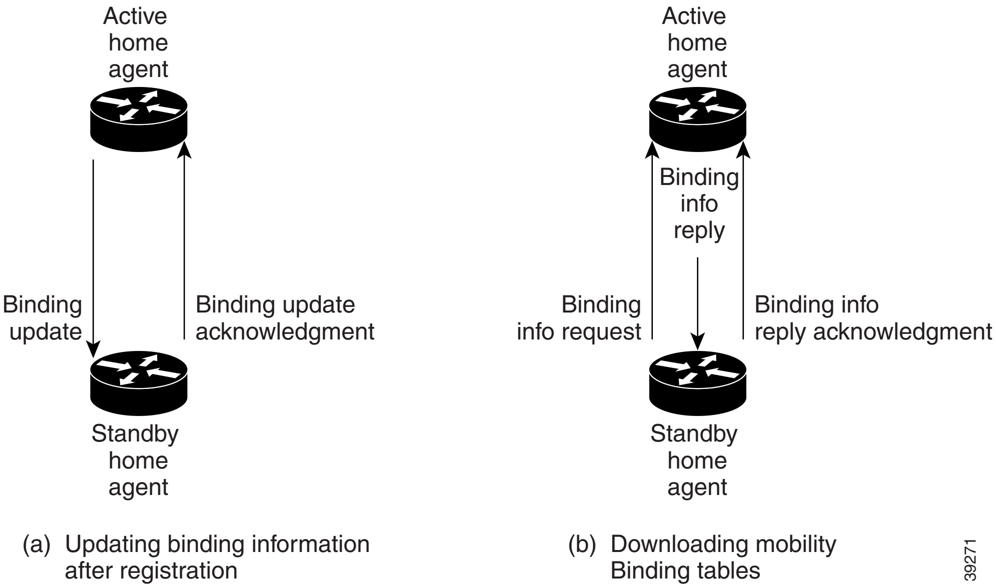
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN.
- An MN that requires the HA interface to be on the same subnet as the MN, that is, the HA and the MN must be on the same home network.

For MNs on physical networks, an active HA accepts registration requests from the MN and sends binding updates to the standby HA. This process keeps the mobility binding table on the active and standby HAs synchronized.

For MNs on virtual networks, the active and standby HAs are peers—either HA can handle registration requests from the MN and update the mobility binding table on the peer HA.

When a standby HA comes up, it must request all mobility binding information from the active HA. The active HA responds by downloading the mobility binding table to the standby HA. The standby HA acknowledges that it has received the requested binding information. Figure 5 illustrates an active HA downloading the mobility bindings to a standby HA. A main concern in this stage of the process is which HA IP interface the standby HA should use to retrieve the appropriate mobility binding table, and on which interface of the standby HA the binding request should be sent.

Figure 5 Overview of HA Redundancy and Mobility Binding Process


Active home agent
Binding update
Binding update acknowledgment
Standby home agent
(a) Updating binding information after registration
Active home agent
Binding info reply
Binding info request
Binding info reply acknowledgment
Standby home agent
(b) Downloading mobility Binding tables
39271

Note The Active HA-Standby HA can also be in Peer HA-Peer HA configuration.

Physical Network Support

For MNs on physical networks, the HAs are configured in the Active HA-Standby HA configurations as shown in Figure 6 and Figure 7. The MNs that are supported on this physical network are configured with the HSRP virtual group address as the HA address. Hence, only the Active HA can accept RRQs from the MN since it is the 'owner' of the HSRP virtual group address. Upon receipt of an authenticated RRQ, the Active HA sends a Binding Update to the Standby HA.

HA Redundancy for physical networks can support multiple HAs in the redundancy group, although only one HA can be in Active state and only one HA can be in Standby state. For example, consider the scenario where there are 4 HAs in the redundancy group, i.e., one Active HA, one Standby HA, and two HAs in Listen state. If the Active HA fails, the Standby HA becomes the Active HA, and the HA in Listen state with higher priority becomes the Standby HA.

Figure 6 Virtual Network Support Using One Physical Network (Peer HA-Peer HA)

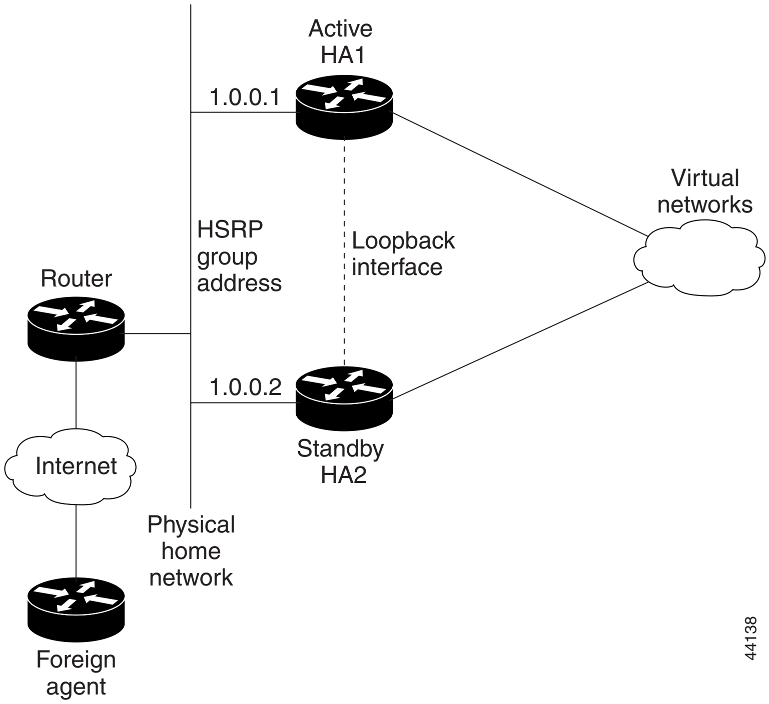
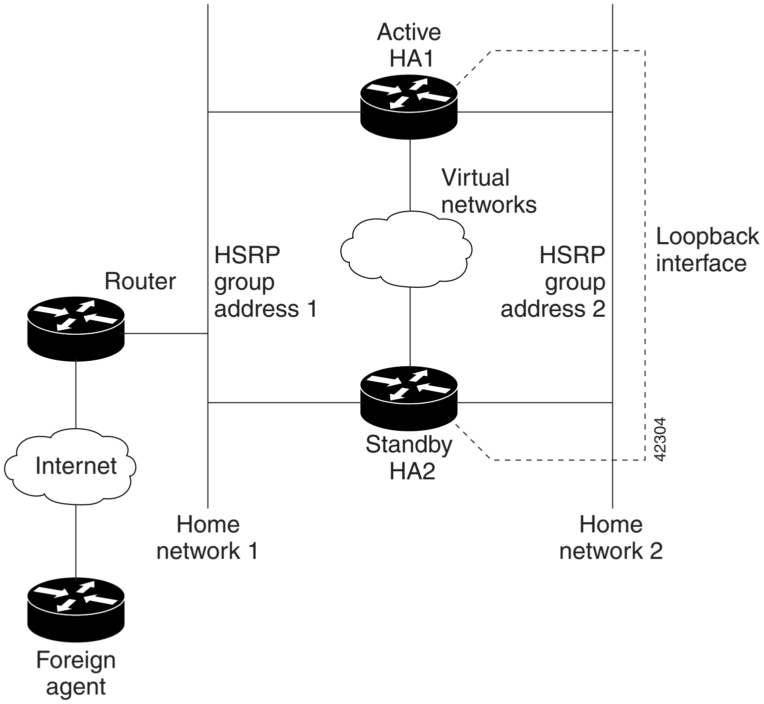


Figure 7 Virtual Network Support Using Multiple Physical Networks (Peer HA-Peer HA)



Home Address Assignment

The Home Agent assigns a home address to the mobile based on user NAI received during Mobile IP registration. The IP addresses assigned to a mobile station may be statically or dynamically assigned. The Home Agent will not permit simultaneous registrations for different NAIs with the same IP address, whether it is statically or dynamically assigned.

Static IP Address

A static IP address is an address that is pre-assigned to the mobile station, and possibly pre-configured at the mobile device. The Home Agent supports static addresses that might be public IP addresses, or addresses in private domain.

Note Use of private addresses for Mobile IP services requires reverse tunneling between the PDSN/FA and the Home Agent.

The mobile user proposes the configured/available address as a non-zero home address in the Registration Request message. The Home Agent may accept this address or return another address in the Registration Reply message. The Home Agent may obtain the IP address by accessing the home-AAA server or DHCP server. The home-AAA server may return the name of a local pool, or a single IP address. On successful Mobile IP registration, Mobile IP based services are made available to the user.

Dynamic IP Address

It is not necessary for a home IP address to be configured in the mobile station in order to access packet data services. A mobile user may request a dynamically assigned address by proposing an all-zero home address in the Registration Request message. The Home Agent assigns a home address and returns it to the mobile in the Registration Reply message. The Home Agent obtains the IP address by accessing the home AAA-server. The AAA server returns the name of a local pool or a single IP address. On successful registration, Mobile IP based services are made available to the user.

Address Assignment for Same NAI - Multiple Static Addresses

The Cisco Home Agent supports multiple Mobile IP registrations for the same NAI with different static addresses. This is accomplished by configuring static-ip-address pool(s) at the home-AAA or DHCP server. When the HA receives a Registration Request message from the mobile user, the HA accesses the home-AAA for authentication, and possibly for assignment of an IP address. The NAI provided by the mobile user is sent to the home-AAA. The home-AAA server returns a list of static-IP-addresses or the static-ip-pool name corresponding to this NAI.

Address Assignment For Same NAI - Different Mobile Terminal

When the same NAI is used for registration from two different mobiles, the behavior is as follows:

- If static address assignment is used in both cases, they are viewed as independent cases.
- If dynamic address assignment is used in both cases, the second registration replaces the first.
- If static is used for the first, and dynamic for the second, the dynamic address assignment replaces the static address assignment.
- If dynamic is used for the first, and static for the second, they are viewed as independent cases.

  Additionally, two flows originating from the same mobile using the same NAI—but two different Home Agents—are viewed as independent cases.

3 DES Encryption

The Cisco Home Agent 1.2 release include 3DES encryption, which supports IPSec on the HA. To accomplish this on the 7200 router platform, Cisco supplies an SA-ISA card for hardware provided IPsec. On the 6500 platform, the MWAM utilizes the Cisco IPSec Acceleration Card.

In this release the HA requires you to configure the parameters for each PDSN before a mobile ip data traffic tunnel is established between the PDSN and the HA.

Note This feature is only available with hardware support.

Mobile IP IPSec

The Internet Engineering Task Force (IETF) has developed a framework of open standards called IP Security (IPSec) that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IS835-B specifies three mechanisms for providing IPSec security:

- Certificates
- Dynamically distributed pre-shared secret
- Statically configured pre-shared secret.

Note IS-835-B Statically configured pre-shared secret is not supported in PDSN Release 1.2. Only CLI-configured, statically configured pre-shared-secret of IKE will be implemented and supported.

Note The Cisco Home Agent Release 1.2 on the Cisco 6500 platform requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500. VPNSM does not have any physical WAN or LAN interfaces, and utilizes VLAN selectors for its VPN policy. For more information on Catalyst 6500 Security Modules visit http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin09186a0080129ead.html

IPSec-based security may be applied on tunnels between the PDSN and the HA depending on parameters received from Home AAA server. A single tunnel may be established between each PDSN-HA pair. It is possible for a single tunnel between the PDSN-HA pair to have three types of traffic streams: Control Messages, Data with IP-in-IP encapsulation, and Data with GRE-in-IP encapsulation. All traffic carried in the tunnel will have same level of protection provided by IPSec.

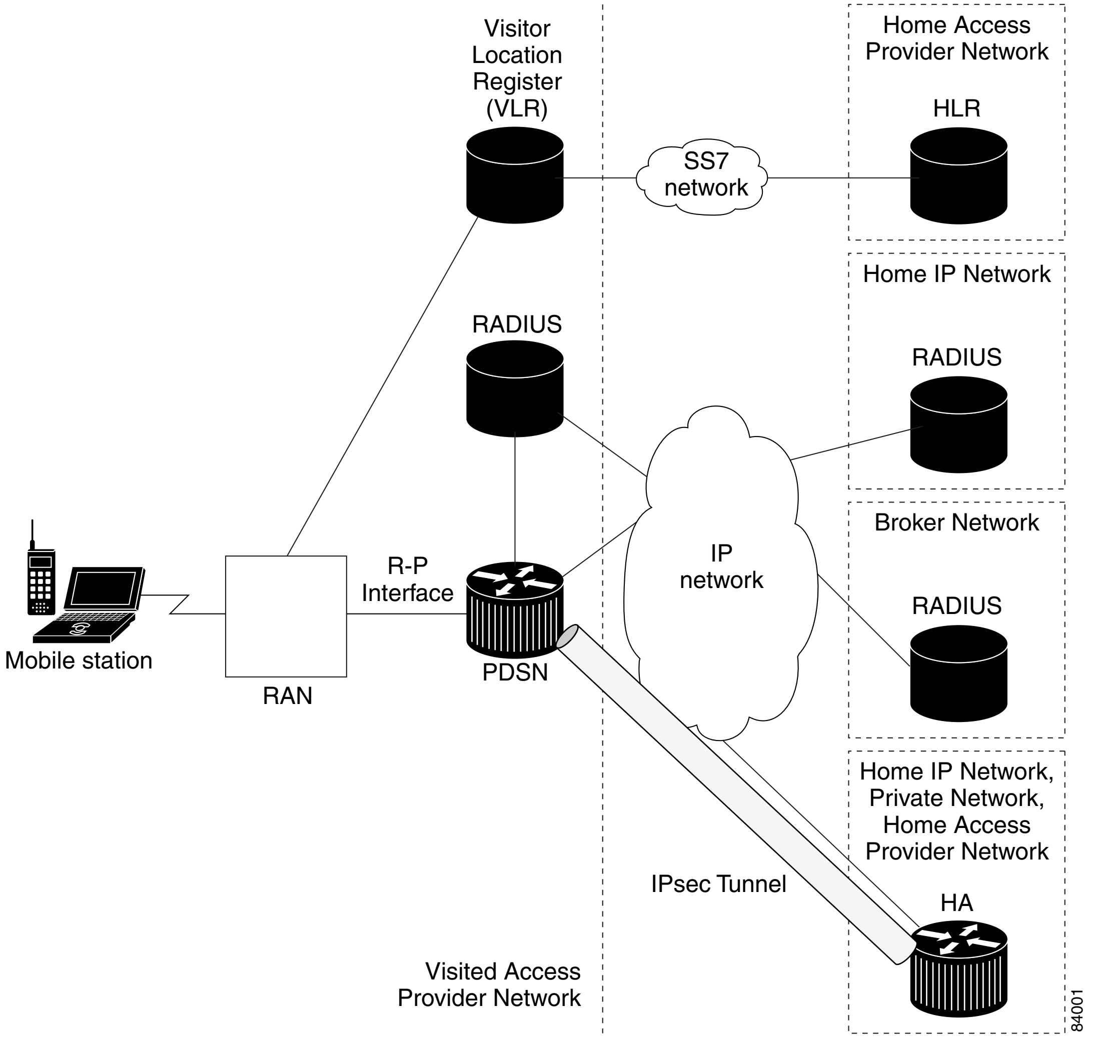
IS835 defines MobileIP service as described in RFC 2002; the Cisco HA provides Mobile IP service and Proxy Mobile IP service.

In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy for the MN to the HA.

Once Security Associations (SAs or tunnels) are established, they remain active until there is traffic on the tunnel, or the lifetime of the SAs expire.

Figure 8 illustrates the IS835 IPSec network topology.

Figure 8 IS835 IPSec Network



User Profiles

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

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

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

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

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

Mobility Binding Association

The mobility binding is identified in the home agent in the following ways:

- For static IP address assignment, NAI+IP
- For dynamic IP address assignment, NAI

The binding association contains the following information:

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

User Authentication and Authorization

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

- Mobile IP Agent Advertisement Challenge Extension
- MN-FA Challenge Extension
- MN-AAA Authentication Extension

Note PAP will be used if no MN-AAA extension is present, and CHAP will always be used if MN-AAA is present.

When configured to authenticate a user with the Home AAA-server, if the Home Agent receives the MN-AAA Authentication Extension in the Registration Request, the contents are used. If the extension is absent, a default configurable password is used.

The Home Agent accepts and maintains the MN-FA challenge extension, and MN-AAA authentication extension (if present), from the original registration for use in later registration updates.

If the Home Agent does not receive a response from the AAA server within a configurable timeout, the message can be retransmitted a configurable number of times. The Home Agent can be configured to communicate with a group of AAA servers, the server being chosen in round-robin fashion from the available configured servers.

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

HA Binding Update

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

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

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

Note The sending of the binding update message is configurable at the Home Agent on a global basis.

Packet Filtering

The Home Agent can filter both egress packets from an external data network and ingress data packets based on the Foreign Agent IP address or the Mobile Node IP address.

Security

The HA uses any present statically configured shared secret(s) when processing authentication extension(s) present in mobile IP registration messages.

Restrictions

Simultaneous Bindings

The Cisco Home Agent does not support simultaneous bindings. When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required, because it is used to maintain more than one flow to the same IP address.

IP Reachability

The Home Agent does not support dynamic DNS updates. Hence the CDMA2000 feature, IP Reachability, is not supported.

Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

Related Documents

For additional information about the Cisco PDSN Release 1.2 software, refer to the following documents:

- *Cisco Packet Data Serving Node (PDSN) Release 1.2 Feature Module.*
- *Release Notes for the Cisco PDSN Feature in Cisco 7200 Series for Cisco IOS Release 12.2(2)XC*
- *Cisco Multi-processor WAN Application Module Installation and Configuration Note*

For more information about:

- The IP Sec configuration commands included in this document, refer to the “IP Security and Encryption” section in the *Cisco IOS Security Configuration Guide*.
- The Cisco IPSec Services Module (VPNSM) on the Catalyst 6500 Security Modules visit http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletin09186a0080129ead.html.
- The AAA configuration commands included in this document, refer to the Cisco IOS Release 12.2 documentation modules *Cisco IOS Security Command Reference* and *Cisco IOS Security Configuration Guide*.
- The RADIUS configuration commands included in this document, refer to the Cisco IOS Release 12.1 documentation module *Cisco IOS Dial Services Command Reference*, as well as the “IP Security and Encryption” section in the *Cisco IOS Security Configuration Guide*.
- Mobile IP, refer to the Cisco Release 12.2 documentation modules *Cisco IOS IP Command Reference* and *Cisco IOS IP Configuration Guide*.

Supported Platforms

Cisco 7200 Router Platform

The Cisco Home Agent is supported on Cisco's 7206VXR routing platform. The Home Agent supports all physical interfaces currently supported on the 7206VXR platform. These interfaces include Fast Ethernet.

For a complete list of interfaces supported on 7206VXR platform, please refer to the on-line product information at Cisco CCO home page. For hardware details on 7206VXR platform, please refer to C7200 product specifications at http://www.cisco.com/warp/public/cc/pd/rt/7200/index.shtml).

The recommended hardware configuration for PDSN Release 1.2 is based on C7206VXR chassis with an NPE-400 processor, 512 MB DRAM, and two FE port adaptors. The I/O controller on the NPE-400 processor supports two more 10/100 based Ethernet ports. A service adaptor, SA_ISA, is required for hardware support of IPSec.

Cisco MWAM on the Catalyst 6500 Switch Support

The Cisco Home Agent is also supported on Cisco's Multi-processor WAN Application Module (MWAM) on the 6500 Catalyst Switch. Each Catalyst 6500 can support up to 6 MWAM modules. Each MWAM has 3 gigabit ethernet interfaces internally connected to the Cat6500 backplane with 802.1q trunking. There are no external visible ports on an MWAM.

The recommended hardware configuration for Home Agent Release 1.2 is based on a Catalyst 6500 chassis with a SUP2, and 512 MB of DRAM.

The recommended MWAM configuration calls for 512 Meg RAM per processor, totalling 1Gigabyte per processor complex.

An IPSec Services Module (VPNSM) is required for hardware support of IPSec.

Each MWAM supports up to 5 IOS images, and each of them can function the same as a Home Agent running on 7200VXR platform. There are no significant feature differences between a Home Agent on an MWAM and a Home Agent on the 7200VXR platform. However, configuring IP sec on the Cisco IPSec Services Module (VPNSM) is completely different than from the 7200. All configuration is done on the Supervisor card and not on the MWAM.

48 port FE or 16 port GE

Note The initial release of the Home Agent on MWAM (1.2) has a tested limit of up to 5 Home agent images on each of two MWAMs

For a complete list of interfaces supported on 6500 platform, please refer to the on-line product information at Cisco.com home page. For hardware details on 6500 platform, please refer to the Catalyst 6500 product specifications at http://www.cisco.com/en/US/products/hw/switches/ps708/index.html).

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

The Cisco PDSN Home Agent is compliant with the following standards:

Standards

- TIA/EIA/IS-835-B, Wireless IP Network Standard
- TIA/EIA/TSB-115, Wireless IP Network Architecture Based on IETF Protocols

MIBs

The Home Agent supports the following MIBs:

- MIB defined in The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.
- The RADIUS MIB, as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

- *IPv4 Mobility*, RFC 2002
- *IP Encapsulation within IP*, RFC 2003
- *Applicability Statement for IP Mobility Support*, RFC 2005
- *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*, RFC 2006
- *Reverse Tunneling for Mobile IP*, RFC 3024
- *Mobile IPv4 Challenge/Response Extensions*, RFC 3012
- *Mobile NAI Extension*, RFC 2794
- *Generic Routing Encapsulation*, RFC 1701
- *GRE Key and Sequence Number Extensions*, RFC 2890

- *IP Mobility Support for IPv4*, RFC 3220, Section 3.2 Authentication
- *The Network Access Identifier*, RFC 2486, January 1999.
- *An Ethernet Address Resolution Protocol*, RFC 826, November 1982
- *The Internet Key Exchange (IKE)*, RFC 2409, November 1998.

Configuration Tasks

The Cisco Home Agent software includes two images, one for the Cisco 7200 and one for the Catalyst 6500. This section describes the steps for configuring the Cisco Home Agent. Each image is described by platform number.

- c7200-h1is-mz HA image
- c6svcmwam-h1is-mz HA image

Upgrading a Home Agent Image

To upgrade an image, you will need a compact flash card that has the MP partition from the current image or later, and a recent supervisor image. To locate the images, please go to the Software Center at Cisco.com (http://www.cisco.com/public/sw-center/).

To perform the upgrade perform the following procedure:

Step 1 Log onto the supervisor and boot the MP partition on the PC.

```
 router #hw-module module 3 reset cf:1
Device BOOT variable for reset = > <cf:1> Warning:  Device list is not verified.
 >
 > Proceed with reload of module? [confirm] % reset issued for module 3
 >router#
```

Step 2 Once the module is online, issue the following command:

copy tftp: *tftp file location* pclc# *linecard #*-fs:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
router #copy tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin pclc#3-fs:
> Destination filename [c6svcmwam-c6is-mz.bin]?
> Accessing tftp://198.133.219.33/images/c6svcmwam-c6is-mz.bin...
> Loading images/c6svcmwam-c6is-mz.bin from 64.102.16.25 (via Vlan1):
> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
> [OK - 29048727/58096640 bytes]

> 29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
> 2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
> 2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
> router #

> 2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeded>
> 2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module
```

Step 3 Boot the MWAM card back to partition 4, and you have an upgraded image.

```
router#hw-module module 3 reset
```

Loading the IOS Image to MWAM

The image download process automatically loads an IOS image onto the three Processor complexes on the MWAM. All three complexes on the card run the same version of IOS, so they share the same image source. The software for MWAM bundles the images it needs in flash memory on the PC complex. For more information, refer to the *Cisco Multi-processor WAN Application Module Installation and Configuration Note*.

Configuring the Home Agent

A typical HA configuration requires that you define interfaces in three directions: PDSN/FA, home network, and AAA server. If HA redundancy is required, then you must configure another interface for HSRP binding updates between HAs. If you are running the HA on the MWAM, the HA will see the access to one GE port that will connect to Catalyst 6500 backplane. That port can be configured as a trunk port with subinterfaces provided for each necessary network access.

VLANs can be defined corresponding to each interface: PDSN/FA, home network, AAA. In the case of multiple HA instances in the same Catalyst 6500 chassis, the same VLAN can be used for all of them.

The Cisco Home Agent can provide two classes of user services: Mobile IP, and proxy Mobile IP. The following sections describe the configuration tasks for implementing the Cisco Home Agent.

MWAM Configuration Tasks (Required for All Scenarios)

- Basic IOS Configuration on MWAM and Catalyst 6500

AAA and RADIUS Configuration Tasks (Required for All Scenarios)

To configure the AAA and RADIUS in the Home Agent environment, complete the following tasks.

- Configuring AAA in the Home Agent Environment
- Configuring RADIUS in the Home Agent Environment

Mobile IP Configuration Tasks (Required for Mobile IP)

To configure Mobile IP on the Home Agent, complete the following task:

- Configuring Mobile IP Security Associations

Home Agent Redundancy Tasks (Required for Mobile IP)

- Configuring HA Redundancy

Network Management Configuration Tasks

- Configuring Network Management

Cisco Home Agent Configuration Tasks

- Configuring the Cisco Home Agent

IP Sec Configuration Tasks

- Configuring IPSec for the HA

Maintaining the HA

- Monitoring and Maintaining the HA

Basic IOS Configuration on MWAM and Catalyst 6500

To configure the Supervisor engine recognize the MWAM modules, and to establish physical connections to the backplane, use the following commands:

Command	Purpose
`router# vlan database`	Enter VLAN configuration mode.
`router(vlan)# vlan vlan-id`	Add an Ethernet VLAN.
`router(vlan)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.
`router(config)# mwam module 7 port 3 allowed-vlan vlan_range`	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM.
`router# session slot MWAM module processor processor number`	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM. *Processor number* is from 2 to 6.
`Router(config)# int gigabitEthernet 0/0`	Specifies the type of interface being configured, and the slot number.
`Router(config-if)# no shut`	Puts the specified GE interfaces in service.
`Router(config-if)# int gigabitEthernet 0/0.401`	
`Router(config-subif)# encapsulation dot1Q 401`	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs.
`Router(config-subif)# ip address 1.1.1.1 255.255.255.0`	
`Router(config-subif)# exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.

Note MWAM modules synchronize their timing functions from the Supervisor engine's clock timers. Do not configure the timers on each individual MWAM.

Configuring AAA in the Home Agent Environment

Access control is the way you manage who is allowed access to the network server and what services they are allowed to use. AAA network security services provide the primary framework through which you set up access control on your router or access server. For detailed information about AAA configuration options, refer to the "Configuring Authentication," and "Configuring Accounting" chapters in the *Cisco IOS Security Configuration Guide*.

To configure AAA in the HA environment, use the following commands in global configuration mode:

Command	Purpose
`Router(config)#` **`aaa authentication ppp default group radius`**	Enables authentication of PPP users using RADIUS.
`Router(config)#` **`aaa authorization network default group radiu`**`s`	Restricts network access to a user. Runs authorization for all network-related service requests. Uses the group radius authorization method as the default method for authorization.

Configuring RADIUS in the Home Agent Environment

RADIUS is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information. For detailed information about RADIUS configuration options, refer to the “Configuring RADIUS” chapter in the *Cisco IOS Security Configuration Guide*.

To configure RADIUS in the HA environment, use the following commands in global configuration mode:

Command	Purpose
`Router(config)#` **`radius-server host`** *`ip-addr`* **`key`** *`sharedsecret`*	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.

Configuring Mobile IP Security Associations

To configure security associations for mobile hosts, FAs, and HAs, use one of the following commands in global configuration mode:

Command	Purpose
`Router(config)#` **`ip mobile secure`** {**`host`** | **`visitor`** | **`home-agent`** | **`foreign-agent`** | **`proxy-host`**} {*`lower-address`* [*`upper-address`*] | **`nai`** *`string`*} {**`inbound-spi`** *`spi-in`* **`outbound-spi`** *`spi-out`* | **`spi`** *`spi`*} **`key`** {**`hex`** | **`ascii`**} *`string`* [**`replay timestamp`** [*`number`*] **`algorithm md5 mode prefix-suffix`**]	Specifies the security associations for IP mobile users.

Configuring HA Redundancy

To configure your routers for Mobile IP HA redundancy, perform the required tasks described in the following sections:

- Enabling Mobile IP (Required)
- Enabling HSRP (Required)
- Enabling HA Redundancy for a Physical Network (Required)
- Enabling HA Redundancy for a Virtual Network Using One Physical Network

Enabling Mobile IP

To enable Mobile IP on the router, use the following command in global configuration mode:

Command	Purpose
Router(config)#**router mobile**	Enables Mobile IP on the router.

Enabling HSRP

To enable HSRP on an interface, use the following command in interface configuration mode:

Router(config-if)#**standby** [*group-number*] **ip** *ip-address*	Enables HSRP.

Configuring HSRP Group Attributes

To configure HSRP group attributes that affect how the local router participates in HSRP, use either of the following commands in interface configuration mode:

Router(config-if)#**standby** [*group-number*] **priority** *priority* [**preempt** [**delay** [**minimum** | **sync**] *delay*]] or Router(config-if)#**standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]	Sets the Hot Standby priority used in choosing the active router. By default, the router that comes up later becomes standby. When one router is designated as an active HA, the priority is set highest in the HSRP group and the preemption is set. Configure the **preempt delay sync** command so that all bindings will be downloaded to the router before it takes the active role. The router becomes active when all bindings are downloaded, or when the timer expires, whichever comes first.

Enabling HA Redundancy for a Physical Network

To enable HA redundancy for a physical network, use following commands beginning in interface configuration mode:

Command	Purpose
Router(config-if)#**standby** [*group-number*] **ip** *ip-address*	Enables HSRP.
Router(config-if)# **standby name** *hsrp-group-name*	Sets the name of the standby group.
Router(config)#**ip mobile home-agent redundancy** *hsrp-group-name*	Configures the home agent for redundancy using the HSRP group name.
Router(config)#**ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address address argument is that of the standby HA. If configured on the standby HA, the IP address address argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Enabling HA Redundancy for a Virtual Network Using One Physical Network

To enable HA redundancy for a virtual network and a physical network, use the following commands beginning in interface configuration mode:

Command	Purpose
`Router (config-if)# standby [group-number] ip ip-address`	Enables HSRP.

`Router(config)#ip mobile home-agent address address`
or
`Router(config)#ip mobile home-agent`
	Defines a global home agent address. In this configuration, the address is the HSRP group address. Enter this command if the mobile node and home agent are on different subnets.
	or
	Enables and controls home agent services to the router. Enter this command if the mobile node and home agent are on the same subnet.

`Router(config)#ip mobile virtual-network net mask [address address]`	Defines the virtual network. If the mobile node and home agent are on the same subnet, use the [**address** *address*] option.
`Router(config)# ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address]`	Configures the home agent for redundancy using the HSRP group to support virtual networks.
`Router(config)# ip mobile secure home-agent address spi spi key hex string`	Sets up the home agent security association between peer routers. If configured on the active HA, the IP address address argument is that of the standby HA. If configured on the standby HA, the IP address address argument is that of the active router. Note that a security association needs to be set up between all HAs in the standby group.

Configuring Network Management

To enable SNMP network management for the HA, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# snmp-server community string [ro | rw]`	Specifies the community access string to permit access to the SNMP protocol.
`Router(config)# snmp-server host host-addr traps version {1 | 2 | 3 [auth | noauth | priv]}`	Specifies the recipient of an SNMP notification operation.
`Router(config)#no virtual-template snmp`	Prevents the virtual-access subinterfaces from being registered with the SNMP functionality of the router and reduces the amount of memory being used, thereby increasing the call setup performance.
`Router(config)#snmp-server enable traps ipmobile`	(Optional) Specifies Simple Network Management Protocol (SNMP) security notifications for Mobile IP.

Configuring the Cisco Home Agent

To configure the Cisco HA, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **ip mobile host** {*lower* [*upper*] | **nai** *string* [**static-address** *addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name* {**address** *addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]}}}{**interface** *name* | **virtual-network** *net mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]	Specifies either static IP addresses or a pool of IP addresses for use by multiple flows with the same NAI.
Router(config)#**ip mobile home-agent** [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel-off**] [**roam-access** *acl*] [**strip-nai-realm**] [**suppress-unreachable**] [**local-timezone**]	Enables and controls home agent services on the router.

Configuring IPSec for the HA

To configure IPSec for the HA, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp** **set peer** *ip address of ha* **set transform-set** transform-set-name **match address** *acl name*	Creates a a crypto map entry for one HA in one Crypto-map set. The Crypto Map definition is not complete until: **1.** ACL associated with it is defined, and **2.** The Crypto-Map applied on Interface. You can configure Crypto MAP for different HAs by using a different sequence number for each HA in one crypto-map set.
Router# **access-list** *acl-name* **deny udp host** *HA IP addr* **eq mobile-ip host** *PDSN IP addr* **eq mobile-ip** **access-list** *acl-name* **permit ip host** *PDSN IP addr* **host** *HA IP addr* **access-list** *acl-name* **deny ip any any**	Defines the access list. The ACL name "acl-name" is same as in the crypto-map configuration
Router# **Interface** *Physical-Interface of PI interface* **crypto map** *Crypto-Map set*	Applies the Crypto-Map on Pi Interface, as the HA sends/receives Mobile IP traffic to/from PDSN on this interface
Router# **ip mobile tunnel crypto map** *crypto-map set name*	Configure Mobile IP to use the configured Crypto-Map set

Monitoring and Maintaining the HA

To monitor and maintain the HA, use the following commands in privileged EXEC mode:

Command	Purpose
`Router# clear ip mobile binding`	Removes mobility bindings.
`Router# clear ip mobile host-counters`	Clears the mobility counters specific to each mobile station.
`Router#clear ip mobile secure`	Clears and retrieves remote security associations.
`Router# debug ip mobile advertise`	Displays advertisement information.
`Router# debug ip mobile host`	Displays mobility event information.
`Router# show ip mobile binding`	Displays the mobility binding table.
`Router# show ip mobile host`	Displays mobile station counters and information.
`Router# show ip mobile proxy`	Displays information about a proxy Mobile IP host.
`Router# show ip mobile secure`	Displays mobility security associations for Mobile IP.
`Router# show ip mobile violation`	Displays information about security violations.

Configuration Examples

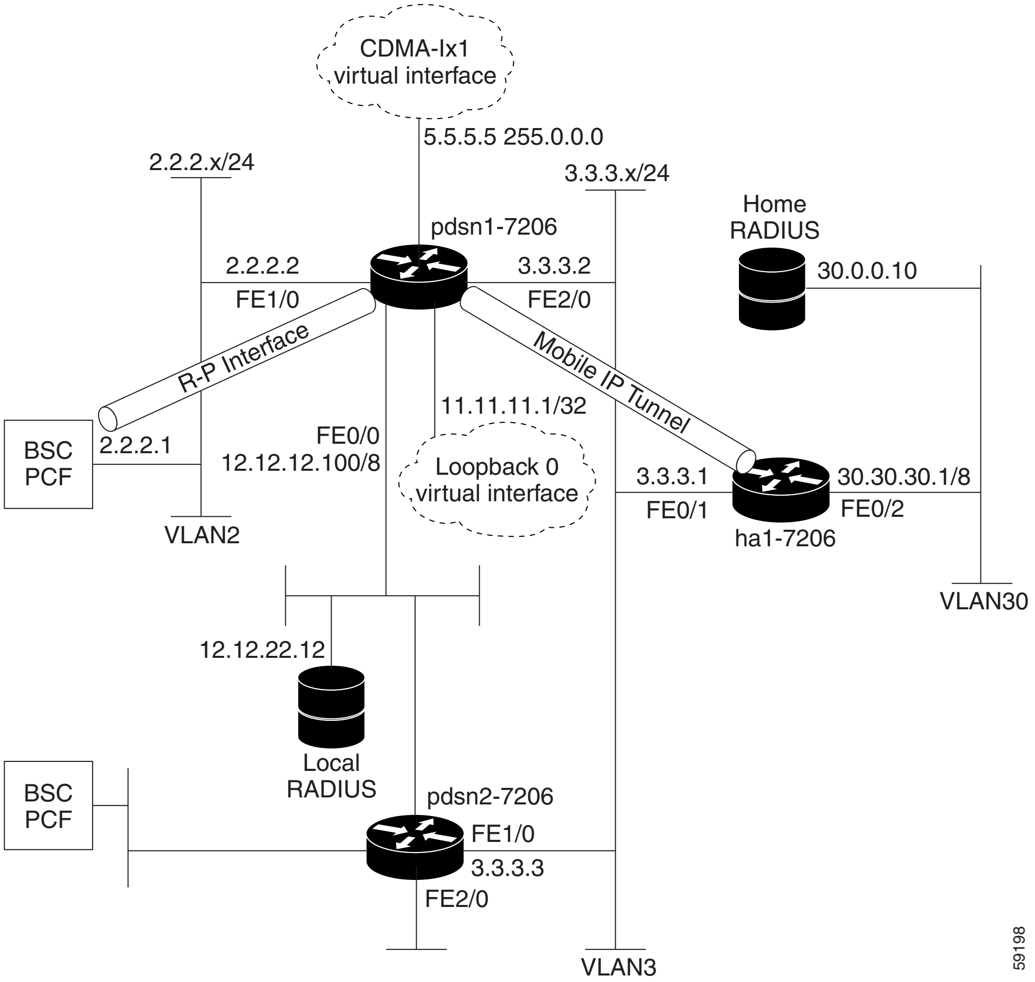
This section provides the following configuration examples:

- Cisco Home Agent Configuration
- Home Agent Redundancy Configuration
- Home Agent IPSec Configuration

Cisco Home Agent Configuration

Figure 9 and the information that follows is an example of the placement of a Cisco HA and it's configuration.

Figure 9 Home Agent —A Network Map



Example 1

```
hostname ha1-7206
!
aaa new-model
!
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
interface FastEthernet0/1
 description To FA/PDSN
 ip address 3.3.3.1 255.255.255.0
!
interface FastEthernet0/2
 description To AAA
 ip address 30.30.30.1 255.0.0.0
!
router mobile
!
ip local pool ha-pool1 35.35.35.1 35.35.35.254
ip mobile home-agent broadcast
ip mobile virtual-network 35.35.35.0 255.255.255.0
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 35.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 30.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
line con 0
 exec-timeout 0 0
 login authentication CONSOLE
```

Example 2 Home Agent Configuration

```
Cisco_HA#sh run
Building configuration...

Current configuration : 4532 bytes
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname USER_HA
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa session-id common
!
username simulator password 0 cisco
username userc-moip password 0 cisco
username pdsn password 0 cisco
username userc password 0 cisco
username USER_PDSN
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
! !
!
 interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!
interface Tunnel1
 no ip address
!
interface FastEthernet0/0
 ip address 9.15.68.14 255.255.0.0
 duplex half
 speed 100
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex half
 speed 10
 no cdp enable
!
interface FastEthernet1/0
 ip address 92.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 ip address 5.5.5.3 255.255.255.0 secondary
 ip address 5.5.5.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
!
router mobile
!
ip local pool ha-pool 6.0.0.1 6.0.15.254
ip local pool ha-pool1 4.4.4.100 4.4.4.255
ip default-gateway 9.15.0.1
ip classless
ip route 3.3.3.1 255.255.255.255 FastEthernet1/1
ip route 9.100.0.1 255.255.255.255 9.15.0.1
ip route 17.17.17.17 255.255.255.255 FastEthernet1/0
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile host nai userc-moip address pool local ha-pool interface FastEthernet1/0
ip mobile host nai userc address pool local pdsn-pool interface Loopback0 aaa
ip mobile secure host nai userc-moip spi 100 key hex ffffffffffffffffffffffffffffffff
replay timestamp within 150
!
!
radius-server host 9.15.200.1 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!

gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 5 15
!
!
end
```

Home Agent Redundancy Configuration

PDSN Configuration

```
~~~~~~~~~~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service cdma pdsn
!
hostname mwt10-7206a
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
virtual-profile aaa
!
interface Loopback0
 ip address 6.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
!
interface CDMA-Ix1
```

```
 ip address 5.0.0.1 255.0.0.0
 tunnel source 5.0.0.1
!
interface FastEthernet1/0
 description to PCF
 ip address 4.0.0.101 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface Ethernet2/0
 description to HA
 ip address 7.0.0.1 255.0.0.0
 no ip route-cache cef
 duplex half
!
interface Ethernet2/1
 description to AAA
 ip address 150.1.1.9 255.255.0.0
 no ip route-cache cef
 duplex half
!
interface Virtual-Template1
 ip unnumbered Loopback0
 ip mobile foreign-service challenge
 ip mobile foreign-service reverse-tunnel
 ip mobile registration-lifetime 60000
 no keepalive
 no peer default ip address
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool pdsn-pool 11.0.0.1 11.0.0.255
ip classless
ip route 9.0.0.0 255.0.0.0 7.0.0.2
ip route 10.0.0.0 255.0.0.0 7.0.0.2
no ip http server
ip pim bidir-enable
ip mobile foreign-agent care-of Ethernet2/0
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
radius-server host 150.1.0.2 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn mip-reg-fail-no-closesession
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii cisco
cdma pdsn secure pcf 4.0.0.2 spi 100 key ascii cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

Active-HA configuration

```
~~~~~~~~~~~~~~~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Ethernet2/0
 description to PDSN/FA
 ip address 7.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 7.0.0.4
 standby priority 110
 standby preempt delay sync 100
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 150.2.1.8 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface 
Ethernet2/0 aaa
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii redundancy algorithm md5 mode 
prefix-suffix
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
```

```
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

Standby-HA configuration

```
~~~~~~~~~~~~~~~~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Ethernet2/0
 description to PDSN/FA
 ip address 7.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 7.0.0.4
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 150.2.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 7.0.0.2 spi 100 key ascii redundancy algorithm md5 mode
prefix-suffix
!
```

```
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

Home Agent IPSec Configuration

Note Once you permit the hosts/subnets you want encrypted, ensure that you put in an explicit deny statement. The deny statement states do not encrypt any other packets.

Note The following example is for IPSec on the Cisco 7200 router only. IPSec on the Cisco Catalyst 6500 is configured on the Supervisor, rather than on the Home Agent.

```
access-list 101 deny   ip any any
access-list 103 deny   ip any any

-------------------------------------------------------

!
! No configuration change since last restart
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname 7206f1
!
aaa new-model
!
!
aaa authentication login CONSOLE none
aaa authentication login NO_AUTHENT none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
enable password 7 151E0A0E
!
username xxx privilege 15 nopassword
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 1.1.1.4
crypto isakmp key cisco address 172.18.60.30
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map tosim 10 ipsec-isakmp
 set peer 1.1.1.4
 set transform-set esp-des-sha-transport
 match address 101
!
crypto map tosim3 10 ipsec-isakmp
 set peer 172.18.60.30
 set transform-set esp-des-sha-transport
 match address 103
!
!
interface Loopback0
 ip address 9.0.0.1 255.0.0.0
!
interface Loopback1
 ip address 12.0.0.1 255.0.0.0
!
interface Loopback10
 ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 1.1.1.1 255.255.255.0
 load-interval 30
 duplex full
 speed 100
 crypto map tosim
!
interface FastEthernet0/1
 ip address 2.1.1.1 255.0.0.0
 load-interval 30
 duplex full
 speed 100
!
interface FastEthernet1/0
 ip address 3.1.1.1 255.255.255.0
 load-interval 30
 duplex full
!
interface FastEthernet2/0
 ip address 172.18.60.10 255.255.255.0
 load-interval 30
 duplex full
 crypto map tosim3
!
router mobile
!
ip local pool ispabc-pool1 12.0.0.2 12.1.0.1
ip local pool ispabc-pool1 12.1.0.2 12.2.0.1
ip local pool ispxyz-pool1 9.0.0.2 9.1.0.1
ip local pool ispxyz-pool1 9.1.0.2 9.2.0.1
ip classless
ip route 172.18.49.48 255.255.255.255 172.18.60.1
no ip http server
ip pim bidir-enable
ip mobile home-agent address 10.1.1.1
ip mobile host nai @ispabc.com address pool local ispabc-pool1 virtual-network 12.0.0.0
255.0.0.0 aaa load-sa lifetime 65535
ip mobile host nai @ispxyz.com address pool local ispxyz-pool1 virtual-network 9.0.0.0
255.0.0.0 aaa load-sa lifetime 65535
!
!
access-list 101 permit ip host 10.1.1.1 host 1.1.1.4
access-list 101 deny   ip any any
access-list 103 permit ip host 10.1.1.1 host 172.18.60.30
access-list 103 deny   ip any any
!
!
radius-server host 172.18.49.48 auth-port 1645 acct-port 1646 key 7 094F471A1A0A
radius-server retransmit 3
radius-server key 7 02050D480809
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
!
exception protocol ftp
exception dump 64.102.16.25
exception memory minimum 1000000
ntp clock-period 17179878
ntp server 172.18.60.1
!
end
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **access list**
- **aaa authorization ipmobile**
- **clear ip mobile binding**
- **clear ip mobile host-counters**
- **clear ip mobile secure**
- **clear ip mobile traffic**
- **crypto map (global IPSec)**
- **ip mobile home-agent**
- **ip mobile home-agent reject-static-addr**
- **ip mobile home-agent redundancy**
- **ip mobile home-agent resync-sa**
- **ip mobile host**
- **ip mobile secure**
- **ip mobile tunnel**
- **ip mobile virtual-network**
- **radius-server host**
- **router mobile**
- **show ip mobile binding**
- **show ip mobile globals**
- **show ip mobile host**
- **show ip mobile secure**
- **show ip mobile traffic**
- **show ip mobile violation**
- **snmp-server enable traps ipmobile**

access list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** global configuration command. Use the **no** form of this command to remove the single specified entry from the access list.

access-list *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

no access-list *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

Syntax Description

access-list-number	Integer that identifies the access list. If the type-code wild-mask arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the address and mask arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a SNAP type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the type-code argument. The wild-mask indicates which bits in the type-code argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
address	48-bit Token Ring address written in dotted triplet form. This field is used for filtering by vendor code.
mask	48-bit Token Ring address written in dotted triplet form. The ones bits in mask are the bits to be ignored in address. This field is used for filtering by vendor code.

Defaults

No numbered encryption access lists are defined, and therefore no traffic will be encrypted/decrypted. After being defined, all encryption access lists contain an implicit “deny” (“do not encrypt/decrypt”) statement at the end of the list..

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use encryption access lists to control which packets on an interface are encrypted/decrypted, and which are transmitted as plain text (unencrypted).

When a packet is examined for an encryption access list match, encryption access list statements are checked in the order that the statements were created. After a packet matches the conditions in a statement, no more statements will be checked. This means that you need to carefully consider the order in which you enter the statements.

To use the encryption access list, you must first specify the access list in a crypto map and then apply the crypto map to an interface, using the crypto map (CET global configuration) and crypto map (CET interface configuration) commands.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match the TCP source port, the type of service value, or the packet's precedence.

Note After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list command lines from a specific access list.

Caution When creating encryption access lists, we do not recommend using the any keyword to specify source or destination addresses. Using the any keyword with a permit statement could cause extreme problems if a packet enters your router and is destined for a router that is not configured for encryption. This would cause your router to attempt to set up an encryption session with a nonencrypting router. If you incorrectly use the any keyword with a deny statement, you might inadvertently prevent all packets from being encrypted, which could present a security risk.

Note If you view your router’s access lists by using a command such as show ip access-list, all extended IP access lists will be shown in the command output. This includes extended IP access lists that are used for traffic filtering purposes as well as those that are used for encryption. The show command output does not differentiate between the two uses of the extended access lists.

Examples

The following example creates a numbered encryption access list that specifies a class C subnet for the source and a class C subnet for the destination of IP packets. When the router uses this encryption access list, all TCP traffic that is exchanged between the source and destination subnets will be encrypted.

```
access-list 101 permit tcp 172.21.3.0 0.0.0.255 172.22.2.0 0.0.0.255
```

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.

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 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.

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
```

Related Commands

Command	Description
show ip mobile host	Displays the mobility host information.

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* | **nai** *string ip_address*}

Syntax Description

all	Clears all mobility bindings.
load *standby-group-name*	(Optional) Downloads mobility bindings for a standby group after clear.
ip-address	IP address of a mobile node.
nai *string*	Network access identifier of the 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*
12.2(2)XC	The **nai** keyword and associated variables were added.

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 host-counters

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

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

Syntax Description

ip-address	(Optional) IP address of a mobile node.
nai *string*	(Optional) Network access identifier of the mobile node.
undo	(Optional) Restores the previously cleared counters.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated variables were added.

Usage Guidelines

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

Examples

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

```
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


Router# clear ip mobile host-counters
Router# show ip mobile host-counters

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
```

Related Commands

Command	Description
show ip mobile host	Displays mobile station counters and information.

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*] | **nai** *string* | **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.
nai *string*	Network access identifier of the mobile node.
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.
12.2(2)XC	The **nai** keyword and associated variables were added.

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	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

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

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.

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 the protocol counters.

crypto map (global IPSec)

To create or modify a crypto map entry and enter the crypto map configuration mode, use the **crypto map** global configuration command. To delete a crypto map entry or set, use the no form of this command.

crypto map *map-name seq-num* **ipsec-manual**

crypto map *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*] [**discover**]

no crypto map *map-name* [*seq-num*]

Syntax Description

map name	The name you assign to the crypto map set
seq-num	The number you assign to the crypto map entry.
ipsec-manual	Indicates that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	Indicates that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Examples

The following example creates a crypto map entry and indicates that IKE will not be used to establish the IPSec security associations for protecting the traffic:

```
Router# crypto map map-name seq-num ipsec-manual
```

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 [**home-agen**t *address*] [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel off**] [**roam-access** *acl*] [**strip-nai-realm**] [**suppress-unreachable**] [**local-timezone**]

no ip mobile home-agent [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel private address**] [**roam-access** *acl*] [**strip-nai-realm**] [**suppress-unreachable**] [**local-timezone**]

Syntax Description

home-agent *address*	(Optional) IP address of the Home Agent.
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-private address	(Optional) Enables support of reverse tunnel by the home agent. By default, reverse tunnel support is enabled. Reverse tunneling is mandatory for Private Mobile IP addresses.
roam-access *acl*	(Optional) Controls which mobile nodes are permitted or denied to roam. By default, all specified mobile nodes can roam.
strip-nai-realm	(Optional) Strips the realm part of the NAI before authentication is performed.
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.
local-timezone	(Optional) Adjusts the UTC time based on the local time zone configured and uses the adjusted time for proxy mobile IP registration.

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.
12.2(2)XC	The **strip-nai-realm** and **local-timezone** keywords were added.

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 1) and sends a reply. (Replay codes are listed in Table 2.) A security violation is logged when foreign agent authentication, MH authentication, or Identification verification fails. (The violation reasons are listed in Table 3.)

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.

By default, the HA uses the entire NAI string as username for authentication (which may be with local security association or retrieved from the AAA server). The **strip-nai-realm** parameter instructs the HA to strip off the realm part of NAI (if it exists) before performing authentication. Basically, the mobile station is identified by only the username part of NAI.

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

Table 1 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 collocated 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.
T	Accept if **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

Table 2 lists the home agent registration reply codes.

Table 2 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 3 lists security violation codes.

Table 3 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

Router (config)#ip mobile home-agent reverse-tunnel ?
  off              Disable reverse tunnel mode
  private-address  Reverse Tunneling Mandatory for Private Mobile IP addresses
```

Related Commands

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

ip mobile home-agent reject-static-addr

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

ip mobile home-agent reject-static-addr

Syntax Description

This command has not arguments or keywords

Command Modes

Sub-command of the **ip mobile home-agent** global configuration command.

Command History

Release	Modification
12.2(8)BY	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
Router# ip mobile home-agent reject-static-addr
```

ip mobile home-agent redundancy

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

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

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

Syntax Description

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

Defaults

No global home agent addresses are specified.

Command Modes

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

Command History

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

Usage Guidelines

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

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 the command is deconfigured, the home agent can remove mobility bindings. The following describes how home agent redundancy operates on physical and virtual networks.

Physical network:

Only the active home agent will receive registrations. 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 is sample output from the **ip mobile home-agent redundancy** command that specifies an HSRP group name of SanJoseHA:

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

ip mobile home-agent resync-sa

To configure the HA to clear out the old cached security associations and requery the AAA server, use the **ip mobile home-agent resync-sa** command global configuration command.

ip mobile home-agent resync-sa *x*

Syntax Description

x	Specifies the time that the HA will use to initiate a resync.

Command Modes

Global configuration.

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

When a MN tries to reregister with the HA, the time change from the original timestamp is checked. If that time period is less than x, and the MN fails authentication, then the HA will not requery the AAA server for another SA.

If the MN reregisters with the HA, and the time between registrations is greater than x, and the MN fails registrations, then the HA will clear out the old SA and requery the AAA server.

Examples

The following example illustrates the **ip mobile home-agent resync-sa** command:

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

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command. For PDSN, use this command to configure the static IP address or address pool for multiple flows with the same NAI.

ip mobile host {*lower* [*upper*] | **nai** *string* {**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*} | **address {***addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]} {**interface** *name* | **virtual-network** *network_address mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

no ip mobile host {*lower* [*upper*] | **nai** *string* {**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*} | **address {***addr* | **pool** {**local** *name* | **dhcp-proxy-client** [**dhcp-server** *addr*]} {**interface** *name* | **virtual-network** *network_address mask*} [**aaa** [**load-sa**]] [**care-of-access** *acl*] [**lifetime** *number*]

Syntax Description

lower [*upper*]	One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional.
nai *string*	Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (realm).
static-address	Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm.
addr1, *addr2*, ...	(Optional) One or more IP addresses to be assigned using the **static-address** keyword.
local-pool *name*	Name of the local pool of addresses to use for assigning a static IP address to this NAI.
address	Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
addr	IP address to be assigned using the **address** keyword.
pool	Indicates that pool of addresses is to be used in assigning a dynamic IP address.
local *name*	The name of the local pool to use in assigning addresses.
dhcp-proxy-client	Indicates that the pool should come from a DHCP client.
dhcp-server *addr*	IP address of the DHCP server.
interface *name*	Mobile node that belongs to the specified interface. When used with DHCP, this specifies the address pool from which the DHCP server should select the address.
virtual-network *network_address mask*	Indicates that the mobile station resides in the specified virtual network, which was created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations from a 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. Possible values are 3 through 65535.

Defaults

No host is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated parameters were added.

Usage Guidelines

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from 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 4 are based on the assumption of one security association per mobile node.

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

The address pool can be defined by a local pool or using a DHCP proxy client. For DHCP, the **interface** *name* specifies the address pool from which the DHCP server selects and **dhcp-server** specifies DHCP server address.

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 4.

Table 4 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).
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
```

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

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 9.0.0.0
255.0.0.0 aaa lifetime 65535
```

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

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

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	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.
show ip mobile host	Displays mobile station counters and information.
ip mobile proxy-host	Configures the proxy Mobile IP attributes of the PDSN.

ip mobile secure

To specify the mobility security associations for the mobile host, visitor, home agent, foreign agent, and proxy host, use the **ip mobile secure** global configuration command. To remove the mobility security associations, use the **no** form of this command.

ip mobile secure {**host** *lower-address* [*upper-address*] | **visitor** *address* | **home-agent** *address* | **foreign-agent** *address*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm md5 mode prefix-suffix**]

no ip mobile secure {**host** *lower-address* [*upper-address*] | **visitor** *address* | **home-agent** *address* | **foreign-agent** *address*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm md5 mode prefix-suffix**]

Syntax Description

host	Security association of the mobile host on the home agent.
lower address	IP address of host, visitor, or mobility agent, or lower range of IP address pool.
upper-address	(Optional) Upper range of IP address pool.
visitor	Security association of the mobile host on the foreign agent.
home-agent	Security association of the remote home agent on the foreign agent.
foreign-agent	Security association of the remote foreign agent on the home agent.
address	IP address of visitor or mobility agent.
inbound-spi *spi-in*	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.
outbound-spi *spi-out*	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
spi *spi*	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
key hex *string*	ASCII or hexadecimal string of 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.
number	(Optional) Number of seconds. Registration is valid if received within the specified time. This means the sender and receiver are in time synchronization (NTP can 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.

Defaults

No security association is specified.

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.

Usage Guidelines

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

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, replay attack protection method, timeout, and IP address.

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

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

Note NTP can be used to synchronize time for all parties.

Examples

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

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

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.
ip mobile proxy-host	Configures the proxy Mobile IP attributes of the PDSN.

ip mobile tunnel

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

ip mobile tunnel {**crypto map** *map-name* | **route-cache** | **path-mtu-discovery** | **nat** {**inside** | **outside**}}

Syntax Description

crypto map	Enables encryption/decryption on new tunnels.
map-name	Specifies the name of the crypto map.
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.
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.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

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.

Examples

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

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

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** ***addr*****]**

no ip mobile virtual-network *net mask* **[address** ***addr*****]**

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 *addr*	(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 address keyword was added.

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 HA IP address is configured on the loopback interface for that virtual network:

```
Router# ip mobile virtual-network

int e0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

int lo0
 ip addr 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
```

radius-server host

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]

no radius-server host {*hostname* | *ip-address*}

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port	Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

Defaults

The **auth-port** port number defaults to 1645; the **acct-port** port number defaults to 1646.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XC	This command was introduced.

Examples

The following example shows the **radius-server host** command:

```
Router# radius server host 20.1.1.1
```

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

Examples

The following example enables Mobile IP:

```
Router# router mobile
```

show ip mobile binding

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

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

Syntax Description

ip address	IP address of the Home agent
home-agent *address*	(Optional) IP address of mobile node.
nai *string*	(Optional) Network access identifier.
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.
12.2(2)XC	The **nai** 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 5 describes the significant fields shown in the display.

Table 5 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.
Src Addr	IP source address of the Registration Request as received by the home agent. Will be either the collocated 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.
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 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.

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 6 describes the significant fields shown in the display.

Table 6 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	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 station counters and information, use the **show ip mobile host** EXEC command.

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.

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 7 describes the significant fields shown in the display.

Table 7 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.
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).
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 mobile station	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from mobile station	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 8 describes the significant fields shown in the display.

Table 8 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.

Table 8 show ip mobile host group Field Descriptions (continued)

Field	Description
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.
clear ip mobile host-counters	Clears the mobile station-specific counters.

show ip mobile secure

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

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

Syntax Description

host	Displays security association of the mobile host on the home agent.
home-agent	Displays security association of the remote home agent on the foreign agent.
summary	Displays all values in the table.
address	IP address.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** and **proxy-host** keywords were added.

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 9 describes the significant fields shown in the display.

Table 9 show ip mobile secure Field Descriptions

Field	Description
IP address	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.
Prefix-suffix	Authentication mode.

Table 9 show ip mobile secure Field Descriptions (continued)

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

show ip mobile traffic

To display Home Agent 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 (0) 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 requests rcvd 7242, denied 2, ignored 0, dropped 0, replied 7242
    Register requests accepted 7240, No simultaneous bindings 0
    Register requests rcvd initial 7241, re-register 0, de-register 1
    Register requests accepted initial 7239, re-register 0, de-register 1
    Register requests replied 7241, de-register 1
    Register requests denied initial 2, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 2, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 0, sent 0 total 0 fail 0
    Binding Update acks received 0 sent 0
    Binding info requests 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
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
```

Table 10 describes the significant fields shown in the display.

Table 10 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 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).

Table 10 show ip mobile traffic Field Descriptions (continued)

Field	Description
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.
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 violation

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

show ip mobile violation [*address* | **nai** *string*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated parameters were added.

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 11 describes significant fields shown in the display.

Table 11 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.

Table 11 show ip mobile violation Field Descriptions (continued)

Field	Description
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.
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply.
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

snmp-server enable traps ipmobile

To configure Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the no form of this command.

snmp-server enable traps ipmobile

no snmp-server enable traps ipmobile

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global Configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at

http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

Debug Commands

This section identifies the debug commands for the Cisco Mobile Wireless Home Agent. For more information, refer to the *Cisco IOS Debug Command Reference*.

- **debug ip mobile advertise**
- **debug ip mobile host**
- **debug ip mobile redundancy**

debug ip mobile advertise

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

debug ip mobile advertise

no debug ip mobile advertise

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command History

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

Examples

The following is sample output from the **debug ip mobile advertise** command. Table 12 describes significant fields shown in the display.

```
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 12 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*

no debug ip mobile host

Syntax Description

acl	(Optional) Access list.

Defaults

No default values.

Command History

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

Examples

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
```

debug ip mobile redundancy

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

debug ip mobile redundancy

no debug ip mobile redundancy

Syntax Description

This command has no keywords or arguments.

Defaults

No default values.

Command History

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

Examples

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

```
Router# debug ip mobile redundancy

00:19:21: MobileIP: Adding MN service flags to bindupdate
00:19:21: MobileIP:  Adding MN service flags 0 init registration flags 1
00:19:21: MobileIP: Adding a hared version cvse - bindupdate
00:19:21: MobileIP: HARelayBindUpdate version number 2MobileIP: MN 40.0.0.20 - sent
BindUpd to HA 7.0.0.3 HAA 7.0.0.4
00:19:21: MobileIP: HA standby maint started - cnt 1
00:19:21: MobileIP: MN 40.0.0.20 - HA rcv BindUpdAck accept from 7.0.0.3 HAA 7.0.0.4
00:19:22: MobileIP: HA standby maint started - cnt 1
```

Glossary

3GPP2—3rd Generation Partnership Project 2

AAA—Authentication, Authorization and Accounting

AH—Authentication Header

APN—Access Point Name

BG—Border Gateway

BSC—Base Station Controller

BSS—Base Station Subsystem

BTS—Base Transceiver Station

CHAP—Challenge Handshake Authentication Protocol

CoA—Care-Of Address

DSCP—Differentiated Services Code Point

DNS—Domain Name Server

ESN—Electronic Serial Number

FA—Foreign Agent

FAC—Foreign Agent Challenge (also FA-CHAP)

HA—Home Agent

HDLC—High-Level Data Link Control

HLR—Home Location Register

HSRP—Hot Standby Router Protocol

IP—Internet Protocol

IPCP—IP Control Protocol

IS835—

ISP—Internet Service Provider

ITU—International Telecommunications Union

L2_Relay—Layer Two Relay protocol (Cisco proprietary)

L2TP—Layer 2 Tunneling Protocol

LCP—Link Control Protocol

LNS—L2TP Network Server

MAC—Medium Access Control

MIP—Mobile IP

MS—Mobile Station (= TE + MT)

MT—Mobile Termination

NAI—Network Access Identifier

NAS—Network Access Server

P-MIP—Proxy-Mobile IP

PAP—Password Authentication Protocol

PCF—Packet Control Function

PDN—Packet Data Network

PDSN—Packet Data Serving Node

PPP—Point-to-Point Protocol

PPTP—Point-to-Point Tunneling Protocol

SLA—Service Level Agreement

TE—Terminal Equipment

TID—Tunnel Identifier

VPDN—Virtual Packet Data Network