



# Cisco Mobile Wireless Home Agent Release 2.1

## 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.
12.2(8)ZB1	This feature was introduced on the Cisco 7600 series Internet router.
12.2(8)ZB6	Two CLI commands were modified.
12.2(8)ZB7	One new CLI command.
12.3(7)XJ	Release 2.0 of the Cisco Mobile Wireless Home Agent
12.3(7)XJ1	Two CLI commands were modified.
12.3(8)XW	Support for ACLs on Tunnel Interface was added.
12.3(11)YF	Release 2.1 of the Cisco Mobile Wireless Home Agent

This document 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, page 2](#)
- [System Overview, page 2](#)
- [Cisco Home Agent Network, page 3](#)
- [Packet Data Services, page 5](#)
- [Features, page 8](#)
- [The Home Agent, page 10](#)
- [Supported Platforms, page 41](#)
- [Supported Standards, MIBs, and RFCs, page 43](#)
- [Configuration Tasks, page 44](#)
- [Monitoring and Maintaining the HA, page 59](#)
- [Configuration Examples, page 60](#)

# Feature Overview

Cisco's Mobile Wireless Packet Data Solution includes the Packet Data Serving Node (PDSN) with Foreign Agent (FA) functionality, the Cisco Mobile Wireless Home Agent (HA), Authentication, Authorization and Accounting (AAA) servers, and several other security products and features. The solution is standards compliant, and is designed to meet the needs of the 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 through the Home Agent. With reverse tunneling, traffic from the terminal is also routed through 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, Catalyst 6500 switches, and Cisco 7600 Internet routers, and acts as an access gateway for Simple IP and Mobile IP stations. It provides FA support and packet transport for virtual private networking (VPN). It also acts as a 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

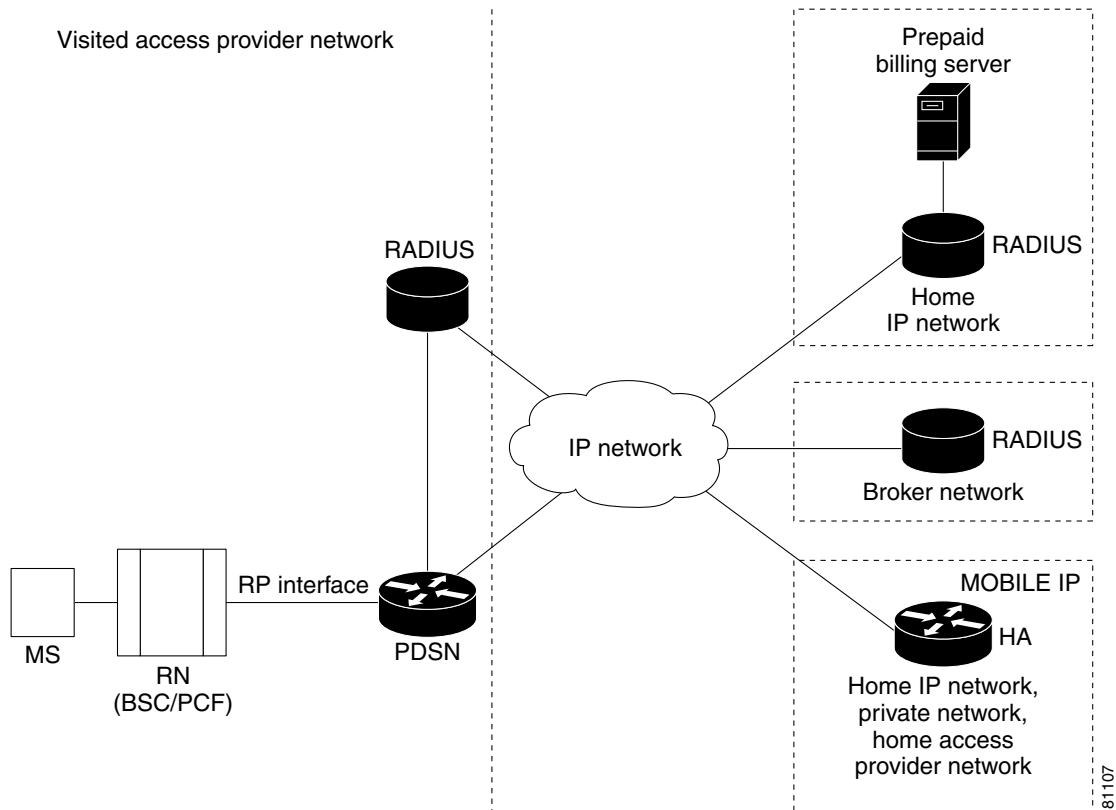
CDMA is one of the standards for mobile communication. A typical CDMA2000 network includes terminal equipment, mobile termination, base transceiver stations (BTSs), base station controllers (BSCs), PDSNs, and other CDMA network and data network entities. The PDSN is the interface between a BSC and a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

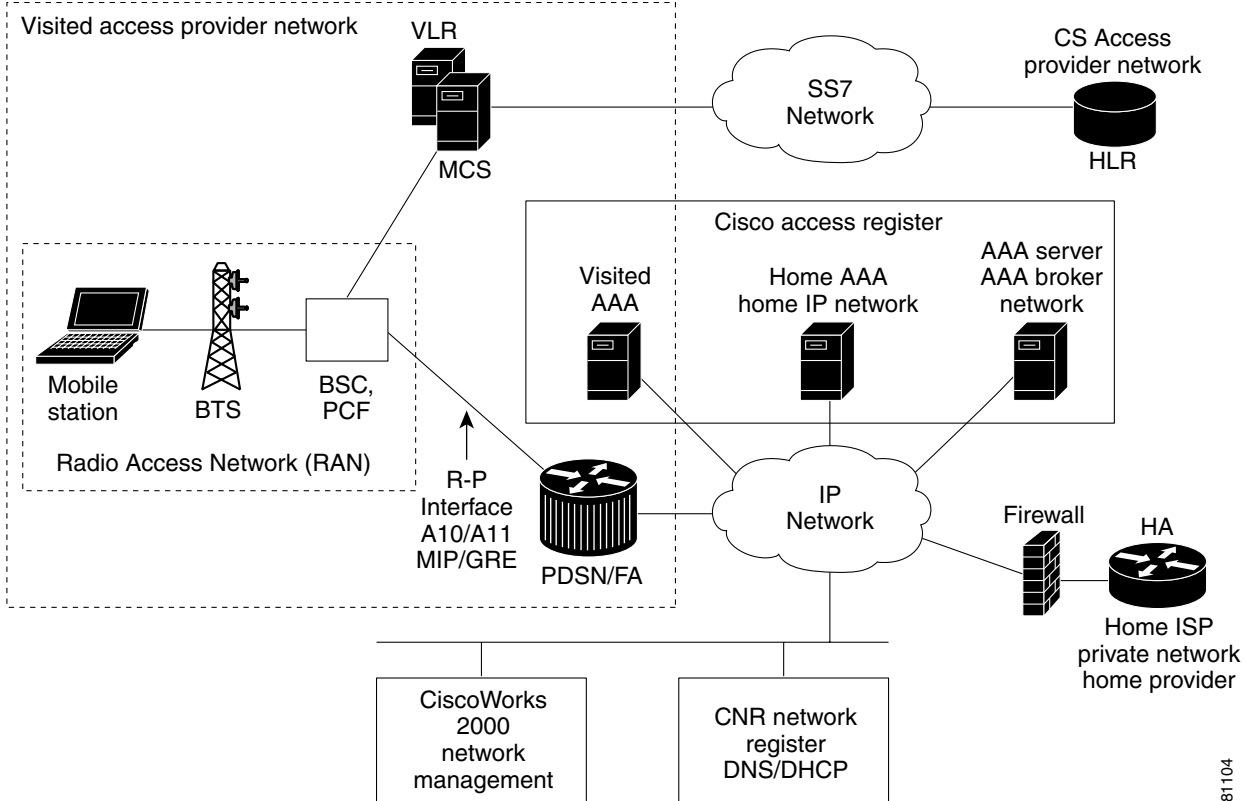


The Home Agent, then, is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic is routed through the Home Agent, and the Home Agent also provides Proxy ARP services. In the case of reverse tunneling, traffic from the terminal is also routed through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

81104

For Mobile IP and Proxy-Mobile IP types of access, these solutions allow a mobile user to roam within and beyond its service provider boundaries, while always being reachable and addressable through the IP address assigned on initial session establishment. Details of Mobile IP and Proxy Mobile IP Services can be found in the [Packet Data Services](#) section that follows.

## Packet Data Services

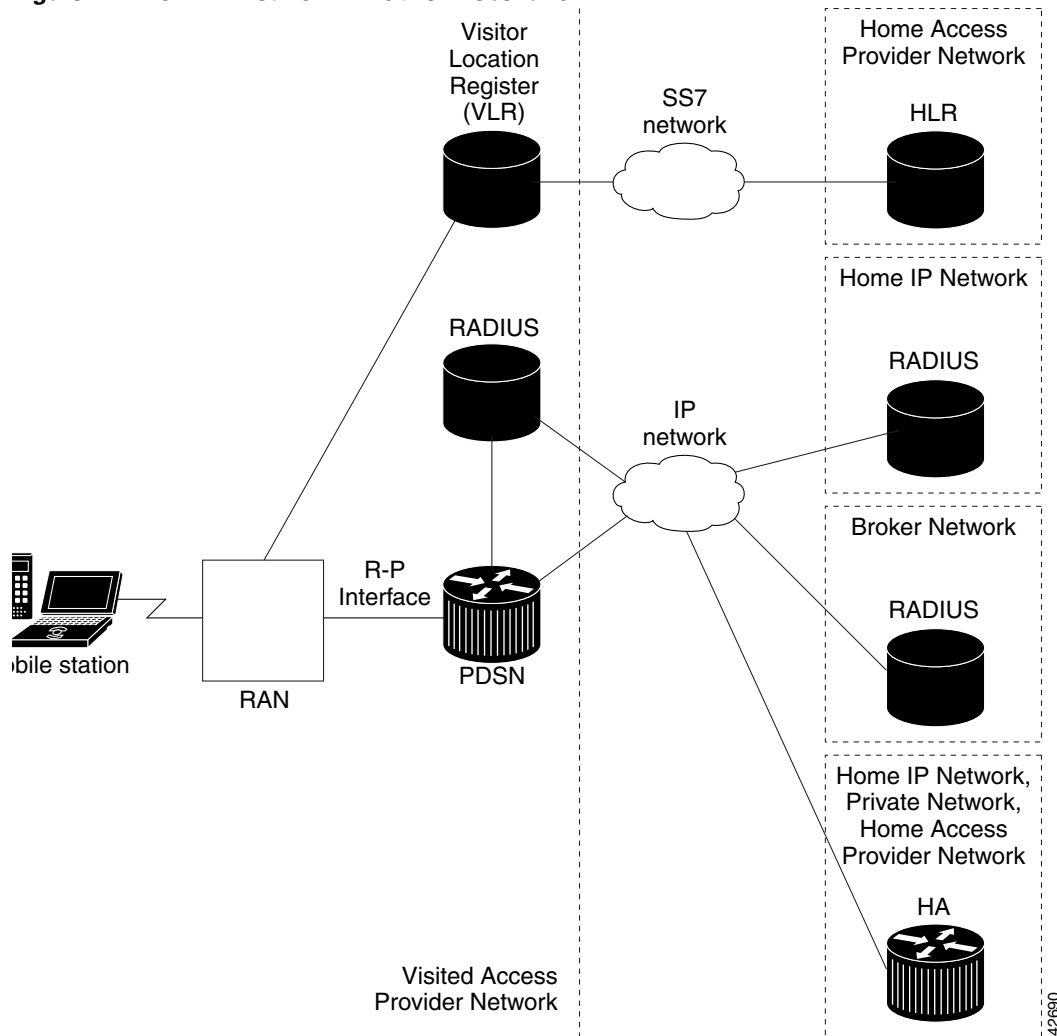
In the context of a CDMA2000 network, the Cisco Home Agent supports two types of packet data services: Mobile IP and Proxy Mobile IP services. From the perspective of the Cisco Home Agent, these services are identical.

### 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



The communication process occurs in the following order:

1. The mobile station registers with its Home Agent (HA) through an 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 renegotiated 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 12.3 documentation modules *Cisco IOS IP Configuration Guide* and *Cisco IOS IP Command Reference*. RFC 2002 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

For certain service providers there is a lack of commercially available Mobile IP client software, while 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 IP control protocol (IPCP).
6. A tunnel is established between the Cisco HA and the FA, or 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

## New Features in Release 2.1

This section describes features that were introduced or modified in Home Agent Release 2.1.

- [Mobile IPv4 Registration Revocation, page 10](#)
- [HA Server Load Balancing, page 12](#)
- [HA Accounting, page 14](#)
- [Skip HA-CHAP with MN-FA Challenge Extension \(MFCE\), page 16](#)
- [VRF Support on HA, page 16](#)
- [Hot-lining, page 19](#)
- [Radius Disconnect, page 21](#)
- [Conditional Debugging, page 21](#)
- [Dynamic Home Agent Assignment, page 22](#)
- [Home Agent Redundancy, page 23](#)
- [Virtual Networks, page 28](#)
- [Home Address Assignment, page 29](#)
- [On-Demand Address Pool \(ODAP\), page 32](#)
- [Mobile IP IPSec, page 33](#)
- [Support for ACLs on Tunnel Interface, page 37](#)
- [Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY, page 38](#)

This section describes key features from previous releases of the Cisco Home Agent:

- [3 DES Encryption, page 33](#)
- [User Profiles, page 38](#)
- [Mobility Binding Association, page 39](#)
- [User Authentication and Authorization, page 39](#)
- [HA Binding Update, page 40](#)
- [Packet Filtering, page 40](#)
- [Security, page 40](#)

## Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7200 series router, Cisco 6500 series switch, or Cisco 7600 series router, 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 Network Access Identifiers (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 time stamps. Nonce-based replay protection is not supported

## Benefits

- 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), unencapsulates 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 Care-of Address (CoA) with the home address, NAI, and security keys 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 (through 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 (through 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 7600, 7200, and 6500 series platforms. A Cisco HA based on the Cisco 7200 series router supports up to 262,000 mobile bindings, can process 100 bindings per second, and is RFC 2002, RFC 2003, RFC 2005 and RFC2006 compliant.

A Cisco HA based on the Cisco 7600 series router or Cisco Catalyst 6500 switch, with two MWAM cards housing five active HA images and five 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>.

## Mobile IPv4 Registration Revocation

Basic Mobile IP resource revocation is an IS-835-C initiative that defines the methods by which a mobility agent (one that provides Mobile IP services to a mobile node) can notify the other mobility agent of the termination of a registration due to administrative reasons or MIP handoff.

This feature is similar to the Cisco MobileIP Bind Update feature. When a mobile changes its point of attachment (FA), or needs to terminate the session administratively, the HA sends a registration revocation message to the old FA. The old FA tears down the session and sends registration revocation acknowledgement message to the HA. In another scenario, if the PDSN/FA needs to terminate the session administratively, the FA sends registration revocation message to the HA. The HA deletes the binding for the mobile and sends registration revocation acknowledgement to FA.

An HA configured to support registration revocation in Mobile IPv4 includes a revocation support extension in all MIP RRP for the associated MIP RRQ from the PDSN that contained a valid registration revocation extension. A registration for which the HA received a revocation support extension, and responded with a subsequent revocation support extension, is considered revocable by the HA.

The following sample call flow illustrates Mobile IP Resource Revocation (Registration phase):

- 
- Step 1** The MS originates a call and PPP session is up.
  - Step 2** The PDSN/FA has been configured to advertise MIPv4 registration revocation support. The PDSN/FA sends advertisement with MIPv4 Registration revocation support bit “X” set.
  - Step 3** The PDSN/FA receives MIP RRQ from MN, includes STC attribute set to **2** in access-request during FA-CHAP. While forwarding the RRQ to the HA, the revocation support extension is appended after the MHAЕ. The I-bit in the revocation support extension will be set to **1** indicating that the MS would get an explicit notification on revocation of the binding whenever necessary.
  - Step 4** The HA, upon receiving the MIP RRQ containing a revocation extension, will send back the MIP RRP including a revocation support extension and setting the I-bit equal to the value received in the MIP RRQ. In case of HA-CHAP (MN-AAA authentication), the STC attribute, with a value of **2**, will be included in the access-request sent to AAA.
  - Step 5** The PDSN receives the MIP RRP containing a revocation support extension, and the data flow is considered to be revocable.
- 

The following sample call flow illustrates Mobile IP Resource Revocation (HA initiated):

- 
- Step 1** Mobile starts a mobile IP data session with PDSN/FA (1).
  - Step 2** PDSN/FA (1) appends registration revocation support extension to the mobile registration request and forwards it to the HA.
  - Step 3** In response, the HA appends the registration revocation support extension to a registration reply, and send it to PDSN/FA (1).
  - Step 4** PDSN-to-PDSN handoff occurs, and the Mobile re-starts a mobile IP data session with PDSN/FA (2).
  - Step 5** PDSN/FA(2) sends registration request to the HA.
  - Step 6** The HA sends registration response to PDSN/FA (2).
  - Step 7** The HA sends Mobile IP resource revocation message to PDSN/FA (1).
  - Step 8** PDSN/FA (1) sends Mobile IP resource revocation acknowledgement to the HA, and terminates the mobile ip data session for the mobile.
- 

The following call flow illustrates a Mobile IP Resource Revocation (FA initiated revocation):

- 
- Step 1** The Mobile starts a mobile IP data session with the PDSN/FA.
  - Step 2** The PDSN/FA appends the registration revocation support extension to the mobile registration request, and forwards it to the HA.
  - Step 3** In response, the HA appends the registration revocation support extension to a registration reply, and sends it to the PDSN/FA.
  - Step 4** Some event occurs in the PDSN/FA, and the PDSN/FA decides to close the session.

- Step 5** The PDSN/FA sends a Mobile IP resource revocation message to the HA.
- Step 6** The HA sends a Mobile IP resource revocation acknowledgement to the HA. The HA clears the binding and the PDSN/FA clears the session.
- 

## I-bit Support

The I (Inform) bit is used during the registration revocation phase to notify the mobile node (MN) of the revoked data service in cases where the mobile node has more than one MobileIP flows. If, during the registration phase, this bit is set to **1** by a mobility agent in the revocation support extension in the RRQ/RRP, it indicates that the agent supports the use of the “I” bit in revocation messages.

In the current implementation, if MobileIP RRQ is received with I bit set in the revocation support extension, then the HA will also set the I-bit to **1**, and the I-bit shall be considered to be used during the revocation phase. When the HA initiates revocation, and if the I bit was negotiated, it shall set the I bit to **1** in the Revocation message if a binding is administratively released, and will set it to **0** if an inter-PDSN handoff is detected by the HA. When revocation is initiated by the PDSN, and the revocation message has I-bit set to **1**, then the HA will also set the I-bit to **1** in the revocation ACK message.

## Mobile IPv4 Resource Revocation Restrictions

The following list identifies the restrictions for Mobile IPv4 Resource Revocation feature for the current release:

- The STC attribute received in access-accept during HA-CHAP (MN-AAA authentication) is ignored, and the feature configuration on the Home Agent will take precedence.
- The Revocation message, Revocation ACK message, and Revocation support extension (not protected by either FHAE or IPSec) will not be discarded, but will be processed. We recommend that you configure an FA-HA security association on the Home Agent, or that an IPSec tunnel exists between the FA and the HA.
- Resource Revocation and Bind Update cannot be enabled simultaneously. Both are mutually exclusive of each other.
- The Home Agent MIB is not updated with the Registration revocation information.
- Mobile IP conditional debugging is not supported.

## HA Server Load Balancing

The HA-Server Load Balancing (HA-SLB) feature is built upon the existing IOS Server Load Balancing (SLB) feature. SLB allows users to represent a group of network servers (a server farm) as a single server instance, balance the traffic to the servers, and limit traffic to individual servers. The single server instance that represents a server farm is referred to as a virtual server. The servers that comprise the server farm are referred to as real servers.

SLB can distribute the traffic to real servers through mechanisms like round robin to real servers. Additionally, it can monitor the health of each real server using the Dynamic Feedback Protocol, choose a server that has the least load, and choose a server that is up and running. Please refer to the following URL for more information on SLB architecture:

[http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps5940/prod\\_white\\_paper0900aecd802921f0.html](http://www.cisco.com/en/US/prod/collateral/wireless/wirelssw/ps5940/prod_white_paper0900aecd802921f0.html)

The HA-SLB feature is available on the 6500 and 7600 series platforms. This feature allows a set of real Home Agents, each running on an MWAM, to be identified by a single virtual server IP address residing on 6500 and 7600 Supervisor.

PDSN/FAs send an initial registration request for a user to the virtual server IP address. HA-SLB running on the SUP intercepts the packets and forwards the registration request to one of the real Home Agents.

A typical call flow would have the following sequence of events:

- 
- Step 1** PDSN/FA forwards a Mobile IP RRQ to virtual server IP address (HA-SLB). If the AAA server returns the HA address to the PDSN/FA, the AAA server must be configured to return the address of virtual server IP address.
- Step 2** SLB picks one of the real server/HAs from its serverfarm and it delivers Mobile IP RRQ to this server.
- Step 3** The real HA responds to MobileIP RRQ with a Reply, the message is sent from the real HA to the PDSN/FA. The HA-SLB does not intercept this packet. The real HA creates binding and local tunnel endpoint.
- Step 4** The PDSN/FA creates a visitor table entry and local tunnel endpoint, and sends/receives traffic through the tunnel directly from Real HA
- Step 5** The PDSN/FA sends a Mobile IP RRQ with lifetime of “0” to the real HA to close the binding.




---

**Note** The packet is not sent to virtual IP address (HA-SLB)

---

- Step 6** The Real HA sends Mobile IP RRP to PDSN/FA. The HA-SLB does not intercept this packet. Real HA closes the binding.




---

**Note** The Mobile IP Messages are not compliant with RFC 2002. But they are compliant to draft-kulkarni-mobile-ip-dynamic-ha-assignment-frmwrk-00.txt.

---

RRQs destined to the HA/SLB virtual IP address, with an HA address of 0.0.0.0 or 255.255.255.255, are forwarded to the actual HA using a weighted “round-robin,” load balancing algorithm. The SLB mechanism supports Dynamic Feedback Protocol (DFP) that gives real servers the ability to communicate real server health to the load balancer, thereby adjusting the weight of the real server in the load balancing algorithms.

Since the MN can send multiple RRQs before it hears a RRP from the HA (either the MN power cycles after sending an initial RRQ, or it is mis-configured to send multiple initial registrations, or RRP is dropped by the network), it is important to keep track of registrations coming from the same MN. This avoids the case where the same MN is registered at multiple HAs, and wastes IP addresses and other resources at those HAs. To solve this problem, HA-SLB would parse the RRQ and create a session object indexed by the MNs NAI. This session object will store the real HA IP address where the RRQ was forwarded. Subsequent registrations from the same MN will be forwarded to this same real HA. The session object will be stored for a configurable period of time (default to 10 seconds). If the HA-SLB does not see a RRQ from the MN within this period of time, the session object is cleared. If HA-SLB sees a RRQ, the timer associated with the session object is reset.

A retry counter is associated with each session object, and is incremented for each re-transmitted RRQ seen by the load balancer. If the number of retries seen is greater than the configured “reassign” threshold, the session sending the retransmissions will be re-assigned to another real HA, and a connection failure is recorded for the original real HA. Real servers are assumed to be down and no more

RRQs re-directed to them when enough connection failures are seen to reach a configured threshold. HA-SLB will restart directing sessions to that real server after a configurable time interval or if the real server sends a DFP message to HA-SLB.

## Load Balancing in HA-SLB

HA-SLB uses a weighted round-robin load-balancing algorithm. This algorithm specifies that the real server used for a new connection to the virtual server is chosen from the server farm in a circular fashion. Each real server is assigned a weight  $n$ , that represents its capacity to handle connections, as compared to the other real servers associated with the virtual server. As an example, assume a server farm comprised of real server ServerA with  $n = 3$ , ServerB with  $n = 1$ , and ServerC with  $n = 2$ . The first three RRQs to the virtual server are assigned to ServerA, the fourth RRQ to ServerB, and the fifth and sixth RRQs to ServerC.

It is possible to configure IOS SLB for either static or dynamic load balancing. Static load balancing is achieved by assigning weights statically to each HA in the server farm. Dynamic load balancing is achieved by configuring Dynamic Feedback Protocol (DFP), with the DFP manager on SLB, and the DFP client on each of the real HAs.

## HA-SLB Operating Modes

HA-SLB operates in two modes, Dispatched mode and Direct (NAT server) mode.

In Dispatched mode the virtual server address is known to the HAs. HA-SLB will simply redirect packets to the HAs at the MAC layer. This requires the HAs to be layer 2 adjacent to SLB.

In Direct mode, HA-SLB works in NAT server mode and routes the RRQs to the HAs by changing the destination IP address in the RRQ to that of the real server. As a result the HAs need not be layer 2 adjacent to SLB.

## HA Accounting

This feature is primarily developed to allow the HA to interoperate with the Service Selection Gateway (SSG) in the CMX solution. However, this feature can also be used without SSG interaction. The HA Accounting feature includes the following activities:

- HA will send Accounting Start record when the first binding for a mobile is created
- HA will send Accounting Stop record when the last binding for a mobile is deleted
- HA will send Accounting Update when Handoff occurs

The following attributes will be sent in Accounting Records:

- NAI in Username attribute (1)
- MN IP Address in Framed IP Address attribute (8)
- FA IP Address in Tunnel End Point attribute (66)
- Home Agent IP Address in NAS IP Address attribute (4)
- Accounting Status Type attribute (40)
- Accounting Session ID (44)
- Accounting Terminate Cause(49) - only in accounting stop
- Accounting Delay Time (41)

## Basic Accounting Messages

Home Agent Release 2.1 supports the Cisco Service Selection Gateway (SSG). In this release, the HA sends only three accounting messages without statistics information. The SSG is designed and deployed in such a way that all the network traffic passes through it.

Since all the traffic passes through the SSG, it has all of the statistical information; however, it does not have Mobile IP session information. The Home Agent has the Mobile IP session information, and sends that information to the SSG.

The HA sends the following messages to the SSG/AAA server:

- **Accounting Start:** The HA sends this message to the SSG/AAA server when:
  - A MN successfully registers for the first time. This indicates the start of new Mobile IP session for a MN.
  - In case of redundant HA configuration, a stand-by HA will send Accounting Start message only when it becomes active and it does not have any prior bindings. This allows the SSG to maintain host objects for MNs on failed HA. However, redundancy is not supported in Phase-1.
- **Accounting Update:** The HA generates this message when the MN changes point of attachment (POA) in the mobile network. For a Mobile IP session, this corresponds to a successful re-registration from an MN when it changes its Care-Of-Address (COA).
- **Accounting Stop:** The HA sends this message to indicate that the Mobile IP session has ended. This can happen in Mobile IP session when:
  - The MN's lifetime expires.
  - The MN sends a successful de-registration request.
  - Home Agent is unconfigured by the HA administrator.

All the messages contain the following information:

- **Network Access Identifier (NAI):** This is the MN's name. It looks something like abc@service\_provider1.com
- **Network Access Server (NAS) IP:** This is the accounting node's IP address. Since HA is the accounting node, this field carries HA address.
- **Framed IP Address:** This is the IP address of the MN. Typically the HA will allot an IP address to a MN after successful registration.
- **Point Of Attachment (POA):** This field indicates the Point of attachment for the MN on the network. For Mobile IP session, this is MN's Care-Of-Address (COA).

## Messages Not Sent By Mobile IP Home Agent

The following messages are not sent by Mobile IP Home Agent.

- **Accounting On Message (Acct-Status-Type=Accounting-On)** when the HA box comes online or boots up: This message is a global entity for the platform, irrespective of Mobile IP configuration. This message is typically implemented by the platform code during initialization, and not by service such as Mobile IP.
- **Accounting Off Message (Acct-Status-Type=Accounting-Off)** when the HA box is shutdown: This message is also global entity for the platform, irrespective of Mobile IP configuration. This message is typically implemented by the platform code during reboot, and not by service such as Mobile IP.

## HA Accounting Restrictions

The following list identifies the restrictions for the HA Accounting feature for the current release:

- HA Accounting does not work with HA Redundancy.

## Skip HA-CHAP with MN-FA Challenge Extension (MFCE)

This feature allows the HA to download a Security Association (SA) and cache it locally on the disk, rather than performing a HA-CHAP procedure with Home AAA server to download the SA for the user for each registration request. When a user first registers with the HA, the HA does HA-CHAP (MN-AAA authentication), downloads the SA, and caches it locally. On subsequent re-registration requests, the HA uses the locally cached SA to authenticate the user. The SA cache entry is removed when the binding for the user is deleted.

## VRF Support on HA

The HA supports overlapping IP address for mobile nodes for the mobile IP flows that are opened for different realms. This feature is based on the Multi-VPN Routing and Forwarding (VRF) CE network architecture, and expands the BGP/MPLS VPN architecture to support multiple VPNs (and therefore multiple customers) per Customer Edge (CE) device. This reduces the amount of equipment required, and simplifies administration, while allowing the use of overlapping IP address spaces within the CE network.

Multi-VRF CE is a new feature, introduced in Cisco IOS release 12.2(4)T, that addresses these issues. Multi-VRF CE, also known as VRF-Lite, extends limited PE functionality to a Customer Edge (CE) router in an MPLS-VPN model. A CE router now has the ability to maintain separate VRF tables in order to extend the privacy and security of an MPLS-VPN down to a branch office rather than just at the PE router node. The CE can support traffic separation between customer networks, or between entities within a single customer network. Each VRF on the CE router is mapped to a corresponding VRF on the PE router.

For more information on Multi-VRF CE network architecture, please refer to Cisco Product Bulletin 1575 at the following URL: [http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575\\_pp.pdf](http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575_pp.pdf).

**Figure 5 VRF-Lite in the Cisco PDSN/Home Agent Architecture**

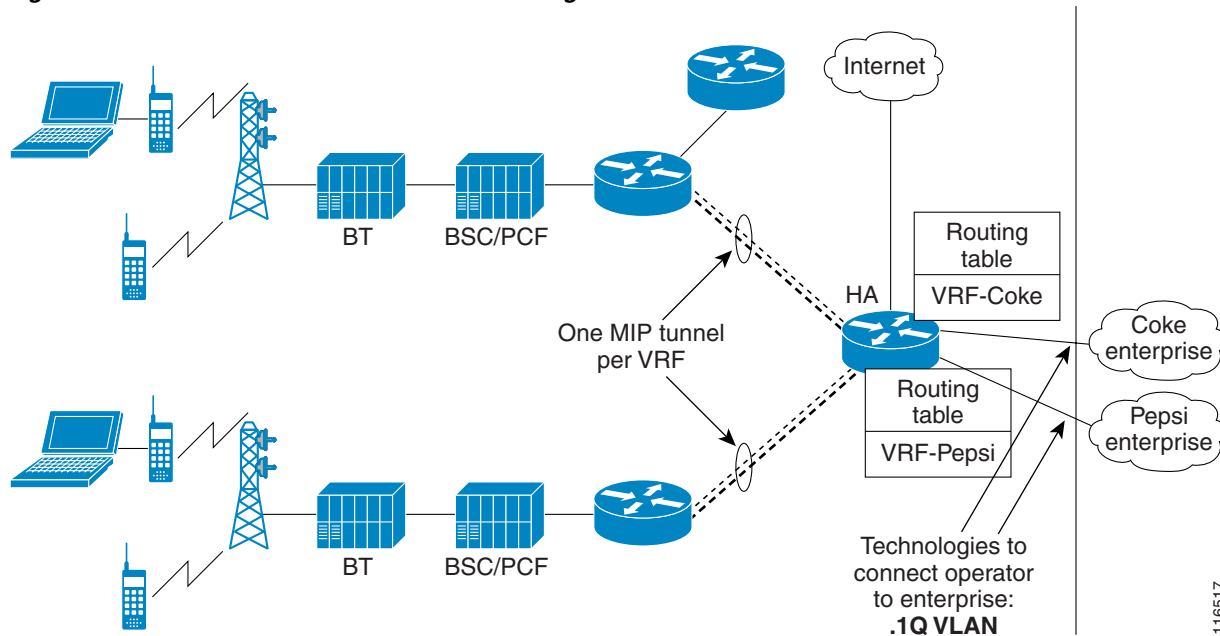


Figure 5 illustrates the PDSN architecture and how the VRF-lite solution is applied to the Home Agent for different realms/enterprises, thus segregating data between the enterprises.

Highlights of the VRF solution include the following:

- Provides a method to identify VRF of the user that is based on domain/realm of the user.
- Provides a method to ensure delivery of packets to the mobile through the PDSN, when different mobiles belonging to different enterprises share the same overlapping IP address.
- Supports IP address and routing table management per VRF.
- Supports management of VRF per enterprise/domain.
- Supports AAA authentication and accounting group per VRF.

The realm is used to identify an enterprise network. One virtual Home Agent is configured per realm. NAI is part of Mobile IP RRQ, and is the main identifier of mobile IP users in the PDSN and HA. The realm part of NAI will be used to identify the virtual Home Agent. Mobile nodes follow the NAI convention of *username@company*, where *company* identifies a realm name that indicates a subscriber community.

Multiple IP addresses are used at the HA to indicate different enterprise connections or VRFs to the PDSN. Thus, there will be one mobile IP tunnel between the PDSN and the HA per realm/VRF.

For an HA that is connected to two enterprises, “abc.com” and “xyz.com,” the HA will be configured with two unique IP addresses (typically configured under a loopback interface). The PDSN will have a MoIP tunnel to an address LA1 to reach “abc.com,” and will have another MoIP tunnel to address LA2 to reach “xyz.com,” where LA1 and LA2 are IP addresses configured under a Loopback interface.

On the home AAA RADIUS server, NAI/domain configuration ensures that the PDSN receives LA1 as the IP address of the Home Agent of enterprise “xyz.com” as part of the Access Response during FA-CHAP or HA-CHAP (MN-AAA authentication); and LA2 as the IP address of Home Agent of enterprise “mnp.com”.

This feature will work with HA-SLB solution for HA load balancing.

## Mobile IP Tunnel Establishment

The following procedure describes a mobile IP flow establishment with HA-SLB and VRF enabled. Elements in this call flow are two Mobile nodes (MN-1 and MN-2) belonging to enterprise ENT-1 & ENT-2 respectively:

- 
- Step 1** When a Mobile IP RRQ arrives at the HA, the HA will read the NAI field of the incoming RRQ, and select a pre-configured IP address to form a Mobile IP tunnel back to the PDSN using this IP address as the source address of the tunnel.
- Step 2** The “Home-Agent address” field in the RRP that is being sent to the PDSN is modified to the IP address as described above.
- Step 3** The Home Agent adds a host route corresponding to the IP address assigned for the mobile in the routing table corresponding to the VRF defined for the realm.
- Step 4** The tunnel end-point at HA is also inserted in the VRF routing table. This enables the mobiles to share common IP address across different realms on the same Home Agent.
- Step 5** MN-1 sends Mobile IP RRQ with Home Agent address set to 0.0.0.0 (dynamic Home Agent) to PDSN over its R-P session.
- Step 6** PDSN initiates FA-CHAP and sends an Access Request to AAA.
- Step 7** AAA responds with Access Response, Home Agent address returned is the IP address of HA-SLB.
- Step 8** PDSN forwards MIP RRQ to HA-SLB.
- Step 9** HA-SLB determines real HA based on load, and forwards the RRQ to HA1.
- Step 10** HA-1 receives the MIP RRQ. It parses the NAI inside the message and determines the VRF of the user based on its realm - enterprise Ent-1. It performs HA-CHAP (MN-AAA authentication), allocates IP address to mobile for Ent-1. It creates a binding for the mobile and populates VRF specific data structures like route entry in route-table of VRF, FIB, etc.
- Step 11** HA1 sends MIP RRP to PDSN, and also establishes mobile IP tunnel between PDSN and HA. End point of the tunnel on HA is L1-IP-1 (rather than IP address of ingress interface in the MIP RRQ).
- 

## VRF Feature Restrictions

The following list identifies restrictions for the VRF feature:

- Only static IP routing between Home Agent and the CE devices is supported. Dynamic routing protocols (for example, OSPF) are not supported to redistribute mobile routes that are added in Home Agent.
- A maximum of 200 VRFs per Home Agent is supported.
- Home Agent MIB is not updated with the VRF information.

## Authentication and Accounting Server Groups Per Realm

Separate authentication and accounting groups can be specified across different realms. Based on the realm of the user, the HA will choose the AAA authentication server based on the authentication group specified for the realm on the HA. Similarly, the HA will choose a AAA accounting server based on the realm of the user if the accounting group is specified for the realm.

**Note**

---

This feature will work in conjunction with the VRF feature.

---

## Hot-lining

HA Release 2.0 (and above) supports hot-lining for mobile nodes based on the Nortel X31-20031013-0xx (October 2003). The hot-lining feature enables you to monitor upstream user traffic using two different scenarios—active and new session. When hot-lining is active for a particular user, the upstream IP packets from the mobile are re-directed to the Re-direct server that is configured for this particular realm. Re-direction is achieved by changing the IP packet destination address to the Re-direct server address. The only mandatory attribute supported in the Change of Authorization (CoA) message from the HAAA is the User-Name attribute to identify the particular user on the Home Agent. Optionally, IP address can also be sent in the CoA message to identify the particular binding for a particular user.

## Active Session Hot-Lining

For active session Hot-lining, the user starts a packet data session. In the middle of the session it is hot-lined and after the account is reconciled, the hot-lining on the session is removed. Hot-lining is done with a RADIUS Change of Authorization (CoA) message. The following procedure lists the events for active session Hot-lining:

- 
- Step 1** Action for normal hot line profile is locally configured on HA.
  - Step 2** Action for active hot line profile is locally configured on HA.
  - Step 3** User joeusr@carrier.com is created at HAAA and assigned a normal hot line profile.
  - Step 4** User joeusr@carrier.com registers with HA.
  - Step 5** The HA sends an Access Request to the HAAA for the user.
  - Step 6** The HAAA responds with an Access Accept that contains a Filter-ID attribute set to normal.
  - Step 7** The HA applies normal hot line action (no redirection) for the user.
  - Step 8** The HA completes MIP registration by sending an RRP.
  - Step 9** Some event occurs at this point to cause the user to be hot lined. The user hot line profile at the HAAA is modified to active.
  - Step 10** The HAAA sends a Change of Authorization command with Filter-ID attribute set to active.
  - Step 11** The RADIUS client at the HA ACKs the Change of Authorization command.
  - Step 12** The HA applies active hot line action (redirection) for the user.

- Step 13** At this point, the user has taken action to reconcile the event that resulted in hot lining of the account. The hot line profile at the HAAA is modified to normal.
- Step 14** The HAAA sends a Change of Authorization command with Filter-ID attribute set to normal.
- Step 15** The RADIUS client at the HA ACKs the Change of Authorization command.
- Step 16** The HA applies normal hot line action (no redirection) for the user.
- 

## New Session Hot-Lining

For New Session Hot-lining, the user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session. The following procedure lists the events for New Session Hot-lining:

- Step 1** Action for normal hot line profile is locally configured on HA.
- Step 2** Action for active hot line profile is locally configured on HA.
- Step 3** User joeusr@carrier.com is created at HAAA and assigned an active hot line profile.
- Step 4** User joeusr@carrier.com registers with HA.
- Step 5** The RADIUS client sends an Access Request for the user.
- Step 6** The Access Accept contains the Filter-ID attribute set to active.
- Step 7** The HA applies active hot line action (redirection) for the user.
- 

## Restrictions for Hot-lining

The following list includes restrictions for the Hot-Lining feature:

- The Hot-lining feature supports only upstream IP packet level re-direction and downstream packets are not hot-lined. Firewall Hot-lining is not supported.
- The Home Agent does not support Correlation ID and NAS-Identifier attributes in the CoA request received from AAA.
- Hot Lining is not supported with HA redundancy.
- On the Home Agent, the hot-lining policy is applied only when the policy is downloaded during HA CHAP.
- The Home Agent will not reject the RRQ if Reverse-Tunnel is not requested by the user and hot lining policy is downloaded for the user.
- The Home Agent will not notify packet data users of the reason for their hot-lined status prior to denial of data service.
- The Home Agent MIB is not updated with the Hot-lining information.

## Radius Disconnect

Radius Disconnect (or Packet of Disconnect (PoD)) is a mechanism where in the RADIUS server can send a Radius Disconnect Message to the HA to release resources. Resources may be released for administrative purposes. Resources are mainly Mobile IP bindings on the HA.

Support for Radius Disconnect on the Cisco Home Agent is in conformance with RFC 3576. The HA communicates its resource management capabilities to the Home AAA server in an Access Request message sent for authentication/authorization procedure by including a 3GPP2 Vendor Specific Session Termination Capability (STC) VSA. The value communicated in the STC VSA will be obtained from configuration. The HA will also include NAS-Identifier attribute containing its Fully Qualified Domain Name (FQDN) in the Access Request when the **radius-server attribute 32 include-in-access-req format** CLI is configured.

The following approach is followed when a Disconnect Request is received on the HA:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Find the user session corresponding to the username (NAI).   |
| <b>Step 2</b> | If Framed-IP-Address attribute is received in the Disconnect Request, terminate the binding with corresponding to the address. |
| <b>Step 3</b> | If Framed-IP-Address is not received in the Disconnect Request, terminate all bindings for the user (NAI).                     |
- 

## Restrictions for RADIUS Disconnect

The following list includes restrictions for the RADIUS Disconnect feature:

- MIB is not updated with Radius Disconnect information.
- Mobile IP conditional debugging is not supported.

## Conditional Debugging

The HA supports conditional debugging based on NAI, as well as conditional debugging based on the MN's Home address. Only AAA and Mobile IP components will support conditional debugging.

To enable conditional debugging based on NAI, you must execute the **debug condition username *nai*** command.

To enable conditional debugging based on the MN's home address, you must execute the **debug condition ip *mn-ip-addr***.

The following MobileIP debugs are supported for conditional debugging :

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

The following AAA debugs are supported for conditional debugging :

- **debug aaa authentication**
- **debug aaa authorization**
- **debug aaa accounting**
- **debug aaa ipc**
- **debug aaa attr**
- **debug aaa id**
- **debug aaa subsys**

The following RADIUS debugs are supported for conditional debugging :

- **debug radius**
- **debug radius accounting**
- **debug radius authentication**
- **debug radius retransmit**
- **debug radius failover**
- **debug radius brief**

## 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 its own IP address in the Home Agent field. At this point, any re-registration requests 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). 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.



### Note

---

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

---

The Home Agent Redundancy feature is supported for Static IP Address assignment and IP Address assignment by AAA. Starting in Release 2.0, the Home Agent Redundancy feature is supported for Dynamic IP Address assignment using local IP address pools and Dynamic IP Address assignment using Proxy DHCP.

When Home Agent Redundancy is configured with Dynamic IP Address assignment using Proxy DHCP, the DHCP information is not synced with the standby while the bindings are brought up, even though the bindings are synced to the standby HA. However, when the standby HA becomes active, a DHCP request for each existing binding is sent out to the DHCP server in order to update the DHCP related information on this Home Agent.

The following features are not supported with HA redundancy:

- Hot-lining support on HA
- HA Accounting
- ODAP/DHCP and local pool addressing schemes are not supported with peer-peer redundancy

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 is lost and all MNs registered with the HA lose connectivity. To reduce the impact of an HA failure, Cisco IOS software supports the HA redundancy feature.



### Note

---

On configurations based on Cisco 7600 series or Catalyst 6500 series platforms, the backup Home Agent image is configured on a different MWAM card from 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 immediately and transparently recovers 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.

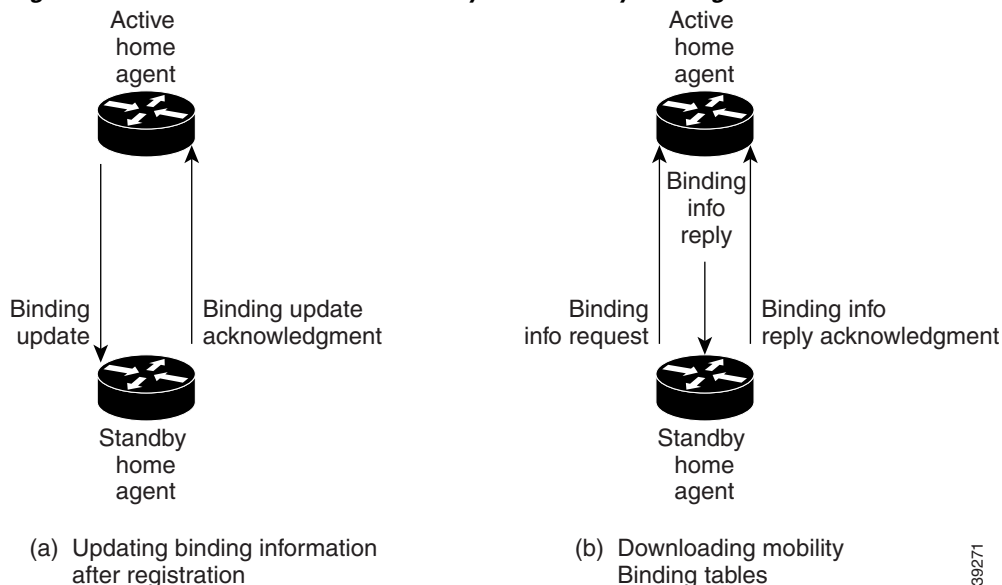
HA functionality is a service provided by the router and is not interface specific. Therefore, the HA and the MN must agree on which HA interface the MN should send its registration requests and, conversely, on which HA interface the HA should receive the registration requests. This agreement must factor 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 tables 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 6](#) 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 6 Overview of HA Redundancy and Mobility Binding Process****Note**

The active HA-standby HA can also be in peer HA-peer HA configuration.

## Support for Binding Deletion Synchrony

In the current implementation of Home Agent redundancy, bindings that are deleted on the active HA in active-standby mode (or on any peer in a peer to peer mode), due to receipt of a revocation message, a RADIUS disconnect message, or an administrative clear, are not synched to the standby HA or the peer HA. Also, the additional extensions and attributes for Revocation and Radius Disconnect are not relayed to the standby. In Cisco IOS release 12.3(7) XJ1, Registration Revocation, Radius Disconnect and Administrative clear using the **clear ip mobile binding** command are supported with HA redundancy. The following list identifies the benefits of this support:

### Active-Standby Mode of HA Redundancy:

- Bindings on the active HA that are deleted by trigger (for example, receipt of a Revocation message, a Radius Disconnect message, or an Administrative clear) will be synched to the Standby HA.
- Bindings that are deleted due to commands that unconfigure (for example, ip mobile host, etc.), will not be synched.
- Bindings that are deleted on the standby HA will not be synched to the active in case of active-standby mode.
- Additional extensions (Revocation Support Extension) and attributes (STC attribute) for Revocation and Radius Disconnect will be relayed to the standby HA.

**Peer-to-Peer Mode of HA Redundancy:**

- Bindings that are deleted on any of the peers by trigger (for instance, a receipt of Revocation message, a Radius Disconnect message, or an Administrative clear), will be synched to the other peer.
- Bindings that are deleted due to commands that unconfigure (for example, ip mobile host, etc.) will not be synched.
- Additional extensions (Revocation Support Extension) and attributes (STC attribute) for Revocation and Radius Disconnect will be relayed to the peer HA.

As part of this support, two new messages —“Bind Delete Request” and “Bind Delete Ack”—are introduced that are exchanged between the redundant HAs when a binding is deleted. The following call flow illustrates when a binding gets deleted on the active Home Agent due to receipt of Revocation message, and the deletion of binding is synched to the standby Home Agent.

1. MS originates a call, PPP session is up and Mobile IP flow is setup on the active Home Agent with Registration revocation capability enabled and negotiated and the same is synched to the standby Home Agent.
2. On the PDSN, when a user issues administrative clear command, a Revocation message is sent out to the active Home Agent and deletes the visitor entry and associated resources are cleared.
3. The active HA, upon receiving the MIP Revocation message identifies the binding to be deleted. On identifying the binding, a Bind Delete Request message is sent out to the standby HA.
4. After a Bind Delete Request is sent out, the active HA cleans-up its resources associated with the binding for which Revocation message has arrived, and sends back a MIP Revocation Ack message to the PDSN.
5. The standby HA, on receipt of Bind Delete Request message, identifies the binding to be deleted, and sends back a Bind Delete Ack message with code as “accept”.
6. If a Bind Delete Ack message is not received within a configured time on the active HA, then a Bind Delete Request message is retransmitted. This process is repeated for the max retransmit count.

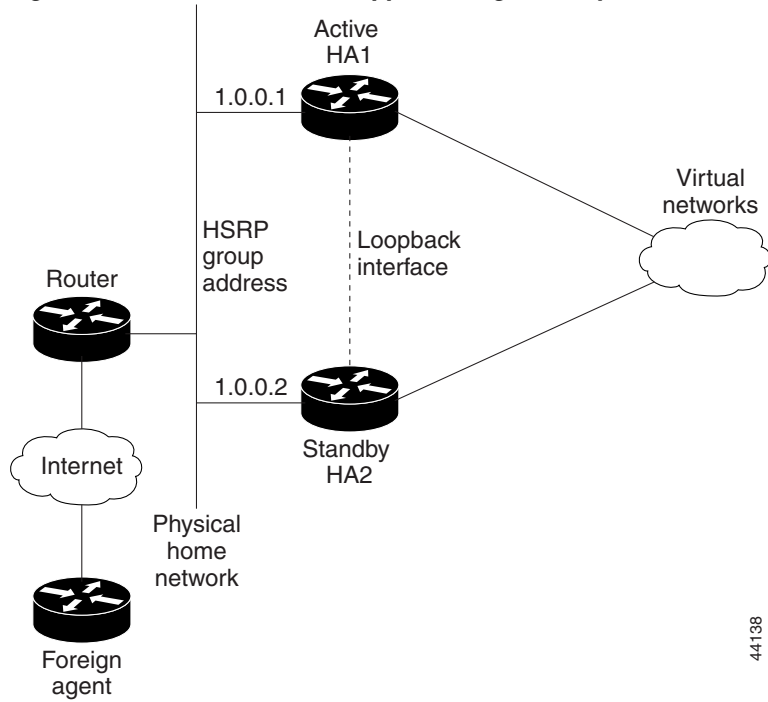
During binding synch, the extensions (Revocation Support Extension) and attributes for Revocation and Radius Disconnect (STC attribute) are synched from active HA to the standby. In scenarios when the active HA goes down and the standby becomes active, the now active HA is capable of deleting bindings on receipt of a RADIUS Disconnect message. For revocation, the bindings on the now active HA are revocable, and the HA is capable of receiving and sending revocation messages.

## Physical Network Support

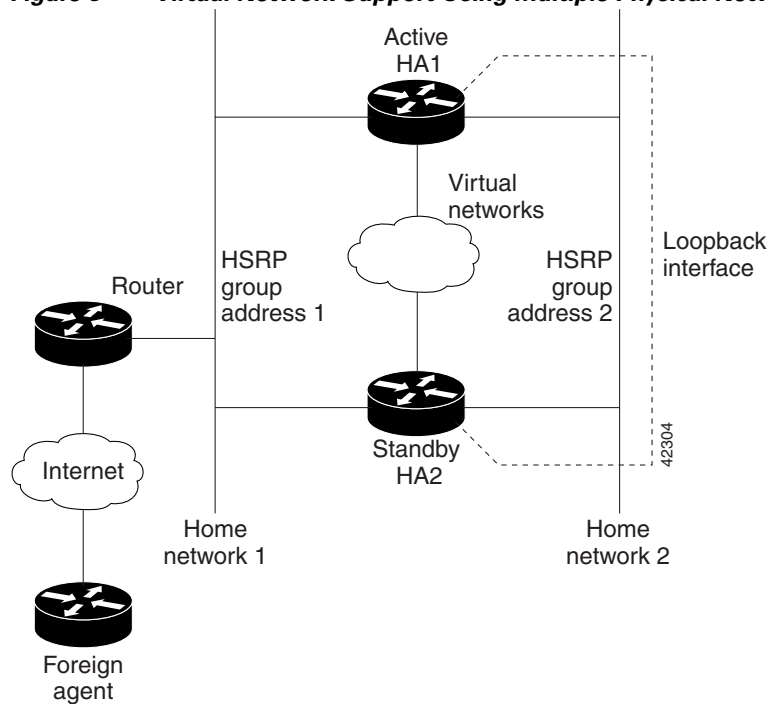
For MNs on physical networks, the HAs are configured in the active HA-standby HA configurations as shown in [Figure 7](#) and [Figure 8](#). The MNs that are supported on this physical network are configured with the HSRP virtual group address as the HA address. Hence, only the active HA can accept RRQs from the MN because 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 in which there are four HAs in the redundancy group (that is, 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 7 Virtual Network Support Using One Physical Network (Peer HA-Peer HA)**



**Figure 8 Virtual Network Support Using Multiple Physical Networks (Peer HA-Peer HA)**



## Virtual Networks

Mobile IP calls for each MN are associated with the home network from which the MN's home IP address is allocated. It is often assumed that this should be a physical network, but there are many cases in deployment where it does not make sense to have each MN attached to a physical network. IOS Mobile IP supports the creation of a software interface called a virtual network. A virtual network is very similar to a loopback interface, but it is owned by the Mobile IP process. Using virtual networks saves Interface Descriptor Blocks (IDBs), and allows Mobile IP specific control over how packets are dropped. When using virtual networks the mobile node is always considered roaming, it can never be attached to its home network. In real world deployments, this can cause some semantic problems. For example in cellular deployment a user may be in their home calling area, but will be roaming from a Mobile IP perspective.

Virtual networks are configured and referenced by a network number and mask pair. It is also possible to associate the virtual network with a Home Agent address for redundancy purposes. Here is an example:

```
ip mobile virtual-network 10.0.0.0 255.255.2550.0 address 192.168.100.1
ip mobile host 10.0.0.1 10.0.0.254 virtual-network 10.0.0.0 255.255.255.0
```

Virtual network routes are owned by the Mobile IP routing process and therefore must be redistributed into other routing protocols in order to be propagated. Here is an example:

```
router rip
 redistribute mobile
```

## Support for Discontinuous IP Address Pools for the Same Realm

This feature allows the user to specify discontinuous IP address pools for the same realm so that mobiles with NAI can have home addresses assigned from a pool of discontinuous IP address ranges. This will allow the Home Agent to accept Mobiles belonging to multiple virtual networks for the same host group.

This is achieved by configuring a local pool on HA covering the IP address ranges for multiple virtual-networks, and specifying one of the virtual-networks as the home network for the given realm.

The following configuration can be used to allow the HA to accept MNs belonging to multiple virtual networks for the same host group.

```
ip local pool pool1 1.1.1.1 1.1.1.250
ip local pool pool1 1.1.2.1 1.1.2.250

ip mobile home-agent
ip mobile virtual-network 1.1.1.0 255.255.255.0
ip mobile virtual-network 1.1.2.0 255.255.255.0
ip mobile host nai @xyz.com address pool local pool1 virtual-network 1.1.1.0 255.255.255.0
aaa lifetime 65535
```

In the above configuration, two virtual networks are configured and the local pool (pool1) is configured to include the IP addresses for both the virtual networks. By specifying one of the virtual networks and the local pool name in the **ip mobile host** command, the HA will accept MNs belonging to both the networks for the same realm.

## Home Address Assignment

The Home Agent assigns a home address to the mobile node 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 does 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 preconfigured 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 or 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.

### Static Home Addressing Without NAI

The original Mobile IP specification supported only static addressing of mobile nodes. The home IP address served as the “user name” portion of the authentication. Static addressing can be beneficial because it allows each device to keep the same address all the time no matter where it is attached to the network. This allows the user to run mobile terminated services without updating the DNS, or some other form of address resolution. It is also easy to manage MNs with static addressing because the home address and the Home Agent are always the same. However, provisioning and maintenance are much more difficult with static addressing because address allocation must be handled manually, and both the Home Agent and MN must be updated. Here is an example configuration:

```
router (config)# ip mobile host 10.0.0.5 interface FastEthernet0/0
router (config)# ip mobile host 10.0.0.10 10.0.0.15 interface FastEthernet0/0
router (config)# ip mobile secure host 10.0.0.12 spi 100 key ascii secret
```

### Static Home Addressing with NAI

Static home addressing can also be used in conjunction with NAI to support a NAI based authorization and other services. It is also possible to allow a single user to use multiple static IP addresses either on the same device, or multiple devices, while maintaining only one AAA record and security association. A user must be authorized to use an address before the registration will be accepted. Addresses can be authorized either locally, or through a AAA server. If a MN requests an address which is already associated with a binding that has a different NAI, the HA will attempt to return another address from the pool unless the command is set.

Here is a sample configuration:

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

## Local Authorization

A static address can be authorized on a per MN or per realm basis using configuration commands. Per MN configurations require that you define a specific NAI in the *user* or *user@realm* form. Per realm configurations require that you define a generic NAI in the *@realm* form, and allow only the specification of a local pool.

Here is a sample configuration:

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com static-address 10.0.0.1 10.0.0.2
interface FastEthernet0/0
router (config)# ip mobile host nai user@staticuser.com static-address local-pool
static-pool interface FastEthernet0/0
router (config)# ip mobile host nai @static.com static-address local-pool static-pool
interface FastEthernet0/0
```

## AAA Authorization

It is also possible to store either the authorized addresses, or local pool name in a AAA server. Each user must have either the **static-ip-addresses** attribute or the **static-ip-pool** attribute configured in the AAA server. Unlike the static address configuration on the command line, the **static-ip-addresses** attribute is not limited in the number of addresses that can be returned.

Here is a sample configuration.

HA configuration:

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

Radius Attributes:

Cisco-AVPair = "mobileip:static-ip-addresses=10.0.0.1 10.0.0.2 10.0.0.3"

Cisco-AVPair = "mobileip:static-ip-pool=static-pool"

## Dynamic IP Address

It is not necessary for a home IP address to be configured in the mobile station 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 MN 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.

## Fixed Addressing

It is possible to configure the Home Agent with a fixed address for each NAI. The fixed address is assigned to the MN each time it registers. This provides users all the benefits of static addressing while simplifying the configuration of the MN. We do not recommend fixed addressing for large-scale deployment because the Home Agent configuration must be updated to perform user all maintenance.

Here is a sample configuration:

```
router# ip mobile host nai user@realm.com address 10.0.0.1 interface FastEthernet0/0
```

## Local Pool Assignment

Local pool assignment requires that one or more address pools be configured on the HA. The HA allocates addresses from the pool on a first come, first served basis. The MN will keep the address as long as it has an active binding in the HA. The MN may update its binding by sending a RRQ with either the allocated address, or 0.0.0.0 as its home address. When the binding expires the address is immediately returned to the pool.



### Note

Currently local pool allocation cannot be used with the peer-to-peer HA Redundancy model. The number of local pools which, can be configured is limited only by the available memory on the router.

Here is a sample configuration:

```
router (config)# ip local pool mipool 10.0.0.5 10.0.0.250
router (config)# ip mobile host nai @localpool.com address pool local mipool
virtual-network 10.0.0.0 255.255.255.0
```

## DHCP Allocation

The Dynamic Host Configuration Protocol (DHCP) is already a widely used method of allocating IP addresses for desktop computers. IOS Mobile IP leverages the existing DHCP proxy client in IOS to allow the home address to be allocated by a DHCP server. The NAI is sent in the Client-ID option and can be used to provide dynamic DNS services.

Here is a sample configuration:

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



### Note

Currently DHCP cannot be used with the peer-to-peer HA Redundancy model.

## Dynamic Addressing from AAA

Dynamic addressing from AAA allows the operator to support fixed and/or per session addressing for MNs without the trouble of maintaining addressing at the MN or HA. The AAA server can return either a specific address, a local pool name, or a DHCP server address. If the AAA server is being used to return a specific address the home address can either be configured as an attribute on the NAI entry in the RADIUS database, or can be allocated from a pool depending on the capabilities of the AAA server being used. The AAA server can also return the name of a local pool configured on the HA or a DHCP server IP address.

Here is a sample configuration.

On the HA:

```
router (config)# ip local pool dynamic-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

AAA Address assignment:

Cisco-AVPair = "mobileip:ip-address=65.0.0.71"

AAA Local Pool attribute:

Cisco-AVPair = "mobileip:ip-pool=dynamic-pool"

AAA DHCP server attribute:  
Cisco-AVPair = "mobileip:dhcp-server=10.1.5.10"

## On-Demand Address Pool (ODAP)

If you use MWAM cards to provide a higher density of HAs, you may choose to have IP addresses allocated from a central source. Cisco's IOS On-Demand Address Pools (ODAPs) provides this functionality. ODAP simplifies HA configuration, in that you will not have to configure a local pool of IP addresses in each HA configuration.

You can use ODAP to centralize the management of large pools of addresses and simplify the configuration of large networks. The ODAP feature consists of two components:

- DHCP ODAP subnet allocation server
- ODAP manager (residing on each HA)

A DHCP ODAP subnet allocation server is configured to create and allocate pools of IP address space on a per-subnet basis. The size of these pools is configurable, and these subnets will be leased to the ODAP managers on the HA, and they provide subnet allocation pools for the ODAP manager allocation. The DHCP ODAP subnet allocation server functionality can reside on one of the HA instances on the MWAM. The DHCP ODAP subnet allocation server functionality can also reside on another external Cisco IOS router, or an external Cisco Access Register.

The ODAP manager functionality resides on each HA image. Rather than using local IP pools, the HA uses the ODAP manager functionality. The ODAP manager leases subnets from the ODAP subnet allocation server based on the demand for IP addresses and subnet availability to each HA. The ODAP manager on the HA assigns addresses to clients from these subnets, and dynamically increases or decreases the subnet pool size depending on address utilization. When an HA ODAP manager leases a subnet, a summarized route is automatically added for each subnet that the HA receives. This route is added to the Null interface and is a static route.

When the ODAP manager on the HA allocates a subnet, the ODAP subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager needs the address space. The binding is destroyed and the subnet returned to the subnet pool only when the HA ODAP manager releases the subnet as the address space utilization decreases.

The DHCP ODAP subnet allocation server has enhanced DHCP functionality. Instead of returning a single IP address, it returns a subnet of addresses. The ODAP manager manages this pool of IP addresses on the HA. This functionality provides a more efficient route summarization for the routing protocols.

### ODAP Restrictions

The following list identifies restrictions for the ODAP feature:

- ODAP with peer-to-peer redundancy is not supported.
- The minimum subnet lease time on the ODAP server must be 10 minutes.
- Pre-emption with rf-interdev support is not working.

### 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 includes 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 7600 and 6500 platforms, the MWAM utilizes the Cisco IPSec Acceleration Card.

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.

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

The HA supports IPSec, IKE, Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B.

IS835-B specifies three mechanisms for providing IPSec security:

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

**Note**

IS835B Static IPSec feature is available only on the Cisco 7200 Internet router platform. The Cisco IOS IPSec feature is available on the Cisco 7200 Internet router, Cisco 6500 Catalyst switch, and Cisco 7600 switch platforms. The HA 2.0 (and above) Release only supports statically configured, pre-shared secret for IPSec IKE.

As per IS-835-B, The HA and AAA should be configured with same security level for a PDSN. The PDSN receives a security level from AAA server and initiates IKE, and the HA responds to IKE request for establishing security policy.

The PDSN receives a security level from the AAA server and initiates IKE, and the HA responds to IKE request for establishing a security policy. All traffic specified by the access-list of the crypto configuration will be protected by IPSec tunnel. The access-list will be configured to protect all traffic between the PDSN and HA, and all bindings belonging to a given PDSN-HA pair will be protected.

IPSec is not applicable to mobiles using Co-located COA

**Note**

The Cisco Home Agent Release 2.0 (and above) on the Cisco 7600 and 6500 platforms requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500 or 7600 router. 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/index.html>.

For more information on the Cisco 7600 Internet Router visit <http://www.cisco.com/en/US/products/hw/routers/ps368/index.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.

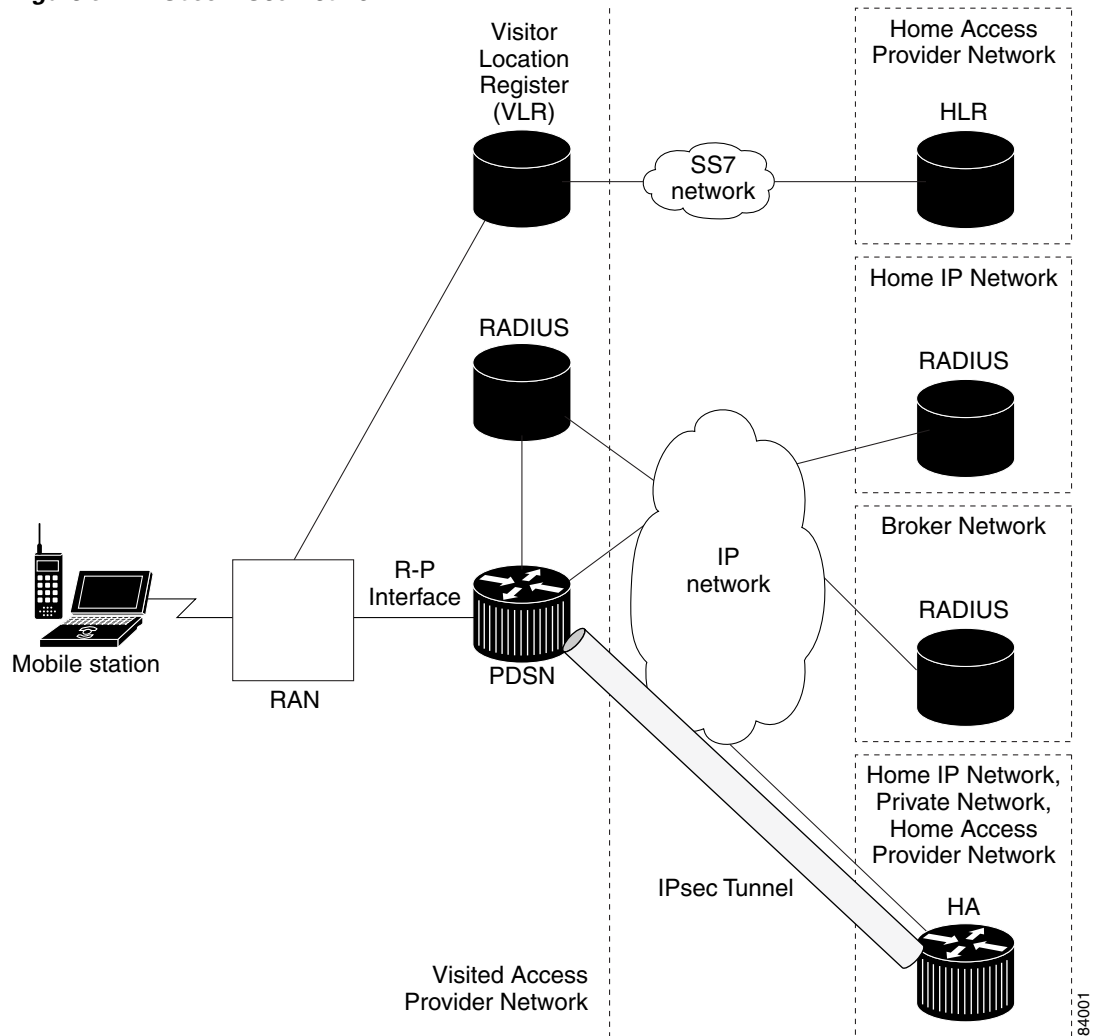
Once Security Associations (SAs or tunnels) are established, they remain active until there is traffic on the tunnel, or the lifetime of the SAs expire.

**Note**

IPSec does not work with HA redundancy, since the IPSec security associations are not replicated to the standby during failover.

Figure 9 illustrates the IS835 IPsec network topology.

Figure 9 IS835 IPsec Network



## IPsec Interoperability Between the PDSN and HA (IS-835-C)

IPsec rules under IS-835C mandates that connections are always initiated from the PDSN to the Home Agent IP address. Certain PDSNs may not be flexible in their approach to IPsec configuration. These PDSNs do not allow any configuration for Remote IPsec termination points, and hence expect that the remote IPsec termination point is always the Home Agent IP address.

The following section illustrates how to handle IPsec Interoperability between such PDSNs and the HA with Home Agent Release 2.0 and above.

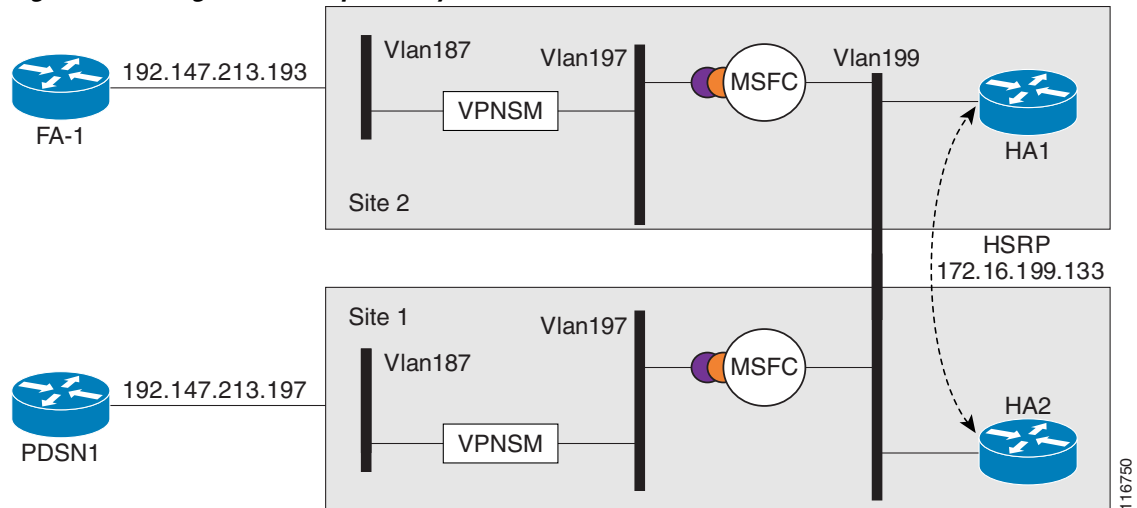
The change in the configuration allows for IPsec connections for the Home Agent IP address but still terminated by the VPNSM.

### Handling Single Home Agent Instance

This solution is achieved by letting SUP IOS own the same Home Agent IP address. Traffic to the Home Agent is then policy routed to the correct Home Agent.

Figure 10 illustrates a possible configuration:

**Figure 10 Single HA Interoperability**



Here is a sample configuration for the Supervisor. The PDSN IP Address is 14.0.0.1, HA3 address is 13.0.0.50, and HA4 is 13.0.0.51

### Single HA Instance - Interoperability

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
  lifetime 60000
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set mobile-set1 esp-3des

# Comment: testmap is used for HA3

crypto map testmap local-address Loopback21
crypto map testmap 20 ipsec-isakmp
  set peer 14.0.0.1
  set transform-set mobile-set1
  match address 131
!

interface Loopback21
  description corresponds to ha-on-proc3
  ip address 13.0.0.50 255.255.255.255
!

interface GigabitEthernet4/1
  description encrypt traffic from vlan 151 to vlan 201& 136 to 139
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
```

```

switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,136,146,151,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
description decrypts traffic from vlan 201 to 151, 139 to 136
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,139,149,201,1002-1005
switchport mode trunk
cdp enable

interface Vlan136
description secure vlan
ip address 15.0.0.1 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA3
no mop enabled
crypto map testmap
!
interface Vlan137
description internal vlan to HA3
ip address 7.0.0.1 255.255.0.0
!
interface Vlan139
no ip address
crypto connect vlan 136
!

access-list 131 permit ip host 14.0.0.1 host 13.0.0.50
access-list 131 permit ip host 13.0.0.50 host 14.0.0.1
access-list 131 permit ip 14.0.0.0 0.0.0.255 13.0.0.0 0.0.0.255

access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any

route-map RRQ-HA3 permit 10
match ip address 2000
set ip next-hop 7.0.0.2
!

```

## Support for ACLs on Tunnel Interface

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

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

### 1. Configure a tunnel template

```

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

```

## 2. Configure the ACL

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

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

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

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

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

MN-HA-SPI (26/57)

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

The following procedure illustrates this support:

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

## User Profiles

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

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

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

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

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

## Mobility Binding Association

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

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

The binding association contains the following information:

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

## 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. The password for PAP users can be set using the **ip mobile home-agent aaa user-password** command.

---

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 using the new PDSN/FA. If PPP idle-timeout is configured on the PDSN virtual-template, the maximum mobile IP lifetime advertised to the mobile will be 1 second less than the idle-timeout.

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

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



### Note

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



### Note

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

## 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 Mobile Wireless Home Agent Release 2.0 and above software, refer to the following documents:

- *Cisco Packet Data Serving Node (PDSN) Release 1.2 Feature Module for IOS Release 12.3(4)T.*
- *Release Notes for the Cisco PDSN Feature for Cisco IOS Release 12.3(4)T.*
- *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/index.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/en/US/products/hw/routers/ps341/index.html>).

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 and 7600 Router Support

The Cisco Home Agent is also supported on Cisco's Multi-processor WAN Application Module (MWAM) on the 6500 Catalyst Switch, and on the 7600 Internet Router. Each Catalyst 6500 or 7600 can support up to 6 MWAM modules. Each MWAM has 3 gigabit ethernet interfaces internally connected to the Cat6500 or 7600 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 or 7600 chassis with a SUP2, and 512 MB of DRAM.

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



#### 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>.

For a complete list of interfaces supported on 7600 platform, please refer to the on-line product information at Cisco.com home page. For hardware details on 7600 platform, please refer to the Cisco Series 7600 product specifications at <http://www.cisco.com/en/US/products/hw/routers/ps368/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](mailto: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://tools.cisco.com/RPF/register/register.do>.

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 SMIPv2, 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 SMIPv2*, 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 three images, one for the Cisco 7200 Series Router, one for the 7300 Series router, and one for the Cisco Catalyst 6500 switch and Cisco 7600 Series router platforms. This section describes the steps for configuring the Cisco Home Agent. Each image is described by platform number.

- c7200-h1is-mz HA image
- c7301-is-mz HA image
- svcmwam-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 pcli# 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 pcli#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 succeeded>
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
```

---

## Upgrading HA Image From XW-based Image to YF-based Image

If you are upgrading the Home Agent from a XW-based image to a YF-based image, you first need to upgrade the SUP image from a SXB-based image to a SXD-based image (for example, c6k222-pk9sv-mz.122-18.SXD2.bin). After you upgrade the SUP image, you can then upgrade the HA image.

### Upgrading the Supervisor Image

To upgrade the Supervisor image, perform the following procedure:

- Step 1** Copy the SUP image to the disks (disk0: / slavedisk0:).
- Step 2** Add the following command to the running config **boot system disk0: *SUP image name***". Here is an example:

```
boot system disk0:c6k222-pk9sv-mz.122-18.SXD2.bin
```



**Note** This step may require you to unconfigure previously configured instances of this CLI in order to enable the image to properly reload.

- Step 3** Perform a “write memory” so that running configuration is saved on both active and standby SUP.
- Step 4** Issue **reload** command on the active SUP.
- Step 5** Both active and standby SUP will reload simultaneously and come up with the the SXD-based image.



**Note** Issuing the **reload** command on the active SUP will cause both the active and standby Supervisors to reload simultaneously, thus causing some downtime during the upgrade process.

### Upgrading the HA Image on MWAM

To upgrade to the YF-based image on the MWAM, perform the following procedure:

- Step 1** Bring down the active HA by issuing the **hw-module module slot # reset cf:1** command. The standby HA will take over as the active HA. 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, copy the YF image to p1c# slot file system by issuing the following command:

**copy tftp: tftp file location p1c# 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 p1c#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 succeeded>
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 cf:4
```

**Step 4** Verify that all the bindings opened with the active HA have synced with the processor with new image.

**Step 5** Bring down the active HA with the XW-based image. The newly loaded YF-based HA will now become active.

**Step 6** Perform steps 1 through 3 as described above.



**Note** The downgrade process is similar to the upgrade process, where the SUP image should be downgraded first followed by the HA image.



**Note** For SXD-based SUP images, if config-on-SUP mode is used on MWAM, the startup configuration is written on both the SUP and local filesystem. This will assist you in upgrading/downgrading the images without losing the HA configuration between XW and YF images.



**Note** The downgraded image always starts with **config-local** due to incompatibility, and so it must be explicitly configured again using **config-on-sup** upon every downgrade. Additionally, any further upgrades will start with the mode used by the same version the image used earlier, otherwise only follow the mode used by the old version.

## Changing Configuration on Home Agent in a Live Network

If you need to change the working configuration on a Home Agent in a live network environment, perform the following procedure:

**Step 1** Bring the standby HA out of service. An example would be to shut down the HSRP interface towards active HA.

**Step 2** Make the necessary configuration changes on the standby HA, and save the configuration.

**Step 3** Issue the **reload** command to bring the standby HA back into service.

**Step 4** Bring the active HA out of service by shutting down HSRP interface. This will cause the standby to takeover as the active HA.

**Step 5** Make the necessary configuration changes on the active HA, and save the configuration.

**Step 6** Issue the **reload** command to bring the active HA back into service.



**Note** Some outage might occur concerning existing calls on the active HA being cleared forcibly.



**Note** Configurations on the active and standby should be the same for HA redundancy to work properly.

## 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, or 7600 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, page 49](#)

### 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, page 49](#)
- [Configuring RADIUS in the Home Agent Environment, page 50](#)

### 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, page 50](#)

**Home Agent Redundancy Tasks (Required for Mobile IP)**

- [Configuring HA Redundancy, page 50](#)
- [Enabling Mobile IP, page 51](#)
- [Enabling HSRP, page 51](#)
- [Configuring HSRP Group Attributes, page 51](#)
- [Enabling HA Redundancy for a Physical Network, page 51](#)
- [Enabling HA Redundancy for a Virtual Network Using One Physical Network, page 52](#)
- [Configuring HA Load Balancing, page 53](#)
- [Configuring Server Load Balancing, page 53](#)

**Network Management Configuration Tasks**

- [Configuring HA Accounting, page 53](#)
- [Configuring Network Management, page 54](#)

**Cisco Home Agent Configuration Tasks**

- [Configuring the Cisco Home Agent, page 54](#)

**IP Sec Configuration Tasks**

- [Configuring IPSec for the HA, page 55](#)
- [Configuring Hot-Lining, page 55](#)

**Other Configuration Tasks**

- [Configuring VRF for the HA, page 56](#)
- [Configuring MIPv4 Registration Revocation, page 57](#)
- [Configuring RADIUS Disconnect Client, page 57](#)
- [Configuring the NAS-ID, page 57](#)
- [Configuring ODAP-based Address Allocation, page 58](#)
- [Configuring ACLs on the Tunnel Interface, page 58](#)
- [Creating Active Standby Home Agent Security Associations, page 58](#)

**Maintaining the HA**

- [Monitoring and Maintaining the HA, page 59](#)

## Basic IOS Configuration on MWAM

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

Command	Purpose
router# <b>vlan database</b>	Enter VLAN configuration mode.
router(vlan)# <b>vlan</b> <i>vlan-id</i>	Add an Ethernet VLAN.
router(vlan)# <b>exit</b>	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.
router(config)# <b>mwam module</b> 7 <b>port</b> 3 <b>allowed-vlan</b> <i>vlan_range</i>	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM.
router# <b>session slot</b> <i>MWAM module</i> <b>processor</b> <i>processor number</i>	Configures the ethernet connectivity from the backplane to the individual processors on the MWAM. <i>Processor number</i> is from 2 to 6.
Router(config)# <b>int gigabitEthernet</b> 0/0	Specifies the type of interface being configured, and the slot number.
Router(config-if)# <b>no shut</b>	Puts the specified GE interfaces in service.
Router(config-if)# <b>int gigabitEthernet</b> 0/0.401	
Router(config-subif)# <b>encapsulation</b> dot1Q 401	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in virtual LANs.
Router(config-subif)# <b>ip address</b> 1.1.1.1 255.255.255.0	
Router(config-subif)# <b>exit</b>	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)# <b>aaa authentication ppp default group radius</b>	Enables authentication of PPP users using RADIUS.
Router(config)# <b>aaa authorization network default group radius</b>	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)# <b>radius-server host ip-addr key sharedsecret</b>	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)# <b>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]</b>	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)# <b>router mobile</b>	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)# <b>standby</b> [group-number] <b>ip</b> 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:

<pre>Router(config-if)#<b>standby</b> [group-number] <b>priority</b>   priority [<b>preempt</b> [<b>delay</b> [minimum   sync]   delay]] or Router(config-if)#<b>standby</b> [group-number] [<b>priority</b>   priority] <b>preempt</b> [<b>delay</b> [minimum   sync]   delay]</pre>	<p>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 <b>preempt delay min</b> 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.</p>
---	--

## 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)# <b>standby</b> [group-number] <b>ip</b> ip-address	Enables HSRP.
Router(config-if)# <b>standby name</b> hsrp-group-name	Sets the name of the standby group.

Command	Purpose
Router(config)# <b>ip mobile home-agent redundancy</b> <i>hsrcp-group-name</i>	Configures the Home Agent for redundancy using the HSRP group name.
Router(config)# <b>ip mobile secure home-agent</b> <i>address spi spi key hex string</i>	Sets up the Home Agent security association between peer routers. If configured on the active HA, the IP address <i>address</i> argument is that of the standby HA. If configured on the standby HA, the IP address <i>address</i> 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)# <b>standby</b> [ <i>group-number</i> ] <b>ip</b> <i>ip-address</i>	Enables HSRP.
Router(config)# <b>ip mobile home-agent address</b> <i>address</i>  or  Router(config)# <b>ip mobile home-agent</b>	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)# <b>ip mobile virtual-network</b> <i>net mask [address address]</i>	Defines the virtual network. If the mobile node and Home Agent are on the same subnet, use the [ <b>address address</b> ] option.
Router(config)# <b>ip mobile home-agent redundancy</b> <i>hsrcp-group-name [[virtual-network] address address]</i>	Configures the Home Agent for redundancy using the HSRP group to support virtual networks.
Router(config)# <b>ip mobile secure home-agent</b> <i>address spi spi key hex string</i>	Sets up the Home Agent security association between peer routers. If configured on the active HA, the IP address <i>address</i> argument is that of the standby HA. If configured on the standby HA, the IP address <i>address</i> 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 HA Load Balancing

To enable the HA Load Balancing feature, perform these tasks:

Command	Purpose
Router(config)# <b>ip mobile home-agent dynamic-address</b> <i>ip address</i>	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to <i>ip address</i> .
Router(config)# <b>ip mobile home-agent dfp-max-weight</b> <i>max-weight-value</i>	Sets the maximum weight that can be set in DFP packets to the HA-SLB. The default value of <i>max-weight-value</i> is 25.
Router(config)# <b>ip mobile home-agent max-binding</b> <i>max-binding-value</i>	Limits the number of bindings that can be opened on the HA. The default value of <i>max-binding-value</i> is 235,000.

## Configuring Server Load Balancing

To enable the Mobile IP SLB feature on the HA, perform the following task:

Command	Purpose
Router(config)# <b>virtual</b> <i>ip address</i> <b>udp 434 service ipmobile</b>	Enables the Mobile IP SLB feature. The <i>ip address</i> is the virtual Home Agent address to which registration requests from PDSN/FA will be sent.

## Configuring HA Accounting

Mobile IP currently uses AAA commands to configure authorization parameters. All of the following commands are required. By default, the HA Accounting feature will be disabled; the HA will NOT send accounting messages to the AAA server unless configured. To enable the HA Accounting feature, perform the following tasks:

Command	Purpose
Router(config)# <b>ip mobile home-agent accounting</b> <i>list</i>	Enables HA accounting, and applies the previously defined accounting method list for Home Agent. <i>list</i> is the AAA Accounting method used to generate HA accounting records.
Router(config)# <b>aaa accounting network</b> <i>method list name</i> <b>start-stop group</b> <i>group name</i>	Sends a “start” accounting notice at the beginning of a process, and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
Router(config)# <b>aaa accounting update newinfo</b>	Enables an interim accounting record to be sent to the accounting server whenever there is new accounting information to report relating to the user in question.
Router# <b>debug aaa accounting</b>	Enables debugging of HA Accounting messages.

Command	Purpose
Router# <b>debug radius</b> Router# <b>debug tacacs</b>	Enables debugging of security protocol specific messages.
Router# <b>debug ip mobile</b>	Enable Mobile IP related debug messages. Accounting will print debug messages only in case of errors.

## Configuring Network Management

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

Command	Purpose
Router(config)# <b>snmp-server community</b> <i>string</i> [ <b>ro</b>   <b>rw</b> ]	Specifies the community access string to permit access to the SNMP protocol.
Router(config)# <b>snmp-server host</b> <i>host-addr</i> <b>traps version</b> { <b>1</b>   <b>2</b>   <b>3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}	Specifies the recipient of an SNMP notification operation.
Router(config)# <b>no virtual-template snmp</b>	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)# <b>snmp-server enable traps ipmobile</b>	(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)# <b>ip mobile host</b> { <i>lower</i> [ <i>upper</i> ]   <b>nai string</b> [ <b>static-address</b> <i>addr1</i> [ <i>addr2</i> ] [ <i>addr3</i> ] [ <i>addr4</i> ] [ <i>addr5</i> ]   <b>local-pool name</b> { <b>address</b> <i>addr</i>   <b>pool</b> { <b>local name</b>   <b>dhcp-proxy-client</b> [ <b>dhcp-server</b> <i>addr</i> ]}}}{ <b>interface name</b>   <b>virtual-network</b> <i>net mask</i> } [ <b>aaa</b> [ <b>load-sa</b> ] [ <b>care-of-access acl</b> ] [ <b>lifetime number</b> ]	Specifies either static IP addresses or a pool of IP addresses for use by multiple flows with the same NAI.
Router(config)# <b>ip mobile home-agent</b> [ <b>broadcast</b> ] [ <b>care-of-access acl</b> ] [ <b>lifetime number</b> ] [ <b>replay seconds</b> ] [ <b>reverse-tunnel-off</b> ] [ <b>roam-access acl</b> ] [ <b>strip-nai-realm</b> ] [ <b>suppress-unreachable</b> ] [ <b>local-timezone</b> ]	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
<pre>Router(config)# <b>crypto map</b> map-name seq-num <b>ipsec-isakmp</b>  <b>set peer</b> ip address of ha <b>set transform-set</b> transform-set-name <b>match address</b> acl name</pre>	<p>Creates a a crypto map entry for one HA in one Crypto-map set.</p> <p>The Crypto Map definition is not complete until:</p> <ol style="list-style-type: none"> <li>1. ACL associated with it is defined, and</li> <li>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.</li> </ol>
<pre>Router# <b>access-list</b> acl-name <b>deny udp host</b> HA IP addr <b>eq</b> <b>mobile-ip host</b> PDSN IP addr <b>eq mobile-ip</b>  <b>access-list</b> acl-name <b>permit ip host</b> PDSN IP addr <b>host</b> HA IP addr  <b>access-list</b> acl-name <b>deny ip any any</b></pre>	<p>Defines the access list.</p> <p>The ACL name “acl-name” is same as in the crypto-map configuration</p>
<pre>Router# <b>Interface</b> Physical-Interface of PI interface  <b>crypto map</b> Crypto-Map set</pre>	<p>Applies the Crypto-Map on Pi Interface, as the HA sends/receives Mobile IP traffic to/from PDSN on this interface</p>

## Configuring Hot-Lining

To configure Hot-lining, perform the following tasks in global configuration mode:

Command	Purpose
<pre>Router(config)# <b>ip mobile realm</b> realm <b>hotline redirect</b> redirect-server-ipaddress</pre>	<p>Enables inbound user sessions to be disconnected when specific session attributes are presented.</p>
<pre>Router(config)# <b>ip mobile cdma-ipsec fa-address</b> ip address <b>security-level</b> 1 2</pre>	<p>Sets the security level with the PDSN specified by the <i>ip address</i>.</p>

## Configuring VRF for the HA

To configure VRF on the HA, perform the following tasks:

Command	Purpose
<pre>Router(config)#ip mobile realm @xyz.com vrf vrf-name ha-addr ip-address [aaa-group [accounting aaa-acct-group   authentication aaa-auth-group]]</pre>	<p>Defines the VRF for the domain @xyz.com.</p> <p>The IP address of the Home Agent that corresponds to the VRF is also defined at the point that the MOIP tunnel will terminate.</p> <p>The IP address of the Home Agent should be a routable IP address on the box.</p> <p>Optionally, the AAA accounting and/or authentication server groups can be defined per VRF.</p> <p>If AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group.</p> <p>If AAA authentication server group is defined, HA-CHAP (MN-AAA authentication) is sent to the server(s) defined in the group.</p>
<pre>Router(config)# ip vrf vrf-name  description VRF for domain1  rd 10:1</pre>	<p>Defines the VRF on the box.</p> <p>Description of the VRF.</p> <p>Router descriptor for VRF. Creates a VRF table by specifying a route distinguisher.</p> <p><b>Note</b> One VRF per domain should be configured on each HA CPU.</p>
<pre>router# interface Loopback1 ip address 192.168.11.1 255.255.255.0 secondary ip address 192.168.10.1 255.255.255.0</pre>	<p>Defines the loopback interface under which the IP addresses for each VRF are configured. These addresses are used as the Mobile IP tunnel source IP addresses for the realm.</p> <p>The mask that is configured for the IP address will be used in the VRF routing table. Host mask (255.255.255.255) or broadcast mask (0.0.0.0) should not be configured.</p>

## Configuring MIPv4 Registration Revocation

To enable MIPv4 Registration Revocation feature on HA, perform the following tasks in global configuration mode:

Command	Purpose
Router(config)# <b>ip mobile home-agent revocation</b>	Enables support for MIPv4 Registration Revocation on the HA.
Router(config)# <b>ip mobile home-agent revocation timeout 5</b> <b>retransmit 6</b>	(Optional) Sets the retransmit count and timeout value for revocation messages.

## Configuring RADIUS Disconnect Client

Perform the following tasks to configure RADIUS disconnect for clients and the associated keys:

Command	Purpose
Router(config)# <b>aaa pod server</b> [ <b>clients</b> <i>ipaddr1</i> [ <i>ipaddr2</i> [ <i>ipaddr3</i> [ <i>ipaddr4</i> ]]] [ <b>port</b> <i>port number</i> ] [ <b>auth-type</b> { <b>any</b>   <b>all</b>   <b>session-key</b> }] [ <b>ignore session-key</b> ] { <b>ignore server-key</b>   <b>server-key</b> <i>string</i> }	Required to enable Packet of Disconnect (POD) services at AAA subsystem level in Cisco IOS. Enables inbound user sessions to be disconnected when specific session attributes are presented.
Router(config)# <b>ip mobile radius disconnect</b>	Enables the functionality of processing RADIUS disconnect messages on HA
Router(config)# <b>radius-server attribute 32 include-in-access-req</b>	This command is required to include the optional NAS-Identifier attribute in Access-Request to Home AAA.

## Configuring the NAS-ID

Perform the following configuration on all PDSNs and HAs in a network to include the optional NAS-Identifier attribute in Access Request to Home AAA:

Command	Purpose
Router(config)# router# <b>radius-server attribute 32 include-in-access-req</b> <i>format format-string</i>	The format string has options to include the hostname, ip-address, and domain name of the PDSN, and should form a Fully Qualified Domain Name (FQDN). For example, the format string can be of type“%h%d” where “%h” includes the hostname and “%d” includes the domain name.

Here is an example of an FQDN NAS-ID: *Pdsnbangalore.abctel.com*.

## Configuring ODAP-based Address Allocation

To enable the HA to support ODAP pools, perform the following task:

Command	Purpose
Router(config)# <b>ip mobile host nai address pool dhcp-pool odap poolname</b>	Enables the HA to support ODAP address pools.

Here is an example:

```
Router (config)#ip mobile host nai @ispbar2.com address pool dhcp-pool ha-dhcp-pool
```

## Configuring ACLs on the Tunnel Interface

To configure ACLs to block certain traffic using the template tunnel feature, perform the following task:

Command	Purpose
Router(config)# <b>interface tunnel 10</b> <b>ip access-group 150 in</b> -----> apply access-list 150 <b>access-list 150 deny any</b> 10.10.0.0 0.255.255.255 access-list permit any any -----> permit all but traffic to 10.10.0.0 network	Configures a tunnel template. Configures the ACL.
<b>ip mobile home-agent template tunnel 10 address 10.0.0.1</b>	Configures a Home Agent to use the template tunnel.

## Creating Active Standby Home Agent Security Associations

The following IOS command is introduced in 12.3(8)XW3 to display active standby Home Agent security associations.

Command	Purpose
Router(config)# <b>show ip mobile secure ?</b>  <b>foreign-agent</b> <b>home-agent</b> <b>host</b> <b>summary</b>	Displays the active and standby Home Agent Security associations. Displays Foreign agent security associations. Displays Home agent security associations. Displays Mobile host security associations. Displays a summary of security associations.

Here is an example of the command:

```
HA#show ip mobile secure hom
HA#show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
    SPI 100, MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'red'
HA#
HA#
```

# Monitoring and Maintaining the HA

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

Command	Purpose
Router# <b>clear ip mobile binding</b>	Removes mobility bindings.
Router# <b>clear ip mobile host-counters</b>	Clears the mobility counters specific to each mobile station.
Router# <b>clear ip mobile secure</b>	Clears and retrieves remote security associations.
Router# <b>clear ip mobile traffic</b>	Clears IP mobile traffic counters.
Router# <b>debug ip mobile advertise</b>	Displays advertisement information.
Router# <b>debug aaa pod</b>	Displays debug information for Radius Disconnect message processing at AAA subsystem level
Router# <b>debug ip mobile</b>	Displays IP mobility activities.
Router# <b>debug ip mobile host</b>	Displays mobility event information.
Router# <b>debug ip mobile redundancy</b>	Displays display IP mobility events.
Router# <b>debug radius</b>	Displays information associated with RADIUS.
Router# <b>debug tacacs</b>	Displays information associated with TACACS.
Router# <b>show ip mobile binding</b>	Displays the mobility binding table.
Router# <b>show ip mobile binding vrf</b>	Displays all the bindings on the HA that are VRF-enabled.
Router# <b>show ip mobile binding vrf realm</b>	Displays all bindings for the realm that are VRF-enabled.
Router# <b>show ip mobile globals</b>	Displays global information for Mobile Agents.
Router# <b>show ip mobile host</b>	Displays mobile station counters and information.
Router# <b>show ip mobile proxy</b>	Displays information about a proxy Mobile IP host.
Router# <b>show ip mobile secure</b>	Displays mobility security associations for Mobile IP.
Router# <b>show ip mobile traffic</b>	Displays Home Agent protocol counters.
Router# <b>show ip mobile tunnel</b>	Displays information about the mobile IP tunnel.
Router# <b>show ip mobile violation</b>	Displays information about security violations.
Router# <b>show ip route vrf</b>	Displays the routing table information corresponding to a VRF.

# Configuration Examples

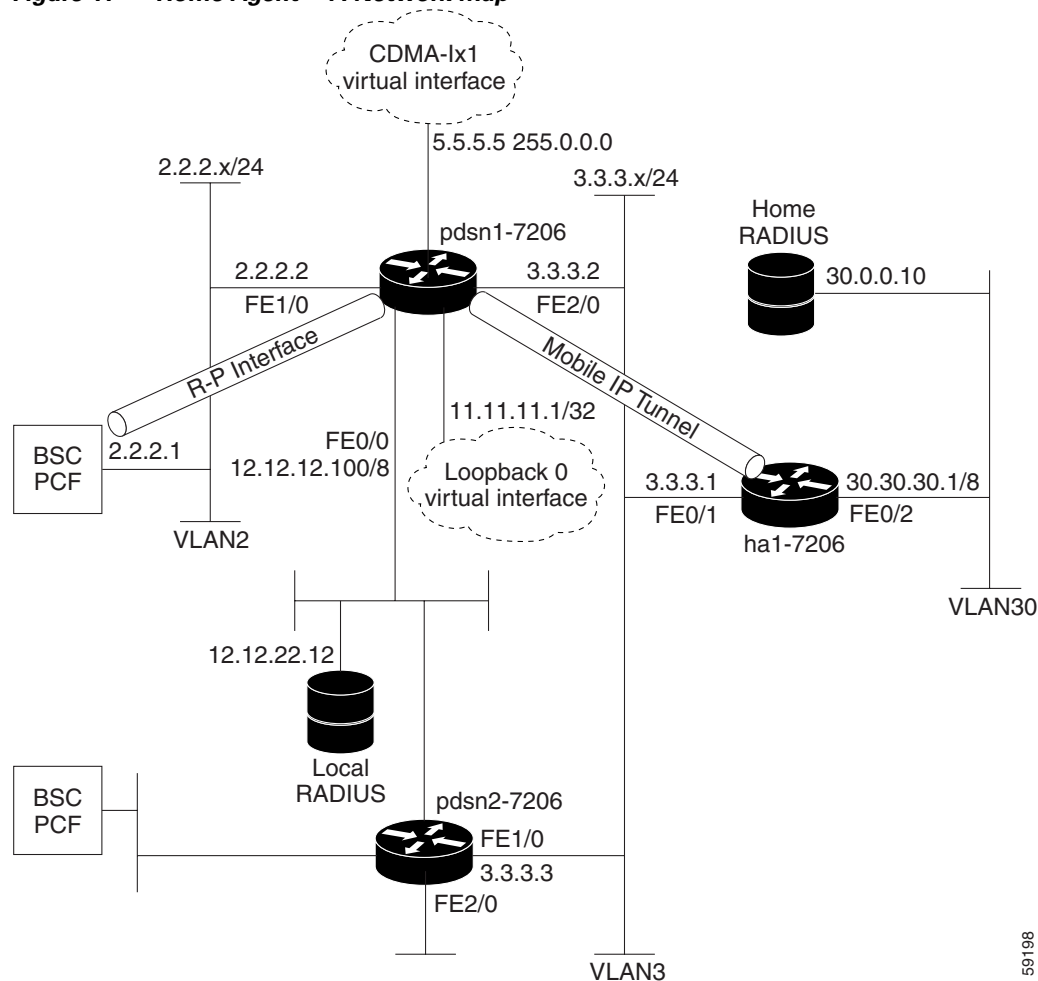
This section provides the following configuration examples:

- [Cisco Home Agent Configuration, page 61](#)
- [Home Agent Redundancy Configuration, page 64](#)
- [Home Agent IPSec Configuration, page 68](#)
- [HA Accounting Configuration, page 70](#)
- [HA-SLB Configurations, page 71](#)
- [ODAP Redundancy Configuration, page 94](#)
- [DHCP-Proxy-Client Configuration, page 97](#)
- [VRF Configuration, page 99](#)
- [VRF Configuration with HA redundancy, page 101](#)

## Cisco Home Agent Configuration

Figure 11 and the information that follows is an example of the placement of a Cisco HA and its configuration.

**Figure 11 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
!
```

59198

```

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 1 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 min 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 and the 7600 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

```

## HA Accounting Configuration

```

aaa new-model
!
!
aaa accounting network mylist start-stop group radius
aaa accounting update newinfo

```

The first block of commands are AAA configurations. An accounting method list (mylist) is created for network accounting. Start-Stop keywords imply that HA will send Start and Stop records. For detailed information, see the *IOS Security Configuration Guide*.

The Second line instructs the HA to send accounting Update records, whenever there is a change in Care-Of-Address (COA).

```

ip mobile home-agent accounting mylist address 3.3.3.1
ip mobile host 3.3.3.2 3.3.3.5 interface Ethernet2/2
ip mobile secure host 3.3.3.2 spi 1000 key ascii test algorithm md5 mode prefix-suffix
!

```

These are Mobile IP commands. On the first line, accounting method list mylist is applied on the Home Agent, thus enabling HA Accounting.

```

!
!
radius-server host 128.107.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3

```

```
radius-server key cisco
!
```

These are RADIUS commands. The first line specifies the RADIUS server address. Make sure the HA can reach AAA server and has proper access privileges.

## Verifying HA Accounting Setup

The HA Accounting status can be verified by issuing the **show ip mobile global** command. The current accounting status is displayed as shown below:

```
router# sh ip mobile global
IP Mobility global information:

Home Agent

    Registration lifetime: INFINITE
    Broadcast enabled
    Replay protection time: 10 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm disabled
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist  D Acct. Status
    Address 3.3.3.1

Foreign Agent is not enabled, no care-of address

1 interface providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled
Tunnel path MTU discovery aged out after 10 min
router#
```

## HA-SLB Configurations

The following examples illustrate various HA-SLB configurations.

### Dispatched MODE WITH STATIC WEIGHTS

#### Configuration on SLB:

The following commands configure a serverfarm “HAFARM”, and associate two real servers (HAs) with the serverfarm. The real servers are configured with a static weight of one.

```
ip slb serverfarm HAFARM
real 20.1.1.51
  weight 1
  inservice
!
real 20.1.1.52
  weight 1
  inservice
```

The following commands configure a virtual server with service as “ipmobile” on the SLB and associates the serverfarm HAFARM with the virtual server. The optional config command below 'idle ipmobile request *idle-time-val* configures the duration for which the session object exists

```
ip slb vserver MIPSLB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm HAFARM
  idle ipmobile request 300
inervice
```

#### Configuration on HA:

The following command configures the virtual server address as a loopback address on the HA. This configuration is required only for Dispatched mode.

```
interface Loopback1
ip address 15.1.1.10 255.255.255.0
```

The following command sets the source address and HA address field in the RRP to that of the real HA's address. This configuration is required only for Dispatched mode.

```
ip mobile home-agent dynamic-address 20.1.1.51
```

#### Show Output on SLB:

The following command displays the status of server farm HAFARM and, the associated real servers, and their status. It also shows the no. of connections assigned to each of the real servers.

The show output below was captured after opening 4 MIP sessions which HA-SLB has load balanced equally across two real HA's (2 connections to each HA).

```
SLB-6500#show ip slb reals
```

real	farm name	weight	state	conns
20.1.1.51	HAFARM	1	OPERATIONAL	2
20.1.1.52	HAFARM	1	OPERATIONAL	2

The following command displays all the sessions during runtime, or as long as the session objects exist.

```
SLB-6500#show ip slb sessions ipmobile
```

vserver	NAI hash	client	real	state
MIPSLB	A984DF0A00000000	15.1.1.51	20.1.1.52	IPMOBILE_ESTAB
MIPSLB	1DC0E31400000000	15.1.1.51	20.1.1.52	IPMOBILE_ESTAB
MIPSLB	2BDEE91100000000	15.1.1.51	20.1.1.51	IPMOBILE_ESTAB
MIPSLB	47E2FD1B00000000	15.1.1.51	20.1.1.51	IPMOBILE_ESTAB

```
SLB-6500#
```

**Show Output on HAs:**

The following command shows that two bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#
```

```
HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

**Dispatched mode with DFP****Configuration on SLB:**

The following commands configure a serverfarm "HAFARM" and associates two real servers (HAs) with the serverfarm.

```
ip slb serverfarm HAFARM
  real 20.1.1.51
    inservice
  !
  real 20.1.1.52
    inservice
  !
```

The following commands configure a virtual server with service as "ipmobile" on the SLB and associates the serverfam HAFARM with the virtual server. The optional config command below 'idle ipmobile request *idle-time-val* configures the duration for which the session object exists.

```
ip slb vserver MIPS LB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm HAFARM
  idle ipmobile request 300
  inservice
```

The following command configures the DFP Manager on HA-SLB and assigns two DFP agents (clients) to which HA-SLB can connect to.

```
ip slb dfp
  agent 20.1.1.51 500
  agent 20.1.1.52 500
  !
```

**Configuration on HA:**

The following command configures the virtual server address as a loopback address on the HA. This configuration is required only for Dispatched mode.

```
interface Loopback1
ip address 15.1.1.10 255.255.255.0
!
```

The following command configures the DFP agent on the real HA. The port num. configured here must match the port number specified on the DFP Manager.

```
ip dfp agent ipmobile
  port 500
  inservice
!
```

The following command sets the source address and HA address field in the RRP to that of the real HA's address. This config is required only for Dispatched mode.

```
ip mobile home-agent dynamic-address 20.1.1.51
```

#### Show Output on SLB:

The following command verifies that the HAs report an initial weight of 25 (default weight) when DFP is configured.

```
SLB-6500#show ip slb dfp weights
  Real IP Address: 20.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
    Set by Agent 20.1.1.51:500 at 14:59:23 UTC 04/21/03
  Real IP Address: 20.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
    Set by Agent 20.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-6500#
```

The following command displays the status of server farm HAFARM and, the associated real servers, and their status. It also shows the no. of connections assigned to each of the real servers.

The show output below was captured after opening 100 MIP sessions which HA-SLB has load balanced equally across two real HA's (50 connections to each HA).

```
SLB-6500#show ip slb reals

real                farm name          weight  state          conns
-----
20.1.1.51           HAFARM             24     OPERATIONAL    50
20.1.1.52           HAFARM             24     OPERATIONAL    50
SLB-6500#
```

#### Show output on HAs:

The following command shows that 50 bindings each were opened on HA1 and HA2

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7200#
```

```
HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7200#
```

## Direct Mode With Static Weights

#### Configuration on SLB:

The following commands configure a serverfarm "HAFARM" and associates two real servers (HAs) with the serverfarm. The real servers are configured with a static weight of one. The command **nat server** configures HA-SLB in Direct (Nat server) mode of operation.

```
ip slb serverfarm HAFARM
nat server
real 20.1.1.51
  weight 1
  inservice
!
real 20.1.1.52
  weight 1
```

```

inervice

ip slb vserver MIPS LB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm HAFARM
  idle ipmobile request 300
inervice

```

**Show Output on SLB:**

The following command displays the status of server farm HAFARM and, the associated real servers, and their status. It also shows the no. of connections assigned to each of the real servers.

The show output below was captured after opening 4 MIP sessions which HA-SLB has load balanced equally across two real HA's (2 connections to each HA).

```
SLB-6500#show ip slb reals
```

real	farm name	weight	state	conns
20.1.1.51	HAFARM	1	OPERATIONAL	2
20.1.1.52	HAFARM	1	OPERATIONAL	2

The following command display all the sessions during runtime, or as long as the session objects exist.

```
SLB-6500#show ip slb sessions ipmobile
```

vserver	NAI hash	client	real	state
MIPSLB	A984DF0A00000000	15.1.1.51	20.1.1.52	IPMOBILE_ESTAB
MIPSLB	1DC0E31400000000	15.1.1.51	20.1.1.52	IPMOBILE_ESTAB
MIPSLB	2BDEE91100000000	15.1.1.51	20.1.1.51	IPMOBILE_ESTAB
MIPSLB	47E2FD1B00000000	15.1.1.51	20.1.1.51	IPMOBILE_ESTAB

```
SLB-6500#
```

**Show Output on HAs:**

The following command shows that 2 bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#
```

```
HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

The following debug when enabled shows NAT server mode is operational:

```

SLB-6500#debug ip slb sessions ipmobile
SLB-6500#
*Apr 21 15:25:58: %SYS-5-CONFIG_I: Configured from console by console
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwtS-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:26:03: SLB_SESSION: v_ip= 15.1.1.10:434 ( 7), real= 20.1.1.51, NAT= S
*Apr 21 15:26:03: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
SLB-6500#

```

## Direct Mode with DFP

### Configuration on SLB:

The following commands configure a serverfarm “HAFARM” and associates two real servers (HAs) with the serverfarm. The **nat server** command configures HA-SLB in Direct (Nat server) mode of operation.

```
ip slb serverfarm HAFARM
nat server
real 20.1.1.51
  inservice
!
real 20.1.1.52
  weight 1
  inservice
!
```

The following commands configure a virtual server with service as “ipmobile” on the SLB and associates the serverfarm HAFARM with the virtual server. The optional **idle ipmobile request** *idle-time-val* config command configures the duration for which the session object exists

```
ip slb vserver MIPS LB
virtual 15.1.1.10 udp 434 service ipmobile
serverfarm HAFARM
idle ipmobile request 300
inservice
!
```

The following command configures the DFP Manager on HA-SLB and assigns two DFP agents (clients) to which HA-SLB can connect to.

```
ip slb dfp
agent 20.1.1.51 500
agent 20.1.1.52 500
```

### Configuration on HA:

The following command configures the DFP agent on the real HA. The port number that is configured must match the port number specified on the DFP Manager.

```
ip dfp agent ipmobile
port 500
inservice
!
```

### Show Output on SLB:

The following command verifies that the HAs report an initial weight of 25 (default weight) when DFP is configured.

```
SLB-6500#show ip slb dfp weights
Real IP Address: 20.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
Set by Agent 20.1.1.51:500 at 14:59:23 UTC 04/21/03
Real IP Address: 20.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
Set by Agent 20.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-6500#
```

The following command displays the status of server farm “HAFARM”, the associated real servers, and their status. It also shows the number of connections assigned to each of the real servers.

The show output below was captured after opening 100 MIP sessions which HA-SLB has load balanced equally across two real HAs (50 connections to each HA).

```
SLB-6500#show ip slb reals
```

```
real                farm name          weight  state          conns
-----
20.1.1.51           HAFARM             24      OPERATIONAL    50
20.1.1.52           HAFARM             24      OPERATIONAL    50
SLB-6500#
```

### Show Output on HAs:

The following command shows that 50 bindings each were opened on HA1 and HA2.

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7200#
```

```
HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7200#
```

The following debug when enabled shows NAT server mode is operational:

```
SLB-6500#debug ip slb sessions ipmobile
SLB-6500#
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwtS-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 15.1.1.10:434 ( 7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwtS-mip-np-user2@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 15.1.1.10:434 ( 7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 15.1.1.51:434 session_key= 1DC0E31400000000
```

## Dispatched Mode of Operation and Crypto Transform Mode is Tunnel

The following command verifies whether or not the IPSEC VPN module status is ok

```
SLB1-6500#show module
Mod Ports Card Type                                Model                                Serial No.
-----
 1     2 Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2                    SAD070701KR
 3    48 SFM-capable 48-port 10/100 Mbps RJ45  WS-X6548-RJ-45                      SAL0706CVFQ
 5     3 MWAM Module                               WS-SVC-MWAM-1                       SAD06420188
 6     2 IPsec VPN Accelerator                   WS-SVC-IPSEC-1                      SAD064902NT

Mod MAC addresses                                Hw   Fw       Sw       Status
-----
 1 0001.6416.4ffe to 0001.6416.4fff             4.2  6.1(3)   7.5(0.94)  Ok
 3 0009.11f4.9b60 to 0009.11f4.9b8f             5.2  6.3(1)   7.5(0.94)  Ok
 5 0008.7ca8.17d8 to 0008.7ca8.17df             0.302 7.2(1)   1.0(0.1)   Ok
 6 0002.7ee4.c34e to 0002.7ee4.c351             1.0  7.2(1)   7.5(0.94)  Ok

Mod Sub-Module                                Model                                Serial                                Hw   Status
-----
```

```

1 Policy Feature Card 2      WS-F6K-PFC2      SAD07060047      3.3      Ok
1 Cat6k MSFC 2 daughterboard WS-F6K-MSFC2      SAD070701FS      2.5      Ok

```

```
Mod Online Diag Status
```

```

-----
1 Pass
3 Pass
5 Pass
6 Pass
SLB1-6500#

```

### Configuration on SLB:

```

ip slb serverfarm FARM1
  real 99.99.11.11
  inservice
!
  real 99.99.11.12
  inservice
!
ip slb vserver IPSECSLB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm FARM1
  inservice

```

The following commands configure IPSEC on HA-SLB:

```

crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco address 15.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map 12tpmap 10 ipsec-isakmp
  set peer 15.1.1.51
  set transform-set esp-des-sha-transport
  match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,15,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet6/2      (outside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,16,1002-1005
  switchport mode trunk
  cdp enable
!
interface FastEthernet3/15
  no ip address
  duplex full
  speed 100
  crypto connect vlan 15
!
!
interface Vlan15

```

```

ip address 15.1.1.15 255.0.0.0
no ip redirects
no ip unreachable
no mop enabled
crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51

```

### Configuration on PDSN:

The following commands configure IPSEC on PDSN:

```

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 15.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 15.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 15.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10

```

### Configuration on HA:

```

interface Loopback1
 ip address 15.1.1.10 255.0.0.0

ip mobile home-agent dynamic-address 99.99.11.11

```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

### Show Output on PDSN (FA):

The following command is used to verify that packets sent out of PDSN are encrypted:

```

PDSN-7200#show crypto ipsec sa

interface: FastEthernet1/0
  Crypto map tag: l2tpmap, local addr. 15.1.1.51

local ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
current_peer: 15.1.1.15
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 16, #recv errors 0

local crypto endpt.: 15.1.1.51, remote crypto endpt.: 15.1.1.15
path mtu 1500, media mtu 1500
current outbound spi: FD2E19D2

```

```

inbound esp sas:
spi: 0x2AEF7930(720337200)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3454)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:
spi: 0xE12F5466(3777975398)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3454)
  replay detection support: Y

inbound pcp sas:

outbound esp sas:
spi: 0xFD2E19D2(4247656914)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3454)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:
spi: 0x87E60F74(2280001396)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3445)
  replay detection support: Y

outbound pcp sas:

```

PDSN-7200#

### Show Output on SLB:

SLB1-6500#sh ip slb reals

real	farm name	weight	state	conns
99.99.11.11	FARM1	1	OPERATIONAL	2
99.99.11.12	FARM1	1	OPERATIONAL	2

SLB1-6500#sh ip slb sessions ipmobile

vserver	NAI hash	client	real	state
IPSECSLB	A984DF0A00000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	1DC0E31400000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	2BDEE91100000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB
IPSECSLB	47E2FD1B00000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB

```
SLB1-6500#
```

The following command is used to verify that packets received by HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa
```

```
interface: Vlan15
  Crypto map tag: l2tpmap, local addr. 15.1.1.15

local ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
current_peer: 15.1.1.51
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
path mtu 1500, media mtu 1500
current outbound spi: 2AEF7930

inbound esp sas:
  spi: 0xFD2E19D2(4247656914)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 10999, flow_id: 49, crypto map: l2tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3488)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0x87E60F74(2280001396)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 10997, flow_id: 49, crypto map: l2tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3488)
    replay detection support: Y

inbound pcp sas:

outbound esp sas:
  spi: 0x2AEF7930(720337200)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11000, flow_id: 50, crypto map: l2tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3488)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0xE12F5466(3777975398)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 10998, flow_id: 50, crypto map: l2tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3488)
    replay detection support: Y

outbound pcp sas:

SLB1-6500#
```

**Show Output on HAs:**

```
HA1-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7200#
```

```
HA2-7200#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7200#
```

**Dispatched Mode of Operation and Crypto Transform Mode is Transport****Configuration on SLB:**

```
ip slb serverfarm FARM1
  real 99.99.11.11
    inservice
  !
  real 99.99.11.12
    inservice
  !
ip slb vserver IPSECSLB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm FARM1
  inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco address 15.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
  mode transport          (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
  set peer 15.1.1.51
  set transform-set esp-des-sha-transport
  match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,15,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet6/2          (outside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,16,1002-1005
  switchport mode trunk
  cdp enable
!
interface FastEthernet3/15
  no ip address
  duplex full
  speed 100
```

```

crypto connect vlan 15
!
!
interface Vlan15
 ip address 15.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachableables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51

```

### Configuration on PDSN:

The following commands configure IPSEC on PDSN:

```

crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 15.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport          (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 15.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 15.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10

```

### Configuration on HA:

```

interface Loopback1
 ip address 15.1.1.10 255.0.0.0

ip mobile home-agent dynamic-address 99.99.11.11

```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

### Show Output on PDSN :

The following command is used to verify that packets sent out of PDSN are encrypted:

```

PDSN-7200#sh crypto ipsec sa

interface: FastEthernet1/0
  Crypto map tag: l2tpmap, local addr. 15.1.1.51

local ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
current_peer: 15.1.1.15
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0

```

```
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 4, #recv errors 0
```

```
local crypto endpt.: 15.1.1.51, remote crypto endpt.: 15.1.1.15
path mtu 1500, media mtu 1500
current outbound spi: 9DB2749C
```

```
inbound esp sas:
spi: 0x29960A54(697698900)
transform: esp-des ,
in use settings =(Tunnel, )
slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
sa timing: remaining key lifetime (k/sec): (4608000/3536)
IV size: 8 bytes
replay detection support: Y
```

```
inbound ah sas:
spi: 0x4CB25D79(1286757753)
transform: ah-sha-hmac ,
in use settings =(Tunnel, )
slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
sa timing: remaining key lifetime (k/sec): (4608000/3527)
replay detection support: Y
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x9DB2749C(2645718172)
transform: esp-des ,
in use settings =(Tunnel, )
slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
sa timing: remaining key lifetime (k/sec): (4607999/3527)
IV size: 8 bytes
replay detection support: Y
```

```
outbound ah sas:
spi: 0x3F9BDD27(1067179303)
transform: ah-sha-hmac ,
in use settings =(Tunnel, )
slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
sa timing: remaining key lifetime (k/sec): (4607999/3527)
replay detection support: Y
```

```
outbound pcp sas:
```

```
PDSN-7200#
```

### Show Output on SLB:

```
SLB1-6500#sh ip slb sessions ipmobile
```

vserver	NAI hash	client	real	state
IPSECSLB	A984DF0A00000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	1DC0E31400000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	2BDEE91100000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB
IPSECSLB	47E2FD1B00000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB

```
SLB1-6500#
```

```
SLB1-6500#sh ip sl
```

```
SLB1-6500#sh ip slb rea
```

```
SLB1-6500#sh ip slb reals
```

```

real                farm name        weight  state        conns
-----
99.99.11.11         FARM1            1       OPERATIONAL   2
99.99.11.12         FARM1            1       OPERATIONAL   2
SLB1-6500#

```

The following command is used to verify that packets received by HA-SLB are decrypted:

```
SLB1-6500#show crypto ipsec sa
```

```

interface: Vlan15
  Crypto map tag: 12tpmap, local addr. 15.1.1.15

local ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
current_peer: 15.1.1.51
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
  path mtu 1500, media mtu 1500
  current outbound spi: 29960A54

inbound esp sas:
  spi: 0x9DB2749C(2645718172)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11011, flow_id: 55, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3540)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0x3F9BDD27(1067179303)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11009, flow_id: 55, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3540)
    replay detection support: Y

inbound pcp sas:

outbound esp sas:
  spi: 0x29960A54(697698900)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11012, flow_id: 56, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3540)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0x4CB25D79(1286757753)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11010, flow_id: 56, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3540)
    replay detection support: Y

```

```
outbound pcp sas:
```

```
SLB1-6500#
```

### Show Output on HAs:

```
HA5-2#sh ip mob binding summary
Mobility Binding List:
Total 2
```

```
HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

## Direct Mode of Operation and Crypto Transform Mode is Tunnel

```
Configuration on SLB:
ip slb serverfarm FARM1
  nat server
  real 99.99.11.11
  inservice
!
  real 99.99.11.12
  inservice
!
ip slb vserver IPSECSLB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm FARM1
  inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco address 15.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
  set peer 15.1.1.51
  set transform-set esp-des-sha-transport
  match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,15,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet6/2 (outside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,16,1002-1005
  switchport mode trunk
  cdp enable
```

```

!
interface FastEthernet3/15
  no ip address
  duplex full
  speed 100
  crypto connect vlan 15
!
!
interface Vlan15
  ip address 15.1.1.15 255.0.0.0
  no ip redirects
  no ip unreachableables
  no mop enabled
  crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51

```

### Configuration on PDSN:

The following commands configure IPSEC on PDSN:

```

crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco address 15.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
  set peer 15.1.1.15
  set transform-set esp-des-sha-transport
  match address 101

interface FastEthernet1/0
  ip address 15.1.1.51 255.0.0.0
  duplex full
  crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10

```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

Show Output on PDSN:

The following command is used to verify that packets sent out of PDSN are encrypted:

```

PDSN-7200#sh crypto ipsec sa

interface: FastEthernet1/0
  Crypto map tag: l2tpmap, local addr. 15.1.1.51

  local ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
  current_peer: 15.1.1.15
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

  local crypto endpt.: 15.1.1.51, remote crypto endpt.: 15.1.1.15
  path mtu 1500, media mtu 1500
  current outbound spi: 1A274E9D

```

```

inbound esp sas:
 spi: 0xD3D5F08B(3554013323)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3026)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:
 spi: 0x7FEE86C3(2146338499)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3026)
  replay detection support: Y

inbound pcp sas:

outbound esp sas:
 spi: 0x1A274E9D(438783645)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3026)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:
 spi: 0x5F9A83(6265475)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3026)
  replay detection support: Y

outbound pcp sas:

```

PDSN-7200#

### Show Output on SLB:

The following command is used to verify that packets received by HA-SLB are decrypted:

SLB1-6500#sh crypto ipsec sa

```

interface: Vlan15
  Crypto map tag: l2tpmap, local addr. 15.1.1.15

local ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
current_peer: 15.1.1.51
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
  path mtu 1500, media mtu 1500

```

```

current outbound spi: D6C550E1

inbound esp sas:
spi: 0x267FCD46(645909830)
  transform: esp-des ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 11027, flow_id: 63, crypto map: 12tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3581)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:
spi: 0xF779A01E(4151943198)
  transform: ah-sha-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 11025, flow_id: 63, crypto map: 12tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3581)
  replay detection support: Y

inbound pcp sas:

outbound esp sas:
spi: 0xD6C550E1(3603255521)
  transform: esp-des ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 11028, flow_id: 64, crypto map: 12tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3581)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:
spi: 0x325BEB84(844884868)
  transform: ah-sha-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 11026, flow_id: 64, crypto map: 12tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3581)
  replay detection support: Y

outbound pcp sas:

```

```
SLB1-6500#sh ip slb sessions ipmobile
```

vserver	NAI hash	client	real	state
IPSECSLB	A984DF0A00000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	1DC0E31400000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	2BDEE91100000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB
IPSECSLB	47E2FD1B00000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB

```
SLB1-6500#
```

```
SLB1-6500#sh ip slb
```

```
SLB1-6500#sh ip slb rea
```

```
SLB1-6500#sh ip slb reals
```

real	farm name	weight	state	conns
99.99.11.11	FARM1	1	OPERATIONAL	2
99.99.11.12	FARM1	1	OPERATIONAL	2

```
SLB1-6500
```

```
Show output on SLB:
```

```
HA5-2#sh ip mob binding summary
```

```
Mobility Binding List:
```

```
Total 2
```

```
HA5-2#
```

```
HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

### Debug Output on SLB:

The following debug when enabled shows NAT server mode is operational:

```
SLB1-6500#debug ip slb sessions ipmobile
*Jul 1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul 1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 ( 7), real= 99.99.11.12, NAT= S
*Jul 1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= A984DF0A00000000
*Jul 1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul 1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 ( 7), real= 99.99.11.11, NAT= S
*Jul 1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= 2BDEE91100000000
*Jul 1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
```

## Direct Mode of Operation and Crypto Transform Mode is Transport

### Configuration on SLB:

```
ip slb serverfarm FARM1
  nat server
  real 99.99.11.11
  inservice
!
  real 99.99.11.12
  inservice
!
ip slb vserver IPSECSLB
  virtual 15.1.1.10 udp 434 service ipmobile
  serverfarm FARM1
  inservice
```

The following commands configure IPSEC on HA-SLB:

```
crypto isakmp policy 1
  authentication pre-share
crypto isakmp key cisco address 15.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
  mode transport (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
  set peer 15.1.1.51
  set transform-set esp-des-sha-transport
  match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,15,1002-1005
  switchport mode trunk
  cdp enable
!
```

```

interface GigabitEthernet6/2          (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 15.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachable
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51

```

### Configuration on PDSN:

The following commands configure IPSEC on PDSN:

```

crypto isakmp policy 1
 authentication pre-share
 crypto isakmp key cisco address 15.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport          (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 15.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 15.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10

```

Execute **clear crypto isakmp** and **clear crypto sa** on the PDSN and SLB. Open multiple MIP flows.

### Show Output on PDSN :

The following command is used to verify that packets sent out of PDSN are encrypted

```
PDSN-7200#sh crypto ipsec sa
```

```

interface: FastEthernet1/0
  Crypto map tag: l2tpmap, local addr. 15.1.1.51

  local ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
  current_peer: 15.1.1.15
    PERMIT, flags={origin_is_acl,}

```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 4, #recv errors 0
```

```
local crypto endpt.: 15.1.1.51, remote crypto endpt.: 15.1.1.15
path mtu 1500, media mtu 1500
current outbound spi: 6A0EBD82
```

```
inbound esp sas:
spi: 0x13E0E556(333505878)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3535)
  IV size: 8 bytes
  replay detection support: Y
```

```
inbound ah sas:
spi: 0xEFEEE153(4025409875)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4608000/3535)
  replay detection support: Y
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0x6A0EBD82(1779350914)
  transform: esp-des ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3535)
  IV size: 8 bytes
  replay detection support: Y
```

```
outbound ah sas:
spi: 0x49BE92A3(1237226147)
  transform: ah-sha-hmac ,
  in use settings =(Tunnel, )
  slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
  sa timing: remaining key lifetime (k/sec): (4607999/3535)
  replay detection support: Y
```

```
outbound pcp sas:
```

```
PDSN-7200#
```

### Show Output on SLB:

```
SLB1-6500#sh ip slb sessions ipmobile
```

vserver	NAI hash	client	real	state
IPSECSLB	A984DF0A00000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	1DC0E31400000000	15.1.1.51	99.99.11.12	IPMOBILE_ESTAB
IPSECSLB	2BDEE91100000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB
IPSECSLB	47E2FD1B00000000	15.1.1.51	99.99.11.11	IPMOBILE_ESTAB

```
SLB1-6500#
```

```
SLB1-6500#sh ip slb rea
```

```
SLB1-6500#sh ip slb reals
```

```
real          farm name      weight  state          conns
-----
99.99.11.11   FARM1           1       OPERATIONAL    2
99.99.11.12   FARM1           1       OPERATIONAL    2
SLB1-6500#
SLB1-6500#
```

The following command is used to verify that packets received by HA-SLB are decrypted:

```
SLB1-6500#sh crypto ipsec sa
```

```
interface: Vlan15
  Crypto map tag: 12tpmap, local addr. 15.1.1.15

local ident (addr/mask/prot/port): (15.1.1.10/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (15.1.1.51/255.255.255.255/0/0)
current_peer: 15.1.1.51
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
path mtu 1500, media mtu 1500
current outbound spi: 13E0E556

inbound esp sas:
  spi: 0x6A0EBD82(1779350914)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11031, flow_id: 65, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3527)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:
  spi: 0x49BE92A3(1237226147)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11029, flow_id: 65, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4607999/3527)
    replay detection support: Y

inbound pcp sas:

outbound esp sas:
  spi: 0x13E0E556(333505878)
    transform: esp-des ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11032, flow_id: 66, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3527)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:
  spi: 0xEFEE153(4025409875)
    transform: ah-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 11030, flow_id: 66, crypto map: 12tpmap
    sa timing: remaining key lifetime (k/sec): (4608000/3524)
```

```

replay detection support: Y

outbound pcp sas:

SLB1-6500#

```

**Show Output on HA:**

```

HA5-2#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-2#

```

```

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#

```

## ODAP Redundancy Configuration

**Active-HA configuration**

```

no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
redundancy inter-device
  scheme standby cisco
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 500
  local-ip 7.0.0.2
  remote-port 500
  remote-ip 7.0.0.3
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 dhcp ping packet 0
ip dhcp pool ha-dhcp-pool
  origin dhcp subnet size initial /30 autogrow /30
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 min 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 classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 33.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 33.0.0.0 255.0.0.0 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

```

no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
redundancy inter-device
scheme standby cisco
!
ipc zone default
association 1

```

```

no shutdown
protocol sctp
  local-port 500
  local-ip 7.0.0.3
  remote-port 500
  remote-ip 7.0.0.2
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 dhcp pool ha-dhcp-pool
  origin dhcp subnet size initial /30 autogrow /30
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 classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 33.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 33.0.0.0 255.0.0.0 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

```

## DHCP-Proxy-Client Configuration

### Active-HA configuration

```

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 Loopback0
ip address 12.0.0.1 255.255.255.255
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 classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile virtual-network 12.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 7.0.0.101 virtual-network 12.0.0.0 255.0.0.0
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!

```

```

ip mobile virtual-network 12.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 5.0.0.101 virtual-network 12.0.0.0 255.0.0.0
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

```

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 Loopback0
ip address 12.0.0.2 255.255.255.255
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 secure home-agent 7.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
ip mobile virtual-network 12.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 7.0.0.101 virtual-network 12.0.0.0 255.0.0.0
!
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

```

## VRF Configuration

The following is a sample configuration on an MWAM HA with VRF support:

```

CiscoHA#show running-config
Building configuration...

Current configuration : 3366 bytes
!
...
!
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa accounting network vrf-auth-grp1 start-stop group vrf-auth-grp1
aaa accounting network vrf-auth-grp2 start-stop group vrf-auth-grp2
aaa session-id common

```

```

ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf-grp1
  rd 100:1
!
ip vrf moip-vrf-grp2
  rd 100:2
!
no virtual-template snmp
!
!
!
interface Loopback1
  ip address 192.168.11.1 255.255.255.0 secondary
  ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0
  no ip address
!
interface GigabitEthernet0/0.11
  encapsulation dot1Q 11
  ip address 9.15.42.111 255.255.0.0
  no cdp enable
!
interface GigabitEthernet0/0.82
  description Interface towards PDSN
  encapsulation dot1Q 82
  ip address 82.82.82.2 255.255.0.0
!
router mobile
!
ip local pool vrf-pool1 5.5.5.1 5.5.5.254 group vrf-pool-grp1
ip local pool vrf-pool2 5.5.5.1 5.5.5.254 group vrf-pool-grp2
ip classless
ip route 9.15.47.80 255.255.255.255 GigabitEthernet0/1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 14.1.0.0 255.255.0.0 GigabitEthernet0/0.82
no ip http server
!
ip mobile home-agent
ip mobile host nai @xyz.com address pool local vrf-pool2 interface GigabitEthernet0/0.82
aaa
ip mobile host nai @cisco.com address pool local vrf-pool1 interface GigabitEthernet0/0.82
aaa
ip mobile realm @xyz.com vrf moip-vrf-grp2 ha 192.168.11.1 aaa-group accounting
vrf-auth-grp1 authentication vrf-auth-grp2
ip mobile realm @cisco.com vrf moip-vrf-grp1 ha 192.168.10.1 aaa-group accounting
vrf-auth-grp2 authentication vrf-auth-grp1
!
!
!
radius-server host 9.15.100.1 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
...
!
end

```

## VRF Configuration with HA redundancy

The following is a sample configuration on a Cisco 7200 HA with HA redundancy and VRF. The following steps are required:

- 
- Step 1** Configure normal HSRP and HA redundancy for the published HA IP address
  - Step 2** Rather than configuring IP addresses on the Loopback (or any other interface IP addresses for tunnel end-point), configure them on the HSRP interface as a secondary standby IP address.
  - Step 3** For ip mobile redundancy, add virtual network for VRF tunnel point subnet.
  - Step 4** Configure the VRF related commands.
  - Step 5** Because the binding update message from active to the standby HA contains the NAI, the standby is able to create the binding using appropriate VRF using the domain of the NAI in the message.
- 

```

Active HA:
HA1#sh run
...
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
  server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
  server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa session-id common
ip subnet-zero
ip gratuitous-arps
!
!
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf
  rd 100:1
!
ip vrf moip-vrf1
  rd 100:2
!
...
!
interface FastEthernet1/0
  ip address 92.92.92.2 255.255.0.0
  duplex auto
  speed auto
  no cdp enable

```

```

standby 10 ip 92.92.92.12
standby 10 ip 192.168.11.1 secondary
standby 10 ip 192.168.12.1 secondary
standby 10 priority 130
standby 10 preempt delay sync 10
standby 10 name cisco
!
!
router mobile
!
ip local pool vrf-pool1 5.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 5.5.5.5 5.5.5.55 group vrf-pool-grp2
ip classless
ip mobile home-agent address 92.92.92.12
ip mobile home-agent redundancy cisco virtual-network address 192.168.0.0
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 92.92.92.3 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 192.168.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 9.15.100.1 auth-port 1645 acct-port 1646 key cisco
!
...
end

Standby HA:
HA2#sh run
...
!
aaa new-model
!
aaa group server radius vrf-auth-grp1
server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip vrf moip-vrf
rd 100:1
!
ip vrf moip-vrf1
rd 100:2

```

```
!
...
!
interface FastEthernet1/0
 ip address 92.92.92.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 92.92.92.12
 standby 10 ip 192.168.11.1 secondary
 standby 10 ip 192.168.12.1 secondary
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
...
!
router mobile
!
ip local pool vrf-pool1 5.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 5.5.5.5 5.5.5.55 group vrf-pool-grp2
ip mobile home-agent address 92.92.92.12
ip mobile home-agent redundancy cisco virtual-network address 192.168.0.0
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 92.92.92.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 192.168.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix ignore-spi
ip mobile secure home-agent 192.168.12.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
no ip http server
!
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 9.15.100.1 auth-port 1645 acct-port 1646 key cisco
...
end
```

## Authentication and Authorization RADIUS Attributes

The Home Agent, and the RADIUS server support RADIUS attributes listed in [Table 1](#) for authentication and authorization services.

**Table 1 Authentication and Authorization AVPs Supported by Cisco IOS**

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In	
						Access Request	Access Accept
User-Name	1	NA	64	string	User name for authentication and authorization.	Yes	No
User-Password	2	NA	>=18 && <=130	string	Password for authentication when using PAP. Password configured using CLI at Home Agent.	Yes	No
CHAP-Password	3	NA	19	string	CHAP password	Yes	No
NAS-IP-Address	4	NA	4	IP address	IP address of the HA interface used for communicating with RADIUS server	Yes	No
Service Type	6	NA	4	integer	Type of service the user is getting. Supported values: <ul style="list-style-type: none"> <li>Outbound sent for PAP</li> <li>Framed sent for CHAP</li> <li>Framed received in both cases</li> </ul>	Yes	Yes
Framed-Protocol	7	NA	4	integer	Framing protocol user is using. . Sent for CHAP, received for PAP and CHAP. Supported values: <ul style="list-style-type: none"> <li>PPP</li> </ul>	Yes	Yes
Framed Compression	13	NA	4	integer	Compression method Supported values: <ul style="list-style-type: none"> <li>0 - None</li> </ul>	No	Yes
Framed-Routing	10	NA	4	integer	Routing method Supported values: <ul style="list-style-type: none"> <li>0 - None</li> </ul>	No	Yes
Vendor Specific	26	NA			Vendor specific attributes	Yes	Yes
CHAP-Challenge (optional)	60	NA	>=7	string	CHAP Challenge	Yes	No
NAS-Port-Type	61	NA	4	integer	Port Type Supported: <ul style="list-style-type: none"> <li>0 - Async</li> </ul>	Yes	No

**Table 1 Authentication and Authorization AVPs Supported by Cisco IOS (continued)**

Authentication and Authorization AVPs Supported By Cisco IOS Name	Type	Vendor	Length	Format	Description	Allowed In	
						Access Request	Access Accept
spi#n	26/1	Cisco	>=3	string	n is a numeric identifier beginning with 0 which allows multiple SAs per user  Provides the Security Parameter Index (SPI), for authenticating a mobile user during MIP registration  The information is in the same syntax as the <b>ip mobile secure host addr</b> configuration command. Essentially, it contains the rest of the configuration command that follows that string, verbatim.	No	Yes
static-ip-addresses	26/1	Cisco	>=3	string	IP address list for static addresses for same NAI but multiple flows.	No	Yes
static-ip-pool	26/1	Cisco	>=3	string	IP address pool name for static address for same NAI with multiple flows.	No	Yes
ip-addresses	26/1	Cisco	>=3	string	IP address list used for dynamic address assignment.	No	Yes
ip-pool	26/1	Cisco	>=3	string	IP address pool name used for dynamic address assignment.	No	Yes
dhcp-server	26/1	Cisco	>=3	string	Get an address from the specified DHCP server	No	Yes
MN-HA SPI Key	26/57	3GPP2	6	integer	SPI for MN HA Shared Key	Yes	No
MN-HA Shared Key	26/58	3GPP2	20	string	Secure Key to authenticate MHAE	No	Yes

# 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

