Cisco Mobile Wireless Home Agent Release 5.1 for Cisco IOS Release 12.4(22)YD1

12.4(22)YD1
02 December 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-21443-01

Cisco Mobile Wireless Home Agent Release 5.1 for Cisco IOS Release 12.4(22)YD1

CONTENTS

CHAPTER 1

Overview of the Cisco Mobile Wireless Home Agent

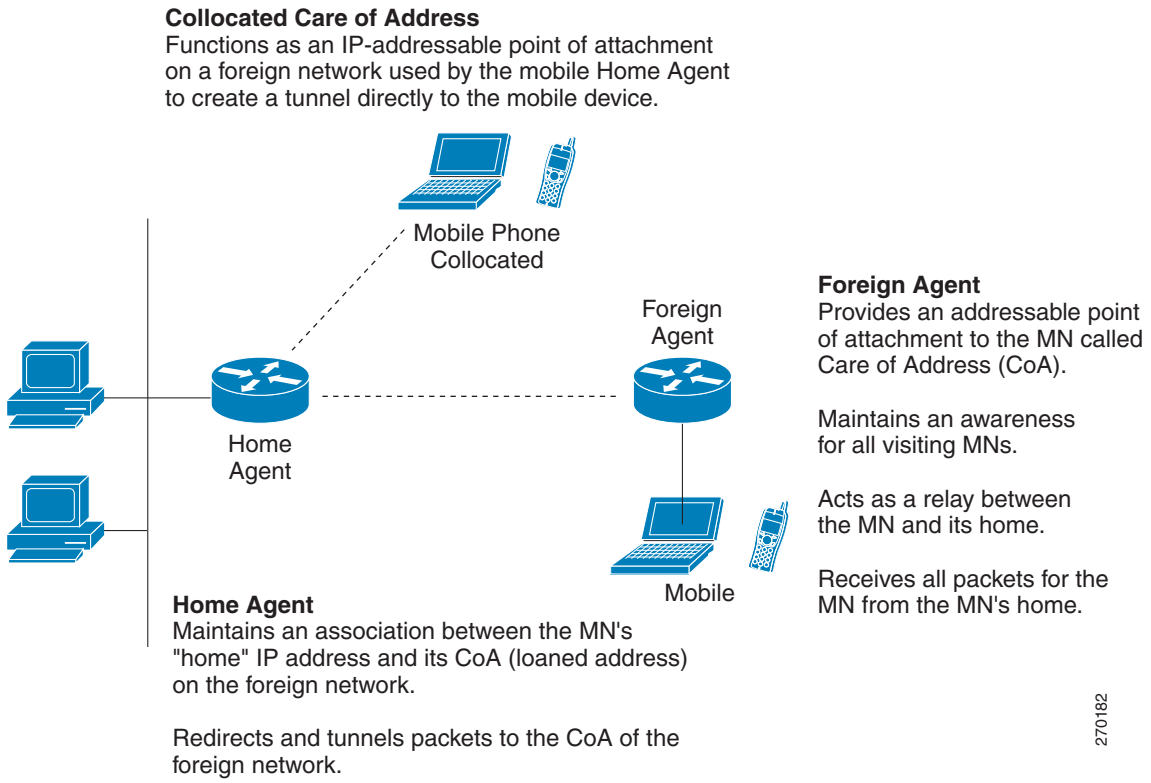
This chapter illustrates the functional elements in a typical Mobile IP packet data system, the Cisco products that are currently available to support this solution. and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

Feature Overview

The Cisco Mobile Wireless Home Agent serves as an anchor point for subscribers, providing easy, secure roaming with quality of service (QoS) capabilities to optimize the mobile user experience. The Cisco Mobile Wireless Home Agent (HA) works in conjunction with a Foreign Agent (FA) and mobile node to provide an efficient Mobile IP solution. Figure 1-1 shows a basic topology.

Figure 1-1 Mobile IP Topology



The Cisco Mobile Wireless Home Agent maintains mobile user registrations-through a foreign agent, or in collocated mode (CCOA), and tunnels packets destined for the mobile device to the foreign agent. It supports reverse tunneling, and can securely tunnel packets to the foreign agent using IP Security (IPSec). Additionally, the Cisco Mobile Wireless Home Agent supports dynamic and static home address assignment—for both public and private addresses—for the mobile device. Home address assignment occurs from address pools configured either locally or remotely using Dynamic Host Configuration Protocol (DHCP) server access, or from the authentication, authorization, and accounting (AAA) server.

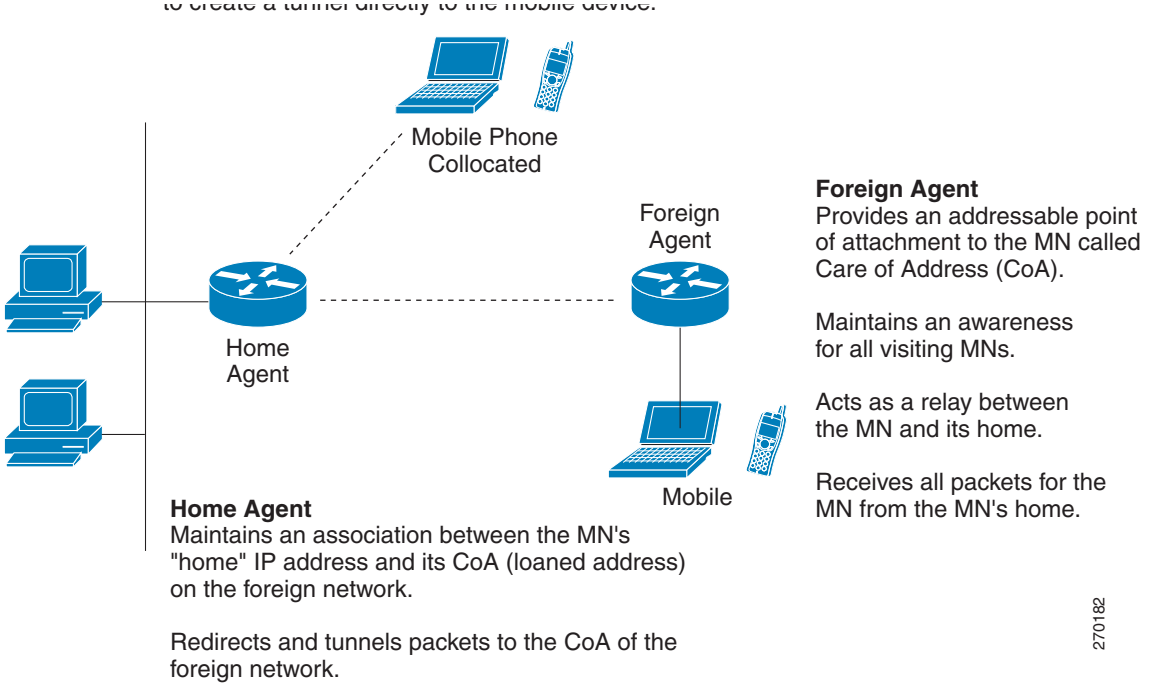
The Cisco Mobile Wireless Home Agent is the anchor point for mobile terminals for which mobile or proxy mobile services are provided. Traffic sent to the terminal is routed using the Home Agent. With reverse tunneling, traffic from the terminal is also routed through the Cisco Mobile Wireless Home Agent. Unique features such as Home-Agent redundancy and load balancing provide a high level of availability and reliability, and allow geographical dispersion while maintaining accounting integrity. Another unique feature, Network Address Translation (NAT) traversal, allows the Cisco Home Agent to be used as an anchor point across many access technologies. This allows users to transparently roam across different access networks while retaining a constant connection and addressability.

Cisco Mobile Wireless Home Agent in a CDMA Environment

CDMA2000 is a third-generation (3G) wireless solution that allows the mobile wireless operator already using CDMA technology to offer packet data services. The Cisco CDMA2000 Packet Data Services solution is designed to meet the needs of the mobile wireless industry as it transitions toward 3G cellular data services. The Cisco Mobile Wireless Home Agent is an important component of this solution. The Cisco CDMA2000 Packet Data Services solution includes the Cisco Packet Data Serving Node (PDSN) with the Foreign Agent function, the CDMA2000-based Cisco Mobile Wireless home agent, the Cisco Network Registrar®, Cisco Access Registrar® server, and several other security products and features. Figure 1-2 illustrates the functional elements in a typical Cisco CDMA2000 Packet Data Services system.

The Cisco Mobile Wireless Home Agent is part of a Cisco Systems® solution that complies with international wireless standards, enables expanded mobility, and is always addressable and reachable through the use of Mobile IP and proxy Mobile IP. The Cisco Mobile Wireless Home Agent, in conjunction with the Cisco Packet Data Serving Node (PDSN) Foreign Agent, allows a mobile station with Mobile IP client functions to access the Internet or a corporate intranet using Mobile IP-based service access. Mobile IP extends user mobility beyond the coverage area and provides roaming capabilities. In a CDMA2000 environment, when another Cisco PDSN is allocated to the call (following a handoff), the new Cisco PDSN performs a Mobile IP registration with the Cisco Mobile Wireless Home Agent. This helps to ensure that the same home address assigned when the initial session is established is allocated to the mobile client. Traffic is routed through the Cisco Mobile Wireless Home Agent, and the home agent also provides proxy Address Resolution Protocol (ARP) services. When reverse tunneling is used, traffic from the terminal also is routed through the home agent. Clients without a Mobile IP client can take advantage of these services by using the proxy Mobile IP or client Mobile IP capabilities. Figure 1-2 shows a CDMA2000 Network with a Cisco Mobile Wireless Home Agent and other required components for packet data services.

Figure 1-2 CDMA2000 Network



As the illustration shows, the mobile station, which must support either Simple IP or Mobile IP, connects to a radio tower and BTS. The BTS connects to a BSC, which contains a component called the Packet Control Function (PCF). The PCF communicates with the Cisco PDSN through an A10/A11 interface. The A10 interface is for user data and the A11 interface is for control messages. This interface is also known as the RAN-to-PDSN (R-P) interface. For the Cisco Home Agent Release 2.1 and above, you must use a Giga Ethernet (GE) interface on the Cisco SAMI platform.

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

For “back office” connectivity, such as connections to a AAA server, the interface is media independent.

The Home Agent, in conjunction with the PDSN and Foreign Agent, allows a mobile station with Mobile IP client function, to access the Internet or corporate intranet using Mobile IP-based service access. Mobile IP extends user mobility beyond the coverage area of the current, serving PDSN/Foreign Agent. If another PDSN is allocated to the call (following a handoff), the target PDSN performs a Mobile IP registration with the Home Agent; this ensures that the same home address is allocated to the mobile station. Additionally, clients without a Mobile IP client can also make use of these services by using the Proxy Mobile IP capability provided by the PDSN.

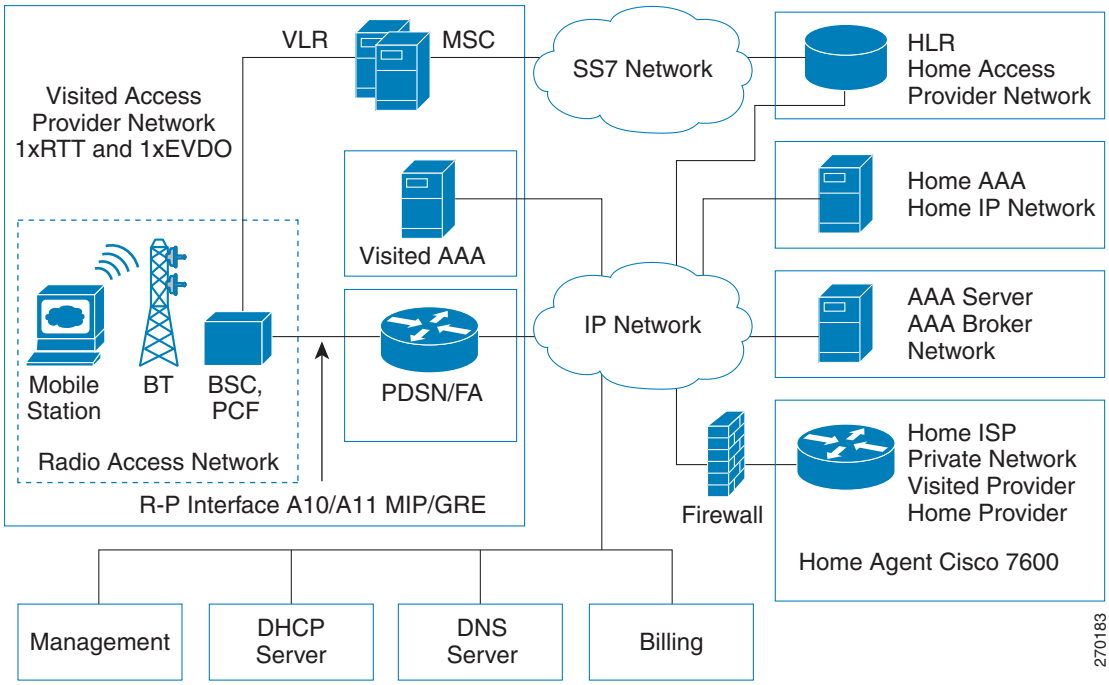
The Home Agent, then, is the anchor point for mobile terminals for which MobileIP or Proxy MobileIP services are provided. Traffic is routed through the Home Agent, and the Home Agent also provides Proxy ARP services. In the case of reverse tunneling, traffic from the terminal is also routed through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

The Cisco Mobile Wireless Home Agent supports all required standards, including the Third-Generation Partnership Project 2 (3GPP2) Technical Specification Group P and X (TSG-P, TSG-X) Standard, and the Wireless IP Network Standard (also known as TIA/EIA/IS-835-D), which defines the overall structure of a CDMA2000 network. It includes features such as enhanced Mobile IP, security, and authentication.

Cisco Mobile Wireless Home Agent in a WiMAX Environment

WiMAX (Worldwide Interoperability for Microwave Access) is fourth-generation (4G) wireless solution based on IEEE standard technology for delivering advanced broadband wireless services in emerging, high-growth and developed markets. WiMAX offers significant additional benefits, most significantly lower deployment costs through the use of an all-data, all-IP architecture, lower spectrum acquisition costs, and a wide range of IP-enabled applications, many of which come from the IP broadband domain. The Cisco Home Agent is part of the Core Service Node in the WiMAX End-to-End Reference Model. The WiMAX end-to-end Reference Model consists of the following logical entities: Mobile Subscriber Station (MSS), Access Service Network (ASN), and Core Service Network (CSN). Further ASN Decomposition is shown in Figure 1-3. The Network Reference Model (NRM) is a logical representation of the network architecture. The NRM identifies functional entities, and reference points over which interoperability may be achieved between functional entities.

Figure 1-3 WiMAX Reference Model



The Access Services Network (ASN)

The ASN is defined as a set of network functions that provide radio access to a WiMAX subscriber. ASN comprises network elements such as Base Station(s) (in one or more Base Station Clusters), and ASN Gateway(s). An ASN may be shared by more than one Connectivity Service Networks (CSN).

Connectivity Service Network (CSN)

The Connectivity Services Network (CSN) is a set of network elements that provides the IP connectivity to the service layer. Provisioning elements such as the AAA and DHCP servers are residing in the CSN as well as the macro mobility anchor point, a function enabled by the Home Agent. The service layer provides the foundation for enabling the delivery of rich services, subscriber identification and policy enforcement. Cisco is helping service providers evolve towards network convergence through its comprehensive IP Next Generation Network (NGN) vision, architecture and networking solutions. The WiMAX Forum Network Reference Model (as defined by the organization's Network Working Group) hints at the use of network, service control and application layer convergence.

Hardware Platform Support

The Cisco Mobile Wireless Home Agent runs on the Cisco Service Application Module for IP (SAMI) for the Cisco 7600 Series. The physical interfaces supported on the Cisco 7600 Series platforms are mainly Fast Ethernet and Gigabit Ethernet, FlexWAN (ATM, Frame Relay), and the new line of Shared Port Adaptor (SPA) and SPA Interface Processor (SIP) line cards, and are independent of physical media.

Additionally, the Cisco Mobile Wireless Home Agent runs on the Cisco 7301 Series router.

Supervisor Support

HA release 5.1 features are supported on the following SUP32, SUP720 and RSP720 variants. The Product Numbers of the supervisors required are:

- WS-SUP32-GE-3B(=)
- WS-SUP32-10GE-3B(=)
- WS-SUP720-3BXL(=)
- WS-SUP720-3B(=)
- WS-SUP720(=)
- RSP720-3C-GE(=)
- RSP720-3CXL-GE(=)
- RSP720-3CXL-10GE(=)

Session Redundancy Infrastructure

In Home Agent Release 5.0 and above, the HA uses the same Session Redundancy infrastructure that is used for other Cisco Msef products. The external behavior for redundancy will change significantly. The Home Agent specific redundancy scheme of Release 4.0 and before is still supported. However, the SR-infrastructure-based approach is not compatible with the previous Home Agent redundancy scheme.

The Home Agent redundancy scheme in 5.0 and above maintains the use of HSRP as the means of Active/Standby role resolution as well as being the mechanism for determining that a failure has occurred.

For more information regarding Session Redundancy, consult the Home Agent Session Redundancy Infrastructure, page 6-3:

Platform Benefits

- Home Agent SAMI service module leverages carrier class Cisco 7600 Series Router, which offers a variety of chassis configurations for different deployment scenarios.
- Highly scalable solution allows the system to rapidly scale by adding more service modules to meet traffic loads
- A very robust and proven approach that has been used to support a variety of different applications in the mobile space.

Packet Data Services

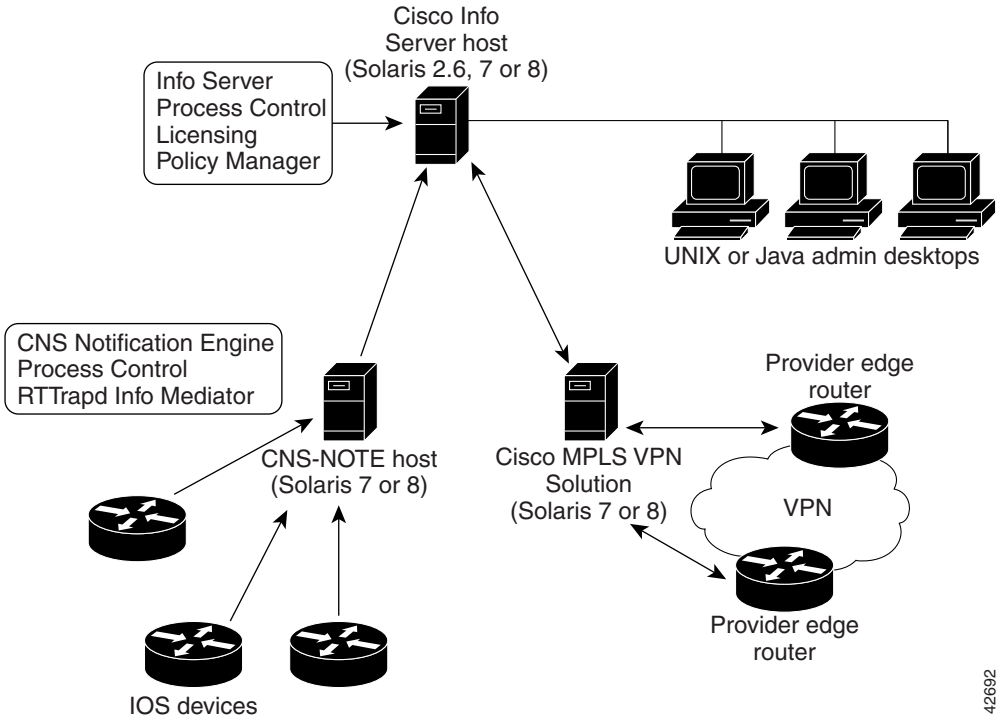
In the context of a CDMA2000 network, the Cisco Home Agent supports two types of packet data services: Mobile IP and Proxy Mobile IP services. From the perspective of the Cisco Home Agent, these services are identical.

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 12.4 documentation modules *Cisco IOS IP Mobility Configuration Guide, Release 12.4* and *Cisco IOS IP Mobility Command Reference, Release 12.4*. 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 IOS Release 12.4(22)YD1

This section describes features that were introduced or modified in Home Agent Release 5.0 for Cisco IOS Release 12.4(22)YD1:

- Conserve Unique IP ID for FA-HA IP-in-IP Tunnel, page 3-20
- Setting Fragmentation Size of First Packet With Offset=0, page 3-21
- CoA for WiMAX Hotlining, page 15-11
- DNS Redirection with Monitoring, page 9-4
- NAI Authentication with Local MN-HA SPI and Key, page 5-4
- IP Redirect for Non-Hotlined Users, page 15-6
- In/Out Access List Per NAI/Realm, page 10-3
- HA - Realm Case-Insensitive Option, page 16-2
- FA-HA Auth Extension Mandatory, page 16-3
- Absolute Timeout Per NAI, page 16-7
- AAA Attributes for “ip mobile host/realm”, page 16-20
- VSE Support for China Telecom Attributes, page 3-22
- OM Metrics for 3GPP2 / WiMAX Bindings, page 16-31
- Single IDB for MIP/UDP Tunnels, page 16-32
- Redundancy Support for Hotlining, page 15-4
- No Authorization for Re-Reg / De-Reg, page 5-4
- Tunnel Stats via SNMP, page 17-2
- 3GPP2 RRQ Without MHAE, page 5-3

This section describes features that were introduced prior to Cisco IOS Release 12.4(22)YD1:

- Single IP Infrastructure
  - Single Interface for MIP, page 3-3
  - Single Interface for Configuration, page 3-3
  - Single Interface for SNMP Management, page 3-4
  - Single Interface for Trouble Shooting and Debug, page 3-4
  - Single Interface for AAA, page 3-4

  - Single Interface for MIP and AAA, page 3-5
  - Single Interface for Failover, page 3-10
  - Trap Generation for AAA Unresponsiveness, page 3-11
  - Intra-Chassis Configuration Synchronization, page 3-14
- Home Agent Session Redundancy Infrastructure, page 6-3
- Unbounded Limit For Maximum Bindings When Configuring CAC on the HA, page 16-14
- Congestion Control Feature, page 16-14
- Foreign Agent Classification, page 16-28
- MAC Address as Show/Clear Binding Key, page 16-30
- Data Path Idle Timer, page 16-30
- Support for RFC 4917, page 16-34
- Address Assignment Feature, page 4-1
- MAC Address as Show/Clear Binding Key, page 16-30
- Accounting Interim Sync, page 12-4
- Single IP Home Agent Accounting Support, page 12-2
- Per Domain Accounting, page 12-4
- Support for Acct-Terminate-Cause, page 16-26
- Authentication Configuration Extension, page 5-2

This section lists features that were introduced or modified before Cisco IOS Release 12.4(15)XM1:

- Support for the Cisco 7301 Series Router platform.
- Support for Service and Application Module for IP (SAMI), page 2-1

  Cisco HA 4.0 and above will run on the Cisco SAMI cards in the 7600 Series Router chassis. The SUP720, SUP32 and RSP720 will be used in the 7600 chassis, and will also host the IOS SLB component for load-distribution.

  Up to 9 SAMI cards can be supported in a single Cisco 7600 Series Router chassis.
- Enhancements to Hot-lining, page 15-1
- Enhancements to Home Agent Quality of Service, page 14-1
- Framed-Pool Standard, page 16-16
- WiMAX AAA Attributes, page 16-19
- MS Traffic Redirection in Upstream Path, page 16-12
- Per Foreign-Agent Access-Type Support, page 16-27
- Support for Call Admission Control (CAC), page 16-14
- Priority-Metric for Local Pool, page 16-16
- Mobile IPv4 Host Configuration Extensions RFC4332, page 16-18

This section describes features that were introduced or modified in prior to Home Agent Release 4.0:

- Support for Mobile Equipment Identifier (MEID)
- Home Agent Accounting Enhancements
  - Home Agent Accounting in a Redundant Setup

  - Packet count and Byte count in Accounting Records
  - Additional Attributes in the Accounting Records
  - Additional Accounting Methods—Interim Accounting is Supported.
- VRF Mapping on the RADIUS Server
- Conditional Debugging Enhancement
- Home Agent Redundancy Enhancements
  - Geographical Redundancy
  - Redundancy with Radius Downloaded Pool Names
- CLI for IP-LOCAL-POOL-MIB
- Mobile-User ACLs in Packet Filtering
- IP Reachability
- DNS Server Address Assignment
- Mobile IP MIB Enhancements in Network Management, MIBs, and SNMP on the Home Agent

This section describes features that were introduced or modified in previous releases of the Cisco Mobile Wireless Home Agent:

- Mobile IPv4 Registration Revocation, page 8-1
- HA Server Load Balancing, page 7-1
- Overview of HA Accounting, page 12-1
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE), page 5-5
- VRF Support on HA, page 13-1
- Radius Disconnect, page 8-4
- Conditional Debugging, page 17-5
- Home Address Assignment, page 4-1
- Home Agent Redundancy, page 6-1
- Virtual Networks, page 6-9
- Mobile IP IPSec, page 11-2
- Support for ACLs on Tunnel Interface, page 16-10
- Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY, page 16-10
- 3 DES Encryption, page 11-1
- User Profiles, page 16-11
- Mobility Binding Association, page 16-11
- User Authentication and Authorization, page 5-1
- HA Binding Update, page 16-12
- Per User Packet Filtering, page 10-1
- Security, page 11-1

Feature Support

In addition to supporting Cisco IOS networking features, a 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.

Features No Longer Supported

In Home Agent Release 5.0 and above, the following features are no longer supported.

- MIP/LAC (PPP Regeneration) Support
- ODAP (On-Demand Address Pool)

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 Mobile Wireless HA supports proxy Mobile IP functionality, and is available on the Cisco 7600 Series Router platforms.

A Cisco HA based on the Cisco 7600 series router, with two SAMI cards housing six active HA images and six standby images, would support the above figures multiplied by 6.

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.

CHAPTER 2

Planning to Configure the Home Agent

This chapter provides information that you should know before configuring a Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

Supported Platforms

The Cisco HA is available on the Cisco SAMI processor blade that fits in the 7600 series routers, and on the Cisco 7301 Series Router. The HA supports Fast Ethernet and Gigabit Ethernet interfaces on these platforms.

Support for Service and Application Module for IP (SAMI)

For information on how to install and configure the Cisco Service and Application Module for IP, use the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps5510/products_installation_and_configuration_guide_book09186a0080875d19.html

Prerequisites

The section below provides general guidelines to follow before configuring a Cisco Mobile Wireless Home Agent in your network:

Home Agent on 7600 Series Router

For platform details and complete list of interfaces supported on 7600 series router, please refer to the following URL on Cisco.com:
http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

The supported configuration for the HA based on the 7600 Series switch is dependent on the desired capacity, interface type to be deployed and whether IPSec support is required.

Before you install the Cisco HA, keep the following considerations in mind:

The SAMI requires either a Supervisor Engine 32, or a Supervisor Engine-720 (WS-SUP720-3BXL), with MSFC-3 (WS-SUP720)/PFC-3 (WS-F6K-PFC3BXL). For details, see the "Upgrading to a New Software Release" section in the Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers. SRB1 or higher is required for Sup32 and Sup720, and SRC is required for RSP720.

A Cisco SAMI module is required to run HA functionality. Each SAMI module supports 6 HA images (6 HA instances).

For IPSec support, an IPSec VPN accelerator for the Catalyst platform (VPNSPA) is required per 7600 chassis.

Configuration Tasks

This section describes the steps for configuring the Cisco Home Agent. Each image is described by platform number.

- c7svcsamifeature-mz HA image

Upgrading the SAMI Software

The SAMI comes preloaded with the operating system software. However, to take advantage of new features and bug fixes, you can upgrade your SAMI with a new version of the software when it becomes available.

The SAMI software (image name c7svcsamifeature-mz) is a bundle of images - comprised of images for the base card and daughter card components.

Each image in the bundle has its own version and release numbers. When an upgrade is initiated using the upgrade hw-module privileged EXEC command, the version and release numbers in the bundle are compared to the versions currently running. If the versions are different, that image is automatically upgraded.

Note The show module command displays the software version of the LCP image, not the version of the full SAMI bundle.

To upgrade the SAMI image, perform the following tasks:

	Command	Purpose
Step 1	`Sup> enable`	Enters privileged EXEC mode.
Step 2	`Sup# upgrade hw-module slot slot_num software file` *`url/file-name`*	Copies the bundled image from the specified URL to the compact flash.
Step 3	`Sup# hw-module module` *`slot_num reset`*	Resets the module by turning the power off and then on. SAMI resets using the new images.
Step 4	`Sup# show upgrade software progress`	Displays status of the upgrades that are occurring.
Step 5	`Sup# show module` *`slot_num`*	Ensures that the SAMI card comes up properly after the reset. The status of the SAMI should be "OK".

Here is an example of the **show module** command:

```
sup#show module 2
Mod Ports Card Type Model Serial No.
--- ----- -------------------------------------- ------------------ -----------
2 1 SAMI Module (h2ik9s) WS-SVC-SAMI-BB-K9 SAD121202UK

Mod MAC addresses Hw Fw Sw Status
--- ---------------------------------- ------------ ------------ -------
2 001f.6c89.0dca to 001f.6c89.0dd1 2.2 8.7(0.22)FW1 12.4(2009020 Ok

Mod Sub-Module Model Serial Hw Status
---- --------------------------- ------------------ ----------- ------- -------
2 SAMI Daughterboard 1 SAMI-DC-BB SAD121204DZ 1.1 Ok
2 SAMI Daughterboard 2 SAMI-DC-BB SAD121204CL 1.1 Ok

Mod Online Diag Status
---- -------------------
2 Pass
```

Configuration Example

To perform an image upgrade on a SAMI in slot 2 of the Cisco 7600 chassis, enter the following commands.

```
Sup>
Sup> enable
Sup# upgrade hw-module slot 2 software file
tftp://10.1.1.1/c7svcsami-h1is-ms
Loading c7svcsami-h1is-ms from <TFTP SERVER IPADDRESS> (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 34940891 bytes]
Sup# hw-module module 2 reset
Proceed with reload of module?[confirm]
% reset issued for module 2
Sup#
Apr 18 17:53:16.149 EDT: SP: The PC in slot 2 is shutting down. Please wait ...
Apr 18 17:53:33.713 EDT: SP: PC shutdown completed for module 2
000151: Apr 18 17:53:33.713 EDT: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off
(Reset)
```

```
000152: Apr 18 17:57:52.033 EDT: %MLS_RATE-4-DISABLING: The Layer2 Rate Limiters have been
disabled.
000153: Apr 18 17:57:51.513 EDT: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal
Diagnostics...
000154: Apr 18 17:57:51.537 EDT: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
000155: Apr 18 17:57:52.073 EDT: %OIR-SP-6-INSCARD: SAMI inserted in slot 2, interfaces
are now online
000156: Apr 18 17:57:59.589 EDT: %SVCLC-5-FWTRUNK: Firewalled VLANs configured on trunks
Sup#
```

User Migration

With the end of life of the Home Agent software on the Cisco 7200 and MWAM, this section addresses the migration path from old releases (R3.1, or prior) on either the Cisco 7200 or MWAM, to Home Agent (HA) Release 4.0 and above on the SAMI platform.

Here are several Migration scenarios that are possible:

Table 2-1 Migration Scenarios

	HA R3.0 or Older	HA R3.1 or Older	HA R4.0 and above
Platform	NPE400/NPE-G1	MWAM	SAMI
Chassis/Power Supply, Fan Trays)	7200VXR	SUP-redundancy/SLB	SUP-redundancy/SLB
		SUP IOS SX based	SUP IOS SRB based
		SUP2/SUP720/SUP32	SUP720/RSP720
		6500/7600	7600

Obviously, there are many possible migration scenarios. Typically, there are many foreign agents sharing the same (one, or more) redundant or non-redundant home agents. The Mobile IP flow gets the home agent address either through a statically configured mobile device, or a foreign agent configuration, or user profile defined on AAA servers. In case of home agent SLB, the real home agent address is given by the SLB server.

The actual migration path should be determined per-customer end-to-end deployment. This means that migration should be engineered, and offers you the opportunity to redesign your network (for example, redesigning IP address schemes and configuring routing protocols, network connectivity between foreign agents and home agents, application connectivity between home agents and AAA servers, routing on the new SAMI home agent, etc.). We recommend that you perform the migration in a maintainence window. For example, if a mobile device is statically configured with the home agent IP address, the migration should be well tested in the your environment. Making a home agent IP address change aware to MS/FA may require massive network service provisioning.

Table 2-2 offers several migration paths:

Table 2-2 Migration Scenarios for the Cisco Mobile Wireless Home Agent on the Cisco SAMI Blade

Scenario	From	To	Comments
1	Non-redundant Non-SLB One 7200VXR/NPE-G1	Non-redundant Non-SLB One SUP720/SAMI	Significant configurationchange for both hardware and software.
2	Non-redundant Non-SLB Multiple 7200VXR/NPE-G1	Non-redundant SLB enabled One SUP720/SAMI	Significant configuration change for both hardware and software.
3	Redundant Non-SLB Two 7200VXR/NPE-G1	Redundant Non-SLB SUP720/redundancy Two SAMI (single chassis)	Significant configuration change (hardware and software)
4	7600/redundant SUP2 HA-SLB enabled redundant MWAM (single chassis)	7600/redundant SUP720 HA-SLB enabled Redundant SAMI (single chassis)	Very large configuration change (from SUP2 to SUP720, the whole chassis is reset) for hardware and software.
5	7600/redundant SUP720 HA-SLB enabled redundant MWAM (Single chassis) SUP IOS SXF	7600/redundant SUP720 HA-SLB enabled redundant SAMI (the same Single chassis) SUP IOS SRB	Minimal configuration change for hardware and software. Changing from SXF to SRB release for SUP requires chassis reset.
6	7600/redundant SUP720 HA-SLB enabled redundant MWAM (Dual chassis) SUP IOS SXF	7600/redundant SUP72 HA-SLB enabled redundant SAMI (Dual chassis) SUP IOS SRB	Minimal configuration change for hardware and software.

Feature Compatibility and Seamless Migration

Migration means far more than simply replacing MWAM modules with SAMI modules. It should be well designed, and conducted in a way that has minimal impact on the existing mobile subscriber's service connections.

If there is no redundancy backward compatibility on Home Agent Release 4.0 and above, HA-SLB can be enabled and configured to avoid service-disruption, which requires extra network configuration and provisioning. If there is redundancy backward compatibility on Home Agent R4.0, network configuration and provisioning will be minimal.

Table 2-3 offers various steps you need to take in order to migrate to the SAMI platform. Each of the possible migration scenarios is considered.

Table 2-3 Migration Steps that Correspond to Migration Scenarios from Table 2-2

Scenario	Migration Steps
1	• Install and configure the Home Agent on the Cisco 7600/SUP720 with SAMI. • Provision MS and Foreign Agents to use the newly added SAMI-based Home Agent (this may be a very large task). • Instead of large provisioning tasks, the SAMI Home Agent can reuse the 7200 NPE-G1-based Home Agent IP addresses and routing schemes (presuming that this is done in a maintainence window, and service is disrupted).
2	• Install and configure the Home Agent on a Cisco 7600/SUP720 with SAMI and SLB enabled. The Home Agent SLB needs to be tested on SUP720 SRB release. • Provision the MS and foreign agents to use the newly added SAMI-based Home Agents (this may be a very large provisioning task).
3	• Install and configure the Home Agent on a Cisco 7600/SUP720 with SAMI, and put them in the same HSRP redundancy group as configured on a 7200-based HA. • Configure higher priority and HSRP preemption on the SAMI-based HA. **Note** SAMI HA R4.0 may not be backward compatible in term of redundancy – HA R4.0 has per-binding based features such as rule-based hotlining, and QoS and host extension attributes (the per-binding feature is also applicable for profile-based hotlining). This actually increases per-binding information compared to the per-binding information in R3.1, or prior. Whether synching bindings from Release 3.x to R4.0 works or not is not yet tested. So far the binding information is only information synched between the active HA and standby HA in HA R3.x. – If HA R4.0 high availability is L3-based, rather than L2 HSRP based, stateful redundancy from HA R3.x to HA R4.0 will not be compatible. If this is the case, the configuration for this redundancy will be quite different between the two releases. – HA R4.0 does batch mode for bulk-sync while HA R3.x sync is on a per binding basis. • This is the ideal case, and does not have to be done in a maintainence window.
4	• For the single chassis, changing from SUP2 to SUP720 is a non-trivial task. The whole chassis is reset so all service modules (such as MWAM and SAMI) are reset, too. • You have to perform this migration during a maintanence window, and user service will be disrupted. • You must verify HA-SLB.

Table 2-3 Migration Steps that Correspond to Migration Scenarios from Table 2-2 (continued)

Scenario	Migration Steps
5	• For a single chassis, changing from SUP720 SXF to SUP720 SRB resets the whole chassis, so all service modules (such as MWAM and SAMI) are reset, too. • You must perform this migration during a maintanence window. • After this, both SUP720 in the same chassis run SRB release. • Configure the SUP720 to support SAMI: 1. Make sure MWAM configurations are saved on SUP720 bootflash 2. Configure the VLAN for SAMI VLAN groups on SUP720 as MWAM 3. Ensure that the SAMI PPC configuration taken from the MWAM processors configurations according to SAMI configuration file name convention in SUP720 bootflash. 4. Power down the standby MWAM and pull it out. 5. Insert the SAMI blade in the same slot, and boot it with the correct HA R4.0 image. 6. The MWAM HA has 5 running IOS configurations while the SAMI has 6 PPC. This implies that either one PPC on the SAMI is unused, or needs to be configured alone. 7. Verify that the SAMI PPC gets the proper configurations. 8. The HA binding synchronization and stateful redundancy faces the same situation as in scenario #3. • Disconnect and remove the active MWAM, and plug in the second SAMI blade . • Verify that HA-SLB works. If HA redundancy does not work across the releases, perform the following tasks (with more configuration on SAMI HSRP). • Insert both SAMI and configure them in redundant mode and add them into SLB server with in-service mode. • Put MWAM out of service on the SLB server farm. • Wait for all MS connections on the MWAM to complete. • Shutdown the MWAM and remove it.

Table 2-3 Migration Steps that Correspond to Migration Scenarios from Table 2-2 (continued)

Scenario	Migration Steps
6	• Upgrade chassis #1 from SUP720 SXF to SUP720 SRB. • Configure chassis #1 to support the SAMI blade. – Ensure that the MWAM configurations are saved on SUP720 bootflash. – Configure the VLAN for the SAMI VLAN groups on SUP720 the same as the MWAM. – Make SAMI PPC configuration from MWAM processors configurations according to SAMI configuration file name convention in SUP720 bootflash – Power down the MWAM in chassis#1 and pull it out – Insert SAMI in the same slot and boot it with the proper HA R4.0 image – MWAM HA has 5 IOS running so 5 configurations while SAMI has 6 PPC; this implies that either one PPC on SAMI is unused or it needs to be configured alone. – Verify SAMI PPC gets the proper configurations – The HA binding synchronization and stateful redundancy faces the same situation as in Scenario#3. If HA redundancy does not work across the releases, perform the following tasks (SAMI HSRP configuration needs to be changed): • Add the SAMI Home Agent in chassis #1 into SLB server with in-service mode • Put MWAM in chassis #2 out of service on the SLB server farm • Wait for all MS connections on MWAM to expire, then repeat the second bullet in chassis #2.

Caveats and Restrictions for SAMI Migration

- HA stateful redundancy may not work across different releases. For example, the binding information in the R3.0 release is the same as R4.0 even if only R3.0 based features are configured on R4.0 release.
- The underneath HSRP implementation may be not the same across different releases.
- Even with the same platform, different releases may have different system behaviors for the same situation. This implies that extra configuration is required in order to have the same consistent behaviors.
- Without thorough testing, these procedures are not suggested
- The MWAM platform is supported by SUP IOS SRB release.

Required Base Configuration

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 SAMI, the HA will see the access to one GE port that will connect to Catalyst 7600 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 7600 chassis, the same VLAN can be used for all of them.

The following sections illustrate the required base configuration for the Cisco Mobile Wireless Home Agent:

Basic IOS Configuration on Supervisor for SAMI Module

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

	Command	Purpose
Step 1	`sup-7602(config)#vlan 3`	Add an Ethernet VLAN. Enters vlan configuration submode.
Step 2	`sup-7602(config-vlan)#exit`	Updates the VLAN database, propagates it throughout the administrative domain, and return to privileged EXEC mode.
Step 3	`sup-7602(config)#interface vlan 3`	
Step 4	`sup-7602(config-if)# ip address 3.3.3.25 255.255.255.0`	
Step 5	`sup-7602(config)#vlan 30`	
Step 6	`sup-7602(config-vlan)#exit`	
Step 7	`sup-7602(config)#interface vlan 30`	
Step 8	`sup-7602(config-if)# ip address 30.0.0.25 255.0.0.0`	
Step 9	`sup-7602#svclc vlan-group 1 3`	
Step 10	`sup-7602#svclc vlan-group 2 30`	
Step 11	`sup-7602#svclc module 8 vlan-group 1,2`	

For information on SAMI configuration details, please go to the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps5510/products_installation_and_configuration_guide_book09186a0080875d19.html

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

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
Step 1	`Router(config)# aaa new model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 1	`Router(config)# aaa authentication ppp default group radius`	Enables authentication of PPP users using RADIUS.
Step 2	`Router(config)# aaa authorization network default group radius`	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*.

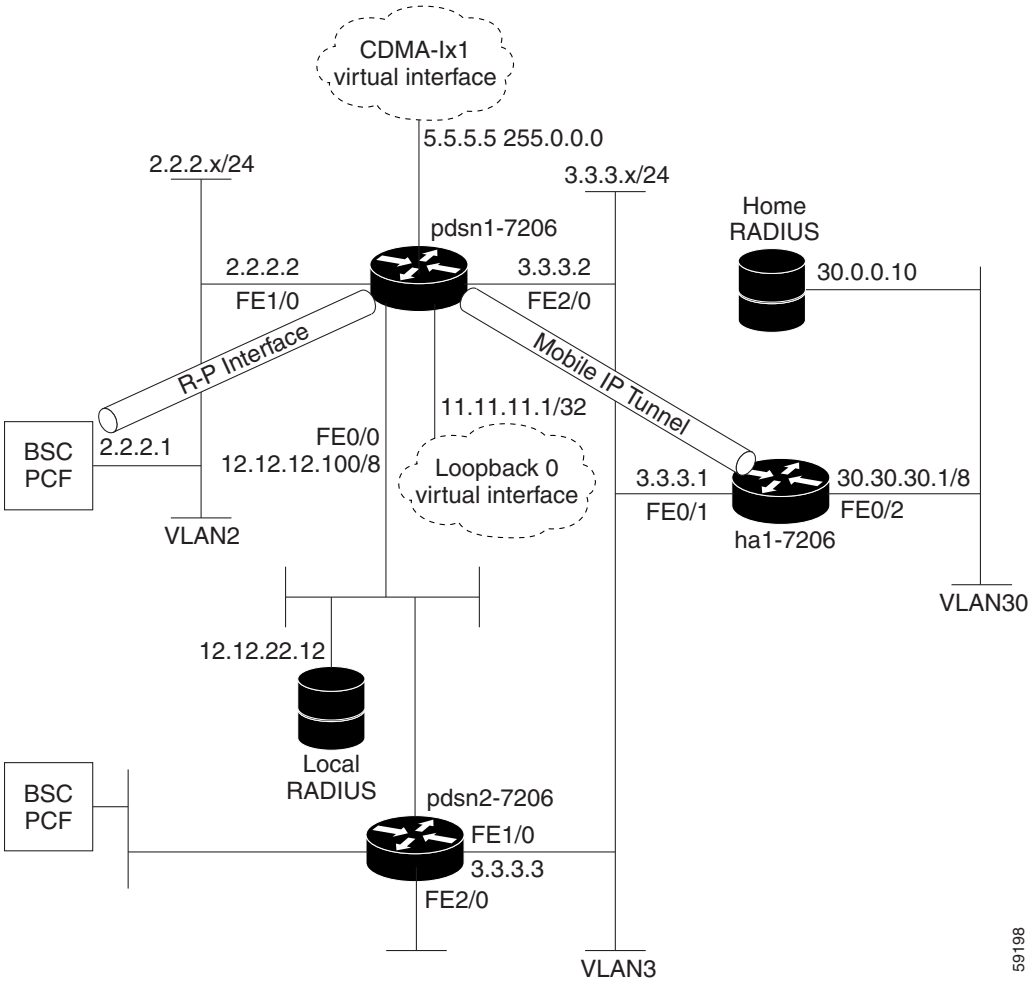
To configure RADIUS in the HA environment, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host ip-addr key sharedsecret`	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.

Configuration Examples

Figure 1 and the information that follows is an example of the placement of a Cisco HA and it's configuration.

Figure 1 Home Agent —A Network Map



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 ha1
!
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
!
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 GigabitEthernet0/0.3
description To FA/PDSN
encapsulation dot1Q 3
ip address 3.3.3.1 255.255.255.0
!
interface GigabitEthernet0/0.30
description To AAA
encapsulation dot1Q 30
ip address 30.30.30.1 255.255.255.0
!
router mobile
!
ip local pool ha-pool1 10.35.35.1 35.35.35.254
ip mobile home-agent broadcast
ip mobile virtual-network 10.35.35.0 255.255.255.0
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 10.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 30.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!

line con 0
exec-timeout 0 0
login authentication CONSOLE
```

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.

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.

Supported Standards, MIBs, and RFCs

RFCs

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following RFCs:

- IPv4 Mobility, RFC 2002
- IP Encapsulation within IP, RFC 2003
- Applicability Statement for IP Mobility Support, RFC 2005
- The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006
- Reverse Tunneling for Mobile IP, RFC 3024
- Mobile IPv4 Challenge/Response Extensions, RFC 3012
- Mobile NAI Extension, RFC 2794
- Generic Routing Encapsulation, RFC 1701
- GRE Key and Sequence Number Extensions, RFC 2890
- IP Mobility Support for IPv4, RFC 3220, Section 3.2 Authentication
- The Network Access Identifier, RFC 2486, January 1999.
- An Ethernet Address Resolution Protocol, RFC 826, November 1982
- The Internet Key Exchange (IKE), RFC 2409, November 1998.
- Cisco Hot Standby Routing Protocol (HSRP), RFC 2281, March 1998

Standards

Cisco IOS Mobile Wireless Home Agent Release 4.0 supports the following standards:

- TIA/EIA/IS-835-B, TIA/EIA/IS-835-C and TIA/EIA/IS-835-D

MIBs

Cisco IOS Mobile Wireless Home Agent Release 4.0 supports the following MIBs:

- CISCO- MOBILE-IP-MIB—provides enhanced management capabilities.
- Radius MIB—as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999.

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The HA supports the MIB defined in The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.

A full list of MIBs that are supported on the Cisco 7600 platform can be found on the Cisco web at the following URL:

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

Session counters maintained in the MIB cannot be reset using SNMP or CLI. The Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

Following additional counters will be supported in Release 3.0 MIB:

- Number of Bindings for FA/CoA
- Number of registration requests received per FA/CoA
- Failure counters per FA/CoA—HA R2.0 supports global failure counters. A per-FA/CoA counter will be added for each of those counters

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 3

Single IP Infrastructure

This chapter discusses concepts related to Single IP Infrastucture and Manageability requirements for the Service Provider Home Agent application. This application is resident on the SAMI service blade of the Cisco 7600 Switch and is part of the Msef product family. This chapter also provides details about how to configure this feature.

This chapter includes the following sections:

Overview of Single IP Feature

The current mSEF gateway-on-SAMI solutions, (Cisco Mobile Wireless Home Agent, WiMax BWG, Cisco GGSN, and PDSN) all offer a multiple-routers-on-a-stick model with the attendant manageability and operational issues. The system design for Home Agent Single IP allows you to manage the gateway-on-SAMI on a per-blade basis. This results in a "factor-of-6 decrease" in operational complexity compared to the previous presentation of six individual processors per blade.

The Single IP feature reapportions functionality on a SAMI service blade from the current model of six independent IOS processors, each executing both control and traffic plane functions, to a model where one IOS processor is designated as a Control Plane (CP) processor and the other 5 designated as Traffic Plane (TP) processors.

Here is an additional targeted subset of functionality that is presented in a per-chassis model. The presentation of a per-blade model applies to the following areas:

- Access Network Protocol
- Authentication/Authorization interactions
- Network Management interaction through SNMP for MIB retrieval
- Retrieval of "load parameters", through SNMP, as a basis for per-subscriber dynamic gateway assignment
- Configuration, Show and Debug functionality
- Failure detection and failover of a blade
- AAA server response time determinations and alarm indications

Additionally, the presentation of a per-chassis model applies to the following targeted functionality:

- Show subscribers present across a chassis with various output filtering capabilities.
- Display the session activity for one or more subscribers across a chassis.
- Monitor Subscriber (Call Trace) for one or more specific subscribers for the purposes of troubleshooting.
- Collation, transfer and storage of bulk statistics for a chassis.

The Home Agent feature behavior as perceived by external systems does not change. The Single IP Home Agent on a blade will look and feel the same as one Home Agent 4.0 image executing on a single processor.

Single IP Interface

The following features fall under the umbrella of Single IP per blade:

- Single Interface for MIP
- Single Interface for Configuration
- Single Interface for SNMP Management
- Single Interface for Trouble Shooting and Debug
- Single Interface for AAA
  - Single Interface for MIP and AAA
- Single Interface for Failover

Single Interface for MIP

The service blade presents a distinct IP address that is the Home Agent IP address. This address is configured the same as in Home Agent Release 4.0. This same IP address is also the endpoint address for the tunnel between the Home Agent and the Care-of-Address (CoA), whether that is a Foreign Agent CoA, or a Collocated CoA. This IP address configuration is present on both control plane and traffic plane processors. This allows configuration of one Mobile IP security association per blade for each of MN-HA and FA-HA, instead of the current six.

The Home Agent IP address should be the loopback address, and this same IP address is also the endpoint address for the tunnel between the Home Agent and the Care-of-Address (CoA)

The service blade implements a packet distribution function in IXP ucode that ensures that user traffic packets are dispatched to the correct traffic plane processor. Packets identified as control plane traffic are sent to the control plane processor. Packets that do not match a specific identification are sent to the control plane processor for treatment.

Single Interface for Configuration

The service blade provides a single point of configuration for blade functionality. This means that you can establish a session to the service blade, the same as performed in Home Agent Release 4.0. The session is established to the control processor on the service blade. From that single session to the service blade, it is possible to configure the Home Agent features with a single execution of each command required for a feature. That configuration is then propagated to all processors that require the same configuration without you having to perform any additional configuration tasks.

The default treatment for any IOS configuration command is that the configuration takes effect on all IOS processors on the service blade. It is possible to define a set of commands that will only execute on the processor hosting the configuration session. Some examples of filtered configuration commands are those relating to OSPF and HSRP.

Single Interface for SNMP Management

The service blade provides a distinct configurable IP address that is the target address for SNMP operations. This IP address is hosted on the control plane processor. All MIBs on a service blade related to Home Agent functionality are accessible through this IP address. Information required from processors other than the control plane processor is either Pushed or Pulled depending on the MIB target.

There are two MIBs related to processor resource usage and memory usage that present information on a per-processor basis. There will be a single Processor Resource MIB result returned with six individual entries, one per processor. Similarly, this also occurs for memory usage.

Single Interface for Trouble Shooting and Debug

The service blade provides a single point of entry (session into the control plane processor) to execute **show** and **debug** commands. By default, **show** commands are executed on the Control Plane processor only. Each command that requires execution on 1 or more traffic plane processors is individually instrumented.

For commands that require additional information from the traffic plane processor, and are qualified per user (either NAI or IP address), the traffic plane processor hosting that user is identified and the command executed on that specific processor.

The results from the various processors are combined into a single presentation before a response to the command is provided.

Conditional debug commands use a similar approach. To support the chassis-wide “Debug a Subscriber” feature, it is necessary to preset a trigger for the identified subscriber before a Mobile IP binding registration request is received for that subscriber. Once the registration request is received, the preset trigger can be removed for all processors except the one where the request was received.

Single Interface for AAA

The service blade presents a single IP address for AAA interactions. This may be one IP address for both Radius-based and Diameter-based interactions, or separate IP address configurations for each protocol.

Radius-based Authentication and Authorization is executed solely from the Control Plane processor.

Radius-based Change of Authorization and Packet of Disconnect exchanges occur with the Control Plane which then triggers the execution of the resulting action on the relevant Traffic Processor. These functions are provided independent of support for Radius-based accounting.

Diameter-based interactions for policy support also execute solely on the Control Plane processor. This is supported as part of the Home Agent 5.0 release.

Radius-based and/or Diameter-based accounting is not supported in this release of Single IP for Home Agent. The service blade packet distribution function does provide for directing of Radius traffic to a specific processor based on the destination UDP port.

Single Interface for MIP and AAA

For the Single IP-based Home Agent, the CP terminates the interface towards AAA servers. For all subscribers, the Authentication is performed by the CP. Note that only Authentication is performed.

To update the information from active/standby CP to the TP, the CP uses the IPC mechanism. The CP waits on process for some control messages while updating to the TP. The following sections contain the specific approach for each control plane messaging case.

Procedures on Active HA

The following control messages are handled by CP of the active Home Agent.

- Registration Request (RRQ) -Registration, Re-Registration and De-Registration of subscriber
- Registration Revocation messages
- Registration Revocation Acknowledgement Messages
- Change of Authorization(COA)
- Packet of Disconnect (POD)

Registration Request of MN on Active-HA CP

1. The CP on the active-HA receives RRQ and the CP performs Authorization for the MN. The interface between the CP and AAA servers remains same as HA4.0.
2. If the authorization failed for the MN, the CP sends a Registration Reply with Error Code to FA.
3. On successful authorization, an IP address assignment is made for the binding. The mechanisms for IP address assignment are the same as for Home Agent 4.0. The CP looks at the Hash Table to get one TP ID based on the assigned MN address.
4. The CP updates binding information to the corresponding TP using an IPC reliable mechanism without waiting for response. And, it will send update information to standby-HA CP over UDP/IP and respond to FA with a Registration Reply.
5. If an acknowledgment is received by the CP without error code from the TP, the CP does not take any action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding and as well initiate “binddeleterequest” to the standby-HA and sends a Registration Revocation Message to the FA if revocation is enabled on the HA.

The following information is updated from CP to TP for binding:

- RRQ Header - Is based on RFC 3344.
- SPI of MHAE as an extension
- NAI extension
- Multipath NVSE
- Address Type CVSE - Indicates DHCP Address allocation for MN
- MR dynamic Network NVSE
- Static/Dynamic pool name
- Class attribute—if received, this is only for Accounting purposes
- CUI—if received, this is only for Accounting purpose and wimax subscribers
- Accounting multi session ID, accounting interim interval - for Wimax subscribers.

- VRF name and corresponding HA IP address, if present.
- In and Out Acl Names
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rule/profile based as NVSEs.

De-Registration of MN on Active-HA

The following call flow describes the de-registration of a MN on the active HA:

1. The CP on the active-HA receives a RRQ for De-Registration and the CP does Authorization for the MN. The interface between the CP and AAA servers is the same as HA Release 4.0 functionality.
2. If the authorization fails for the MN, the CP send a Registration Reply with Error Code to FA.
3. On successful authorization, the CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During De-Registration the CP does not wait for the response from the TP.
4. The CP sends a Registration Reply with MN address and error code as **0**.
5. The CP on the active-HA sends a binding delete request to its peer.

The following information is updated from the CP to the TP for binding,

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

Registration Revocation Message on Active-HA

The following call flow identifies the procedure for Registration Revocation on the active HA:

1. The CP on the active-HA receives a Registration Revocation Message. The CP sends a Registration Revocation ACK with error code to the FA, if any parsing failure or authentication failure with FHAE.
2. The CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During Delete Request, the CP does not wait for the response from TP.
3. The CP on the active-HA sends a binding delete request to it's peer.
4. The CP delete binding information for the MN.
5. The CP sends a Registration Revocation Ack with MN address and error code as **0.**

The following information is updated from the CP to the TP for binding:

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

Registration Revocation Acknowledgement on Active-HA

The CP on the active-HA receives a Registration Revocation ACK for corresponding Registration Revocation Message that is sent by the active-HA. The CP does not take any action to update the TP for updating binding information, but it does complete FHAE or IPSec Authentication.

COA Received on Active-HA

The following call flow highlights the procedure for COAs received on the active HA:

1. The CP on the active-HA receives a COA and the CP does authorization for the MN. The interface between the CP and AAA servers is identical to that of Home Agent Release 4.0.
2. If the authorization fails for the MN, the CP sends COA NAK Error Code to the AAA Server.
3. The CP sends COA NAK if any failure occurs while parsing hotline information to the AAA Server. The CP does not update any information to the TP, or to the standby-HA.
4. The CP sends interim update information to the corresponding TP using IPC reliable mechanism without waiting for response. It also sends interim update information to the standby-HA CP over UDP/IP, and respond to AAA with COA Ack.
5. If acknowledgment is received by the CP without an error code from the TP, the CP does not take any further action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding and initiates a “binddeleterequest” to the standby-HA. A Registration Revocation Message is sent to the FA if revocation is enabled on HA.

The following information is updated from the CP to the TP for binding,

- MN Address
- HA IP Address
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rules/profiles as NVSEs.

POD Received on Active-HA

The following call flow identifies the procedure when POD is received on an active HA:

1. The CP on the active-HA receives a POD and CP does authorization for the MN. The interface between the CP and AAA servers is identical to that of Home Agent 4.0.
2. If the suthorization fails for the MN, the CP sends a POD NAK Error Code to the AAA Server.
3. The CP constructs a Registration Revocation Message for the MN Address and sends it to the corresponding care-of-address.
4. The CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During Delete Request, the CP does not wait for the response from the TP.
5. The CP on the active-HA sends a binding delete request to its peer.
6. The CP deletes the binding information for the MN.
7. The CP waits to receive a Registration Revocation Ack with MN address and error code as **0**. If a timeout occurs before getting a response, the HA re-tries with a Registration Revocation to the PDSN.

Procedures on Standby Home Agent

The CP on the standby Home Agent will update Traffic Processors in two cases of active/standby synchronization.

- Dynamic Sync
- Bulk Sync

Bind UpdateRequest received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standy-HA will handle a “BindUpdate Request” from the active-HA for Registration/Re-Registration of MN.

1. The standby-CP receives “BindUpdateRequest” from the active-CP, and the standby-CP does authorization for the MN. This validates the received “BindUpdateRequest”.
2. If the HHAE authentication failed between the active/standby-HA, the standby CP sends a “BindUpdate Ack” with finite error code.
3. On successful authorization, the CP creates binding on received Home-Address. And the CP looks at the hash table to get the one TP ID based on the assigned MN address.
4. The CP updates binding information to the corresponding TP using IPC reliable mechanism without waiting for response. It acknowledges the active-HA with “bindudpate ack”.
5. If acknowledgment is received by the CP without error code from the TP, the CP does not take any action.
6. If failure happens due to timeout or received invalid response from the TP, the CP deletes the binding on the standby-HA. The binding deletion on standy-HA should not interfere with the active-HA binding information.

The following information shall be updated from the CP to the TP for binding,

- RRQ Header - Is based on RFC 3344.
- SPI of MHAE as an extension
- NAI extension
- Multipath NVSE
- Revocation Support Extension,
- Address Type CVSE - It will indicate DHCP Address allocation for MN
- MR dynamic Network NVSE
- Static/Dynamic pool name
- Class attribute - if received, this is only for Accounting purpose
- CUI - if received, this is only for Accounting purpose and wimax subscribers
- Accounting multi session id, accounting interim interval - for wimax subscribers.
- VRF name and corresponding HA IP address, if present.
- In and Out Acl Names
- Hotline basic Information
- Hotline accounting Indication
- List of Hotline rule/profile based as NVSEs.

BindDeleteRequest received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standby-HA handles a “BindDelete Request” from the active-HA after receivinga De-Registration/Revocation Request/POD for MN.

1. The standby-CP receives a “BindDeleteRequest” from the active-CP, and the standby-CP does authorization for the MN.
2. If the HHAE authentication fails between the active/standby HA, the standby CP sends a “BindDelete Ack” with finite error code.

3. On successful authorization, the CP sends binding information to the corresponding TP using IPC reliable mechanism to delete the binding. During the Delete Request, the CP does not wait for the response from the TP.
4. The CP sends “BindDelete Ack” with MN address and error code of **0** to the active-HA.

The following information is updated from the CP to the TP for binding:

- Message Type and Error Code
- MN Home-Address
- Home-Agent Address
- Care-of-Address

BindInterimUpdate received by CP on Standby-HA during Dynamic-Sync

The following call flow describes how the standby CP handles a “BindInterimUpdate” message during dynamic-sync:

1. The standby-CP receives “InterimUpdateRequest” from the active-CP, and the standby-CP performs authorization for the MN.
2. If the HHAE authentication fails between the active/standby-HA, the standby-CP sends “InterimUpdateAck” with finite error code.
3. On successful authorization, the CP updates the Interim Update information with hot-lining rules to a binding that was already created on the CP.
4. The CP updates the binding information to the corresponding TP using IPC reliable mechanism without waiting for response. It acknowledges the active-HA with a “interimupdate Ack” with error code of **0**.
5. If acknowledgment is received by the CP without an error code from the TP, the CP does not take any action.
6. If failure occurs due to a timeout or it receives invalid response from the TP, the CP deletes the binding on the standby-HA. The binding deletion on the standy-HA should not interfere with active-HA binding information.

The following information is updated from the CP to the TP for binding:

- MN Address
- HA IP Address
- Hotline basic Information
- Hotline Accounting Indication
- List of Hotline rules/profiles as NVSEs.

BindUpdateRequest received by CP on Standby-HA during BulkSync

During Bulksync, the active-HA CP sends binding information for multiple bindings to the CP on the standby-HA. After successful creation of each binding on the standby-HA CP, the binding information is updated to the TP through IPC mechanism without waiting for the response.

At any stage, the CP-TP response message status should not interfere with the bulk sync message flow. Once the response is received, the “bindupdaterequest” message treatment is applicable on that binding.

Miscellaneous Cases

During a MIP Session Termination due to Hotline Timer Expire, no update is sent from the CP to the TP on the active/standby HA. The binding information is automatically deleted on the CP/TP of the active/standby HA once the hotline timer expires.

During a MIP Session expire based on Registration Lifetime, the above functionality is also applicable on the binding.

Single Interface for Failover

The current SAMI failure mode is for a per-processor failure whenever possible. For the single IP model, a failure detected on the blade will result in a blade level failover, even if a processor-level failover is sufficient. This includes interface failures in so far as they are detectable by the SAMI platform. This requires platform support for such a failure mode.

Operation and Management

This section discusses features that fall under the umbrella of Operation and Management.

Chassis-Wide MIB for Application Related Parameters

This feature provides a single MIB within which all application related parameters are reported across the chassis. For the Home Agent, this functionality is provided on a per-Home Agent instance basis.

For all Home Agent instances on a single service blade, this information is available through a SNMP Get to a single IP address. The information is available in the CISCO-MOBILE-IP-MIB and in the CISCO-IP-LOCAL-POOL-MIB. The SNMP manager is responsible for executing the necessary number of SNMP GET operations to retrieve a MIB per Home Agent instance. This release of the Single IP Home Agent feature supports one Home Agent instance per service blade, thereby reducing the number of Get operations from 12 per service blade to 2.

Reporting of Chassis-Wide Loading on a Per Application Instance Basis

Service Provider networks typically use AAA capabilities to dynamically assign a Home Agent for a subscriber at the time of subscriber network entry. The criteria for Home Agent selection varies by Service Provider. Service Providers want proof of the loading of each Home Agent instance configured in a chassis, not the chassis as a whole. This loading is based on IP address pool usage within that Home Agent instance.

This information is contained in the CISCO-IP-LOCAL-POOL-MIB. This information allows Home Agent instance selection based solely on IP address pool usage. The MIB contains statistics of InUse addresses and Free Addresses on both a per-pool and a per-pool group basis. The AAA server is responsible to use this information per-IP pool and pool-group configured at the Home Agent instance.

In addition, the SNMP traps triggered on pool usage threshold crossing are sent to the same SNMP host that retrieves the CISCO-IP-LOCAL-POOL-MIB.

Trap Generation for AAA Unresponsiveness

This feature allows the HA to send a new SNMP trap/notification to the NMS server when the HA is authenticating MNs, and notices that the AAA is unresponsive. The trap is added when a timeout occurs. It is now possible to set a threshold (defined as a percentage of the maximum response time) on round trip delay, and generate a trap when that threshold is exceeded. An additional trap is generated when the round-trip delay falls below a second threshold.

For each RADIUS server, you can configure the threshold percentage values (*normal* or *high*). When the round-trip time of RADIUS messages between the HA and AAA server goes above or below the configured threshold values, a notification is sent to the NMS server indicating AAA server un/responsiveness. Similarly, when the number of RADIUS retransmit messages goes above or below the configured threshold values, an SNMP trap/message is sent to the NMS server indicating AAA server un/responsiveness.

The RADIUS-CLIENT-AUTHENTICATION-MIB contains entries for timeout on AAA access. The trap is added in the CISCO-RADIUS-MIB.

To enable this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# radius-server snmp-trap timeout-threshold normal high`	Enables you to generate SNMP traps that denote AAA unresponsiveness. *normal* is the normal threshold in percentage, used to generate traps. *high* is the high threshold in percentage, used to generate traps.
Step 2	`Router(config)# radius-server snmp-trap retrans-threshold normal high`	When this command is configured, a trap (SNMP notification) is generated when round trip time or retransmit value goes above the high threshold value and comes below the normal threshold value. The trap is generated for either round trip time or retransmits time. *normal* is the normal threshold in percentage, used to generate traps. *high* is the high threshold in percentage, used to generate traps.

Note This feature is only supported only on the Cisco SAMI card on the 7600.

The RADIUS-CLIENT-AUTHENTICATION-MIB contains entries for timeout on AAA access. A trap is added based on this timeout occurring. It is also possible to set a threshold on round trip delay (defined as a percentage of the maximum response time), and generate a trap when that threshold is exceeded. An additional trap is generated when the round-trip delay falls below a second threshold. This provides a level of delay for trap generation.

Show Subscriber

This feature provides—from a single point in the chassis—summary listings of subscribers hosted by the Home Agent instances in the chassis. The Home Agent 5.0 Release supports a single Home Agent instance per service blade, so the sequence of steps necessary is limited to requesting the desired information using IOS CLI commands for one, or all, service blades.

The HA Named Service corresponds to the name configured using the IOS **hostname** command for the Home Agent instance on the service blade.

Table 3-1 lists the feature's functionality:

Table 3-1 List of Show Subscriber Functionality

All	Summary of all users on the chassis	To display the total of all registered users on the chassis, use the **show ip mobile binding summary** command on the control processor once per active service blade. The total from each blade is then summed, and the result displayed at the supervisor where the capability was initiated. There is a maximum number of subscribers that can be displayed for a single command. We recommend a value of 1000. If the number of registered subscribers is greater than that, the output is saved to a file, and the name and location of the file is indicated to the user.
Card	Summary of all users on one specific Card/Slot	To display the total of all registered users on one service blade, use the **show ip mobile binding summary** command on the control processor of the service blade identified with the desired result being the **total** line
CPU	Summary of all users on one specific CPU	To display the total of all registered users on a given traffic processor on a service blade, use the **show ip mobile binding summary** command on the service blade, plus the TP identified in the command.
Lifetime	Summary of all users with MIP Lifetime >, <, = to a value	This option filters the output by Granted Registration Lifetime. The raw output is generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
LifetimeRem	Summary of all users with MIP Lifetime Remaining >, <, = to a value	This option filters the output by Remaining Registration Lifetime. The raw output is generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
Connect	Summary of all users with A Connect Time >, <, = to a time value	This option displays the time since the subscriber first registered, not the time since the last re-registration

Table 3-1 List of Show Subscriber Functionality (continued)

FA	Summary of all users from a specific FA IP address	This option filters the output by Foreign Agent IP address. The raw output can be generated using the **show ip mobile binding** command. This can be executed for All, Card or CPU.
HA	Summary of all users from a specific HA IP address	Use this option to determine the Home Agent instance corresponding to the Home Agent IP address, and then configure the **show ip mobile binding** command on the control plane processor of that Home Agent.
HA-Name	Summary of all users from a specific HA Named Service	Use this option to determine the Home Agent instance corresponding to the Home Agent Name, and then configure the **show ip mobile binding** command on the control plane processor of that Home Agent. The Home Agent name is defined by the **hostname** command in the service blade configuration.
Pool	Summary of all users from a specific Pool Name or Pool Group	The raw output for this command is provided by the **show ip local pool** command which will provide the ip address range(s) of those pools. Based on this, the relevant information can be retrieved using the show ip mobile binding and show ip mobile host commands.
CallType	Summary of all users for this Call Type (could be something like MIP, WiMax, 3G, PDIF, etc)	This is filtering by Access-Type. The raw output can be generated using **show ip mobile binding**. The access type supported by a Foreign Agent is determined by the **show ip mobile** command. This can be executed for All, Card or CPU.
NAI/User	Summary of all users for this NAI (must support wildcards in the NAI). Example “show user summary nai *ptt*” for finding Push to Talk users on the box.	This is filtering by wild-carded NAI. Native IOS CLIs do not support such a wild-carding concept. The raw output can be generated using ‘show ip mobile binding’. This can be executed for All, Card or CPU.
ACL-IN	Summary of all users that were assigned this Input ACL	This is filtering by Input ACL. The raw output can be generated using **show ip mobile binding**. This can be executed for All, Card or CPU.
ACL-OUT	Summary of all users that were assigned this Input ACL	This is filtering by Output ACL. The raw output can be generated using **show ip mobile binding**. This can be executed for All, Card or CPU.

Here is a list of the possible output display formats:

- Summary - Totals without reporting per user information
- Summary Traffic - adds traffic totals, Bytes In/Out, Packet In/Out, Dropped In, Dropped Out by ACL, provided by show ip mobile host command.
- Brief - Single line of output per user matching the command filters. The output comprises the assigned IP address, NAI, Home Agent IP address, Foreign Agent IP address, Remaining Registration Lifetime
- Brief Traffic - As for 3 above plus the traffic totals, Bytes In/Out, Packet In/Out, Dropped In, Dropped Out by ACL, from the show ip mobile host command.
- Verbose - Full display as provided by the combined outputs of the show ip mobile binding and show ip mobile host commands
- Verbose MIP - Full display as provided by the output of the show ip mobile binding command

The output of the **summary** command gives you a count of the number users that match the query option. It also tallies of Bytes In/Out, Packet In/Out, Dropped in.Out by ACL etc.

This feature is supported under the umbrella of OSLER for Home Agent. Please refer to the OSLER section of this chapter for more information.

This functionality is not supported through SNMP.

Intra-Chassis Configuration Synchronization

This feature provides that any configuration command executed on the active blade will automatically be synchronized on the partner standby blade. This applies to all commands except those used to configure the active/standby partnering model (**ip mobile home-agent redundancy**), and those for configuring HSRP (**standby**) as a failure detection mode for redundancy.

Note It is not possible to execute configuration commands on the standby Home Agent. EXEC commands are permitted.

How an active or standby HA is determined is based on the RF infrastructure used for SSO support, as well as for Session Redundancy support for various mSEF gateways.

Initialization

The SSO configuration synchronization happens automatically during bootup without any pre-required configurations. The same cannot be applied to the Home Agent as IP connectivity between the redundant units is required prior to RF negotiation, so different yet related configurations are necessary for the Active and Standby blades.

Additionally, the SSO configuration sync feature does not support any unique configuration on each of the redundant units. On the Home Agent, HSRP and RF Interdev protocols are required, both of which require certain unique configurations on the redundant units.

The existing commands that require unique configurations for each unit are modified to accommodate configurations for the peer unit in that same command. A new command identifies the peer slots. These commands are parsed and the RF negotiation state RF_PROG_STANDBY_CONFIG is used to trigger configuration sync automatically.

RF Client

As in the case of SSO configuration sync, the Home Agent configuration sync is also an RF client. The configuration sync feature registers a callback with RF for the progression events and status events. The RF notifies each of these registered clients in order with the progression of events and any status events. This allows the HA to know when to sync the configuration files.

Configuration Files and Synchronization

Here is a brief explanation of the startup configuration and running configuration process that comprises the configuration synchronization feature.

The startup configuration is stored in NVRAM as a text file. This file is synced whenever you perform operations such as “write memory”, “copy running startup”, etc. If the file is opened for a write operation, when it is closed the sync is initiated.

A running configuration sync is dynamically generated by certain operations, so any time the sync is performed the running configuration must be generated.

In the SSO implementation, before the sync process begins, the primary is locked. A bulk sync of the startup configuration and the running configuration is performed. After that is completed, the parser mode sync is done.

After both the processors are in sync and the primary is unlocked, the line-by-line sync begins.

All of the above syncing processes require a transport mechanism to communicate between the redundant units, and currently each of the platforms uses either IPC or some other transport mechanisms.

The Home Agent configuration sync feature could use one the following transport mechanisms:

- Reliable IPC mechanism currently being used for CP-TP messaging
- RF/CF SCTP-based approach for IPC messaging
- New SCTP-based approach for IPC messaging

The first is the fastest solution from an implementation perspective but it does not scale well for an Inter-chassis solution. Currently we use the second option, RF/CF SCTP.

Startup Configuration Sync

In the SSO implementation the Startup config is synced during bootup right when the RF state is ready to perform bulk sync. You must lock the router prior to initiating the startup config sync. The same design is adopted for the Single IP Home Agent configuration sync feature.

When a **write memory** or **copy** *file1* **startup-config** is executed there are two ways to hande the scenario:

- Bulk sync the startup configuration file.
- Perform a line-by-line sync of the EXEC command.

The second option is used for the SSO feature, but for the Single IP Home Agent the first option is used because it allows the active unit to save configuration changes to the standby location.

Running Configuration Sync

With a running configuration sync, the redundancy units carry the same state of information.

Initially, after the secondary unit establishes RF Interdev communication, the running config file is bulk synchronized. The bulk sync will induce a self-reload of the standby unit if the running configuration has changed on the active unit prior to its bootup. After the reload, the standby will come up with the running config of the active unit.

After this the line-by-line sync occurs between the two units. As you configure each command, the same command is passed on to the secondary side after executing the same on the primary.

The bulk sync of the running configuration is done using the RCSF in the SSO implementation, and the same is done (using the RF Interdev SCTP) for the Single IP Home Agent feature.

Bulk Sync

RF Interdev communication needs to be established between the two units prior to initiating the bulk sync. Each unit will parse it's startup configuration and this will cause the unit to become active / standby. The active unit will then bulk sync its running and private configuration files to the standby if there has been running/private config modifications on it post bootup. After the bulk sync, the standby will reload itself and come up with the altered configs. During this standby reload phase, no configurations are allowed on the active unit.

The configurations that are synced during initialization include:

- Private configuration
- Running configuration

The startup configuration is not synced because the startup config files in the SUP are always in sync.

If a private configuration is changed after bootup, the active unit copies its private configuration file into a buffer and transports the same using RF Interdev SCTP to the standby

If running configs change after bootup, the active unit copies its running config file into a buffer and transports it using RF Interdev SCTP to the standby end

After both the previous steps are complete, the active sends a message to the standby to commence parsing the received buffers

The standby unit save the received buffer contents locally, and reloads itself so as to apply the modified to itself.

Line by Line Sync

When both active and standby units are up and running, the commands entered from the active unit are executed first, the same command is propagated to the standby and executed, and returns the result back to active.

The Parser Return Code (PRC) scheme is used in the SSO implementation to have all the parser action routine for each command set the return code. This return code is a combined form of all information including the class of the error code, component ID, sync-bit, sub-code, etc.

Parser Mode Synchronization is an effort to maintain the same parser mode between the active and standby units before a command is sent to the standby for synchronization.

In the SSO implementation syncing process is done through RPC, which is blocking the current process until active RP receives return code message from standby RP. Thus, the commands are executed in order for both units.

If a command fails on standby unit, then the result is conveyed back to active. On the active, a stub registry for policy maker is invoked, and leaves the decision on what to do with the returned result to the calling/upper layer.

The Single IP Home Agent configuration sync feature will use the SSO line by line sync implementation as is.

Configuration Details

Since configurations must be synced as is, the CLIs on both the units should be the same. The following commands are currently unique to each redundant unit, and have been modified:

- **ipc zone default**
- **association** *no*>
- **protocol sctp**
- **unit1-port** *port1*
- **unit1-ip** *ip1*
- **unit2-port** *port2*
- **unit2-ip** *ip2*

The following new CLIs are introduced:

```
interface GigabitEthernet0/0.23
redundancy ip address unit1 <ip1> <mask1> unit2 <ip2> <mask2>
```

The **redundancy ip address** command CLI is a per-interface CLI. The HSRP protocol uses this IP address configured for its negotiation, and not the one configured using the regular **ip address** command. The **ip address** configuration is not required for a sub-interface which is dedicated for HSRP negotiation with the peer.

```
redundancy unit1 slot <x> unit2 slot <y>
```

This is a global configuration and is used for identifying the peer slot.

Use the following commands to configure Intra-chassis Configuration Synchronization:

router(config)# **redundancy unit1 slot** <x> **unit2** slot *y*

router#(ipc-assoc-protocol-sctp)#**unit1-port** *portnum* , **unit2-port** *portnum*

router(config)#**unit1-ip** *address1* , **unit2**-ip *address2* -- under the ipc-unit1-port and ipc-unit2-port modes respectively

redundancy ip address unit1 *address1 mask1* unit2 *address2 mask2* -- Under the interface and sub-interface modes.

Here is the sequence of configuration steps, and must be performed on each of the cards.

	Command	Purpose
Step 1	`Router#show redundancy states`	Execute the following commands on both SAMIs before running any redundancy commands. **my state** should be active on both the cards.
Step 1	`Router(config)# redundancy inter-device`	Enables intra-chassis configuration synchronization.
	`redundancy unit1 slot 9 unit2 slot 6`	Configures global redundancy unit-slot mapping.

	`interface GigabitEthernet0/2`
	`encapsulation dot1Q 20`
	`redundancy ip address unit1 4.0.0.1 255.255.255.0`
	`unit2 4.0.0.2 255.255.255.0`
	`standby 0 ip 4.0.0.4`
	`standby 0 name hsrp`
		Configures an interface for HSRP.
		HSRP needs unique IPs for the standby and active units and you need to use the **redundancy ip address** command.
		Note Do not configure the **ip address** command on this interface.

Step 2	`Router(donfig)# redundancy unit1` *hostname name 1* `unit2` *hostname name2*	Used to identify and configure the peer slot in the same chassis.
Step 3	`Router(config)# redundancy inter-device scheme standby hsrp`	Associates the HSRP scheme name to the RF Interdevice.

	`ipc zone default`
	`association 1`
	`no shutdown`
	`protocol sctp`
	`unit2-port 5000`
	`unit2-ip 4.0.0.2`
	`unit1-port 5000`
	`unit1-ip 4.0.0.1`
		Configures ipc information for the RF Interdevice.

After you execute the above configuration, save the configs and reload one of the cards (standby is preferred). Once they come up they will do an HSRP negotiation followed by an RF Interdev negotiation after which the configuration sync feature sets in. The above steps are the same as are needed to get RF Interdev working on a fresh card for the first time.

Monitor Subscriber

This feature allows you from a single point in the chassis to establish conditional debugs based on NAI or assigned IP address. This is possible without knowing which Home Agent instance in the chassis hosts the subscriber session or is selected to host the subscriber session for cases when the session is not yet established. This feature make use of the OSLER tool that allows centralized execution of IOS commands with the ability to receive responses and present those responses in a clear and concise format.

There will be two output formats, **brief**, where the debug output is succinctly presented, and **verbose** which is the full debug output available.

The operator must login to the Supervisor of the 7600, and then execute the command debug condition “qualifier” protocols, or something similar.

A two-stage process will result.

1. Determine the Home Agent instance in the chassis hosting the session.
2. If a session is present, apply the **debug** conditional command on that Home Agent instance and then apply the specific **debug** commands requested. If no session is present, establish a pre-trigger condition for debug followed by the requested **debug** commands on all Home Agent instances configured in the chassis.

It is possible to specify the protocol subsystems for which conditional debugging applies. The choices are all, mobile-ip or aaa (including Radius).

There is a limit of 10 simultaneous monitored subscribers per chassis. But there is no restriction on distribution of those monitored subscribers across blades within a chassis.

Only 1 subscriber can be monitored per monitoring session. To monitor 10 subscribers, you must establishe10 independent monitoring sessions.

The **verbose** output format comprises all debugs generated by IOS for the selected protocols. This is a large amount of information that requires expert analysis to be useful. The **brief** format is a subset of the possible debugs.

There are no changes required to the **debugs** available within the Home Agent IOS code base.

This feature is supported under the umbrella of OSLER for Home Agent. Please refer to the OSLER section for more specific information.

Show Subscriber Session

You “login” to the Supervisor of the 7600 and then execute the **show subscriber session** command where the subscriber is identified by NAI or IP address.

This results in a two step process:

- Determine the Home Agent instance in the chassis hosting the session
- Execute the commands for **show ip mobile host** ***ip-address*** **| nai**, **show ip mobile secure host** *ip-address* **| nai**, **show ip mobile violation address | nai** *string* and **show ip mobile host-counters**.

Bulk Statistics Collection

This feature is capable at a single point, to perform the following functions:

- To initiate the periodic collection of the available Home Agent statistics, identifiable by name, from each active service blade in the chassis.
- To collect the specified statistics by enabling IOS Bulk Statistics collection at each selected service blade. This mechanism allows the collection of statistics for MIB variables. If the required measure is not part of a MIB, it cannot be collected as part of the bulk statistics collection feature.
- To transfer the file to an external TFTP server identified by a URL.

You can set the statistics collection period in 15 minute increments, the minimum collection period being 30 minutes. The maximum collection period is 24 hours.

The file content contains summary statistics for each blade except for the CPU usage and memory occupation information which are available on a per-CPU basis collected per blade. The per-blade file has an entry for each application CPU on that blade.

The file format comprises a sequence of “variable_name value” pairs separated by commas.

In HA Release 5.0, the variable name will be the OID of the variable as this is the level of support available from the IOS Bulk Statistics Collection CLI.

There are a predefined set of statistics that are collected, including the variables available in the MIBs supported by the Home Agent application. The OID assigned to the statistic corresponds directly to the OID in the related MIB.

The following variables of interest are not present in a MIB. These will not be supported as part of the Bulk Statistics Collection feature:

- HARegRevocationsSent
- HARegRevocationsReceived
- HARegRevocationsIgnored
- HARegRevocationAcksSent
- HARegRevocationAcksReceived
- HARegRevocationAcksIgnored

The time-period over which collection is made is indicated in the file in the form of period yy:mm:dd:hh:mm:ss yy:mm:dd:hh:mm:ss. The first date is the start, the second date the end.

If you want to alter the set of subsystems for which statistics collection is enabled, you must first cancel the ongoing statistics collection and initiate and a new collection. Any information that you collect during the cancelled session will be saved.

In the event that the external server is unavailable, the file is saved in local non-volatile memory. The last transferred file is saved locally until the next file is successfully transferred. On successful transfer of the new file, the currently saved file is replaced with the new one.

No new IOS commands are used to support the bulk statistics feature in the Single IP Home Agent Release 5.0.

Conserve Unique IP ID for FA-HA IP-in-IP Tunnel

This feature supports several hundred thousand sessions in the Single IP architecture. This is achieved by setting the unique ID in the IP header only when the packet is likely to fragment. Otherwise, the ID field in the IP header should be set to **0**.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router#`**`ip mobile tunnel ip-ip conserve-ip-id threshold`** *`value`*	Sets a unique IDin the IP header when the packet is likely to fragment. The threshold-value range is *576-1500*, and indicates the outer IP packet size. This feature is only supported for the IP-IP tunnel.

When you configure the **ip mobile tunnel ip-ip conserve ip-id threshold** command, if the packet size is more than the **threshold** *value*, it is sent with a unique IP ID in the outer IP header. Otherwise, the identification field is set to **0**. If you set the threshold to 1400 bytes, then packets with size 1401 and above are sent out with a unique IP ID.

This functionality is not the default behavior, and needs to be enabled through this command. Additionally, there is no default threshold value.

Setting Fragmentation Size of First Packet With Offset=0

This feature allows you to set the first fragment size to avoid further fragmentation of the second fragment in the network. Also, when IP fragmentation happens, the first fragment may not include the L4 header information of the inner packet. This could cause the firewalls on the network that does the deep inspection up to L4, to drop the first fragment.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	Router#**ip fragment first minimum size** *size*	Sets the first fragment size to avoid addtional fragmentation. The range is *8-560* bytes. The size includes only the payload, and does not include any header.

Note The "payload size" must be in multiples of 8 bytes. Otherwise, the command is rejected with the following error: "%% First fragment payload size is not in multiples of 8 bytes"

This is an IP level command, and size configuration considers only the payload of the IP packet.

For example, if you configure the first fragment size as 48 bytes, it creates the first fragment with the size of 68 bytes including the 20 byte IP header.

In case of an IP-IP tunnel packet, the configured payload size includes inner the IP header. For fragmentation code, the inner IP is seen as the payload to the outer IP header.

- The command configuration only indicates the minimum value for the payload of the first fragment. If the existing fragmentation mechanism in CEF selects the first fragment larger than the configured value, then the configuration is not enforced. Otherwise, the BWG will generate more fragments than expected.
- Also, if the configured first fragment size is more than the MTU of the output interface, the configured value is not enforced.

The following examples illustrate how the packet would be for IP and IP-IP tunnel packet:

```
router(config)# ip fragment first minimum size 80
IP Packet:

10:27:59.660 IST Mon Apr 13 2009                Relative Time: 2.990258
Packet 8 of 26                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x0092,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x582D (OK)
      Source: 50.1.1.200,     Dest: 13.2.2.15

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x1A45 ERROR: C661
      Identifier: 006A,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E794 B5A4 ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   20 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   40 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   60 : ABCD ABCD ABCD ABCD ABCD ABCD ............
```

```
IP-IP tunnel packet:
20:39:40.394 IST Sun Apr 12 2009                Relative Time: 2.967188
Packet 7 of 22                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x8008,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 4 (IP-IP),   Checksum: 0xD9F5 (OK)
      Source: 14.0.0.1,     Dest: 50.1.1.150

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 1500,   ID: 0x0086,   Flags-Offset: 0x0000
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x40D0 (OK)
      Source: 50.1.1.200,     Dest: 65.0.0.2

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x72CB ERROR: 7C6A
      Identifier: 005E,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E49E 6020 ABCD ABCD ABCD ABCD ABCD ABCD
```

VSE Support for China Telecom Attributes

In HA Release 5.1 (which is a single IP architecture), the following changes are made as part of this feature support:

- Ensure that syncing of these NVSEs / attributes between the active and standby is working properly with the SR infrastructure introduced in HA 5.0.
- Ensure that syncing these NVSEs between CP and TP is correct.
- Ensure that the interface with accounting is working properly.
- Ensure that the **show ip mobile binding** output displays the attributes indicating this information.

  Here is sample output:

```
Active-HA#sh ip mobile binding
    Mobility Binding List:
Total 1
ct-cisco@cisco.com (Bindings 1):
        Home Addr 60.0.2.1
    Care-of Addr 4.0.2.3, Src Addr 4.0.2.3
    Lifetime granted 00:33:20 (2000), remaining 00:33:15
    Flags sbdmg-t-, Identification C1F3C1D5.0000000F
    Tunnel1 src 40.0.11.20 dest 4.0.2.3 reverse-allowed
    Routing Options -
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000005
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Correlation Id cisco-ha(vendor id 20942)
    Calling Station Id cisco
    Served MDN CT-MDN
    Charging Type 0x00000001
    Traffic Plane Id:7
```

The following attributes are supported as part of this feature.

- Correlation-Id
- Calling-Station-Id
- Served-MDN
- Charging-Type
- HA-Service-Address

Also, as part of this feature support, interactions with the FA and AAA server are slightly modified. The following sub-sections provide additional details.

Interactions with FA

With this feature support, the HA processes the following attributes that are received in RRQ:

- **Calling-Station-Id:**

  To support the Calling Station ID attribute in MIP RRQ message, so that the PDSN/FA has to send the user's IMSI to the HA. The HA uses this attribute to send to AAA server during Authentication.

- **Correlation-Id:**

  The HA processes the received Correlation-Id from the FA in the format of defined in RFC 3115 for Vendor specific attributes for MobileIP.

  When the HA receives new values for the correlation-id or calling-station-id attributes in an RRQ during re-registration, the HA sends an Accounting Stop and Start for the MIP session.

Interaction with AAA

The HA will deal with the following attributes during the interaction with AAA for authentication and Accounting,

- **Correlation-Id**

  The received Correlation-Id in RRQ is sent in Accounting Start/Stop/Interim Messages to the AAA server. This attribute is not included during Authentication with AAA.

- Calling-Station-Id

  The received Calling-Station-Id in RRQ is sent in an Access-Request during Authentication with AAA for MN subscriber. This attribute is also sent in Accounting Start/Stop/Interim Messages to AAA server. The HA sends the Calling-Station-Id to AAA in the format of standard RADIUS Attribute [31] , as defined in RFC 2865.

- **Served-MDN**

  The HA receives the Served MDN value in an tAccess-Accept after successful authentication with the AAA server. The received attribute is sent in Accounting Start/Stop Messages only to the AAA for accounting purposes.

- **Charging-Type**

  The HA receives the Charging-Type value in an Access-Accept after successful authentication with the AAA server. The received attribute is sent in Accounting Start/Stop messages only to the AAA for accounting purposes.

  Charging-Type values include the following:

  - 0x00000001- Post-paid accounting
  - 0x00000002- Pre-paid accounting
  - 0x00000003- both post-paid and pre-paid accounting

- **HA-Service-Address**

  The HA sends the user's HA service address to the AAA in an accounting-start message.

Table 3-2 illustrates how the HA incorporates the attribute values in various Radius messages (RFC 2865 and 2866) during interaction with AAA.

Table 3-2 HA Attributes in Radius Messages During AAA

Attribute	Attribute Value	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Calling-Station-Id	31	0-1	0	0-1	0-1	0-1
Correlation-Id	26/5535/44	0	0	0-1	0-1	0-1
Served-MDN	26/ 20942/ 100	0	0-1	0-1	0-1	0

Table 3-2 HA Attributes in Radius Messages During AAA

Charging-Type	26/ 20942/ 101	0	0-1	0-1	0-1	0
HA-Service-Addres	26/5535/7	0	0	0-1	0-1	0

Redundancy Support in Home Agent Release 5.0

Redundancy support for Home Agent 5.0 features is identical to Release 4.0 of the Home Agent with the exception of the Home Agent Accounting, MIP-LAC, Mobile Router, VRF, and Home Agent as LNS features.

The active—standby redundancy interaction is between the control processors of the active and standby service blades.

Performance Requirements

The Single IP Home Agent will support the following performance figures:

- 500,000 registered subscribers per service blade
- 5 Gbps throughput.
- The time required to bulk-sync an Active Home Agent service blade hosting 500,000 subscriber registrations to a reloaded Standby Home Agent service blade will take no longer than the time taken to bulk-sync a fully loaded Active to Standby service blade in the “six independent processor” model. There is no intention to proportionately reduce the bulk-sync time from x to x * (500,000 / 1,400,000).
- The call per second rate is no slower than for a single processor in the “six independent processor model”. The call per second rate meets or exceeds the rate measured during performance verification for Sprint.

Single IP Support - Reused and New CLIs

The following CLIs are provided to allow IPC to communicate with IXP, and to allow GTP and IPC over GTP modules to provide the reliable, acknowledged and unacknowledged communication capability between the SAMI PPCs:

EXEC Mode

- **debug sami ipc gtp ipc 3-8>**
- **debug sami ipc gtp ipc**
- **debug sami ipc gtp any**
- **debug sami ipc detail**
- **debug sami ipc**
- **debug sami ipc stats detail**
- **debug sami ipc stats**
- **debug sami configuration sync**

- **test sami tp-config [enable|disable]** (available on TPs in SingleIP image)

Show Commands

- **show sami ipcp ipc gtp**
- **show sami ipcp ipc ixp**
- **show sami ipcp ipc processor**

Config Mode:

- **default sami ipc crashdump**
- **default sami ipc keepalive**
- **default sami ipc retransmit**
- **default sami ipc retries**
- **sami ipc crashdump**
- **sami ipc keepalive**
- **sami ipc retransmit**
- **sami ipc retries**

Distributed Configuration on Single IP Home Agent

The Distributed CLI agent distributes the configuration information from the CP to each of the TPs using the IPC protocol.

By default, the CLI agent allows all the commands, but only filter the ones that might trigger some functionality on the TP that is not needed.

For the single IP model, an EXEC banner is displayed when logging in to a TP and warns the user to be aware that “normal” maintenance activities should be run from CP.

Table 3-3 lists the commands that Home Agent Single IP supports, and indicates whether they are filtered at the CP or also sent to the TPs.

If the command is sent to the TPs, then it is executed at each of the TPs.

Table 3-3 Home Agent Commands for Single IP

Command (Config Commands)	Purpose	To be filtered at Control Processor
aaa authentication ppp default group radius	Enables authentication of PPP users using RADIUS.	No
aaa authentication login default group radius	Specifies RADIUS as the default method for user authentication during login.	No
aaa authorization commands	Reestablish the default created when the **aaa authorization commands** command was issued,	No

Table 3-3 Home Agent Commands for Single IP (continued)

aaa authorization ipmobile default group radius	Authorizes Mobile IP to retrieve security associations from the AAA server using RADIUS	No
aaa authorization network default group radius	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.	No
aaa accounting network default start-stop group radius	Enables accounting by sending a "start" accounting notice at the beginning of a process and "stop" accounting notice at the end of a process to RADIUS servers.	No
aaa accounting system default start-stop group radius	Enables the HA to send system messages.	No
aaa accounting update newinfo	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.	No
aaa session-id common	Ensures that all session identification (ID) information that is sent out for a given call will be made identical.	No
aaa server radius dynamic author	Enables support for received Change of Authorization message	No
radius-server host *ip-addr* **key** *sharedsecret*	Specifies the IP address of the RADIUS server host and specifies the shared secret text string used between the router and the RADIUS server.	No
radius-server retransmit *retries*	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.	No
radius-server vsa send authentication 3gpp2	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor- specific attributes to only authentication attributes.	No

Table 3-3 Home Agent Commands for Single IP (continued)

radius-server vsa send accounting 3gpp2	Enables the use of vendor-specific attributes (VSA) as defined by RADIUS IETF attribute 26. Limits the set of recognized vendor-specific attributes to only accounting attributes.	No
radius-server vsa send authentication wimax	Enables use of WiMax specific attributes	No
radius-server vsa send accounting wimax	Enables use of WiMax specific attributes	No
radius-server snmp-trap retrans-threshold *50 - 75*	Generates a trap (SNMP notification) when a retransmit value goes above the high threshold value, and comes below the normal threshold value.	No
radius-server snmp-trap timeout-threshold *50 - 75*	Generates a trap (SNMP notification) when a round trip value goes above the high threshold value, and comes below the normal threshold value.	No
router mobile	Enables mobile IP on the router	No
ip mobile host {*lower* [*upper*] | **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | **local-pool** *name*}] [**address** {*addr* | **pool** {**local** *name* | **dhcp-proxy- client** [**dhcp-server** *addr*]}]} {**interface** ***name*** | **virtual-network** *network-address mask*} [**aaa** [**load-sa** [**permanent**]]] [**authorized-pool** *name*] [**skip-aaa-reauthentication**][**care-of-access** *access-list*] [**lifetime** *seconds*]	Configures mobile host or mobile node group (ranging from lower address to *upper* address group) to be supported by the home-agent.	No
ip mobile virtual-network *netmask* [**address** *address*]	Defines a virtual network	No
router(config-if)#standby [*group-number*] **ip** ***ip-address***	Enables HSRP	Yes
router(config-if)#standby [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]	Sets the Hot Standby priority used in choosing the active router.	Yes
router(config-if)# standby name *hsrp-group-name*	Sets the name of the standby group	Yes

Table 3-3 Home Agent Commands for Single IP (continued)

ip mobile home-agent redundancy *hsrp-group-name*	Configures the Home Agent for redundancy using the HSRP group name.	Yes
ip mobile home-agent dynamic-address *ip address*	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to ip address.	No
ip mobile home-agent revocation	Enables support for MIPv4 Registration Revocation on the HA	Yes
interface tunnel *10*	Configures a tunnel template.	No
ip mobile home-agent template tunnel *10* **address** *10.0.0.1*	Configures a Home Agent to use the template tunnel.	No
ip mobile home-agent accounting *list*	Enables HA accounting, and applies the previously defined accounting method list for Home Agent. List is the AAA Accounting method used to generate HA accounting records.	No
ip mobile home-agent *method* **redundancy [virtual-network address** *address***] periodic-sync**	Syncs the byte and packet counts for each binding to the standby unit using an accounting update event. This sync only occurs if the byte counts have changed since the last sync.	No
ip mobile realm *realm* **hotline redirect** *redirect-server-ipaddress*	Enables inbound user sessions to be disconnected when specific session attributes are presented.	No
ip mobile home-agent dfp-max-weight *dfp-max-weight-value*	This command enables the maximum dfp weight that can be allowed on HA. By default, the max dfp weight value is 24.	**No**
ip mobile home-agent max-cps *max-cps-value*	This command enables the maximum cps that can be allowed on HA. By default, the max cps value is 160cps with accounting support.	**No**
ip mobile home-agent max-binding *max-binding-value*	Limits the number of bindings that can be opened on the HA. The default value of max-binding-value is 235,000.	No

Table 3-3 Home Agent Commands for Single IP (continued)

ip mobile home-agent host-config url *url*	As part of this feature, a new CLI has been introduced to configure the URL on the HA. This is needed as sometimes HA will not be able to provide the configs requested by MN. To address this situation this generic site specified by the URL will help MN to download its configs parameters. Sample configuration: **ip mobile home-agent host-config** url http://www.cisco.com	No
ip mobile realm *realm* **hotline capability profile-based redirect ip**	This command configures a profile-based hot-lining for users with ip-redirection rules. Here, the realm can be nai/realm. The no version of this CLI will delete the profile-based ip-redirection rules.	No
ip mobile realm *realm* **hotline capability profile-based redirect http**	This command configures a profile-based hot-lining for users with http-redirection rules. Here, the realm can be nai/realm. The no version of this CLI will delete the profile-based http-redirection rules.	No
ip mobile home-agent aaa attribute framed-pool	Support the download of the RADIUS Framed Pool name downloaded during the authentication	No

Table 3-3 Home Agent Commands for Single IP (continued)

Router(config-cmap)#**match flow mip-bind** Router(config-pmap-c)#**police rate mip-binding [bc** *bytes***] [peak-rate mip-binding [be** *bytes***]]**	To classify packets for each binding, belonging to a class of MN users with a specified rate, the following CLI is configured in MQC class-map config mode. To police the individual MN binding already identified to MQC, based on the specified rate, the following CLI is specified in policy-map config mode specific to a configured class. Sample Configuration: class-map class-mip match flow mip-binding policy-map policy-mip-flow class class-mip police rate mip-binding [bc <bytes>] [peak-rate mip-binding [be <byes>]] conform-action <action> exceed-action <action> violate-action <action>	No
ip mobile home-agent service-policy [input *policy-name* **[output** *policy-name***]**	This CLI attaches the HA to QoS police function through the service-policy command. It helps identify HA by associating service-policy to the HA virtual interface object. The command is configured for both traffic directions.	No
ip local pool *poolname start_address end_address* **group** *customer-x* **priority** *0..255*	The new option "priority 0..255" is an optional to ip local pool. By configuring this option, priority will be assigned to the newly created pool and the same will be used in assigning IP Address.	No
ip mobile realm *@xyz.com* **vrf** *vrf-name* **ha-addr** *ip-address* **[aaa-group [accounting** *aaa-acct-group* **| authentication** *aaa-auth-group***]]** [**dns dynamic-update method** *word*] [**dns server** *primary dns server address secondary dns server address* [**assign**]] [**hotline**] [**ppp-regeneration** [**setup-time** *number*]]	Defines the VRF for the domain @xyz.com. The option "ppp-regeneration <setup-time <number>" will be optional to "ip mobile realm" command. By configuring this option, PPP regeneration feature will be enabled and every MIP session matching this realm will be mapped to a corresponding L2TP session.	No
router ospf *process-id*	Enables OSPF routing, which places you in router configuration mode.	Yes

Table 3-3 Home Agent Commands for Single IP (continued)

network *ip-address wildcard-mask* **area** *area-id*	Defines an interface on which OSPF runs and define the area ID for that interface.	Yes
ip ospf cost *cost*	Explicitly specifies the cost of sending a packet on an OSPF interface.	Yes
ip ospf retransmit-interval *seconds*	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.	Yes
ip ospf transmit-delay *seconds*	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.	Yes
ip ospf priority *number-value*	Sets priority to help determine the OSPF designated router for a network.	Yes
ip ospf hello-interval *seconds*	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.	Yes
ip ospf dead-interval *seconds*	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.	Yes
ip ospf authentication-key *key*	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.	Yes
ip ospf message-digest-key *key-id* **md5** *key*	Enables OSPF MD5 authentication. The values for the *key-id* and *key* arguments must match values specified for other neighbors on a network segment.	Yes
ip ospf authentication [**message-digest** | **null**]	Specifies the authentication type for an interface.	Yes
access-list *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	Defines a standard IP access list.	No
ip access-list {**standard** | **extended**} *access-list-name*	Define an IP access list by name.	No
snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]	Enables the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) Notifications.	Yes

Table 3-3 Home Agent Commands for Single IP (continued)

snmp-server enable traps ipmobile	Enables Simple Network Management Protocol (SNMP) security notifications for Mobile IP	Yes
snmp mib [bulkstat | community-map | notification-log | persist]	Defines bulk statistics collection	Yes

Note For any configuration command that is filtered, its sub configuration commands are also filtered.

Distributed Show and Debug

By default, all the **debug** commands are executed in the TPs, and the trace gets displayed from the CP. The CP does not perform any aggregation for distributed debug.

For debug AAA / RADIUS commands, these are executed on the TP as well as the CP but as no Radius transactions occur on the TP, the debugs will not be displayed. For example, the radius transaction corresponding to a received PoD or CoA is only handled at the CP. An internal event is passed from CP to the appropriate TP indicating that a PoD/CoA has occurred but this is not in the form of a Radius transaction.

debug ip mobile commands are not executed at the TP as, when a subscriber binding is created, this occurs at both the CP and the selected TP. Only one set of debug output is necessary.

Distributed Show - By default the show commands are not executed at all TPs. Only for the commands listed in Table 3-4 is aggregation done periodically at the CP for the data collected from the TPs (traffic counters are maintained by the TPs).

Note The **Execute On … clear** command is now a Service Internal command

The Table 3-4 lists the show and debug commands that are supported on the Single IP Home Agent for Release 5.0:

Table 3-4 show and debug Commands That are Supported on the Single IP Home Agent

Command (Show and Debug)	Purpose	Aggregation Required? (Yes/No)	Is the exec command sent to TP ?
show ip mobile binding [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **police** [**nai** *string*] | **summary**]	Displays the mobility binding table on the home agent (HA).	Yes	No
show ip mobile host [*address* | **interface** *interface* | **network** *address* | **nai** *string* | **group** | **summary**]	Displays mobile node information.	Yes	No
show ip mobile traffic	Displays HA protocol counters	Yes	No

Table 3-4 show and debug Commands That are Supported on the Single IP Home Agent (continued) (continued)

show ip mobile tunnel [*interface*]	Displays information about the mobile IP tunnels.	Yes	No
show policy-map [apn *mn-apn-index* **[realm** *string* **]]**	CLI in exec mode will display aggregate policing statistics for flows across the MN-APN interface.	No	No
show ip mobile hot-line capability [realm *word***] [all]**	Display hot-line capability of username/nai or realm. If the username or realm is not specified, display information all the user or realms currently hot-lined on HA.	No	No
show ip mobile globals	Displays global information for Mobile Agents.	No	No
show ip mobile secure	Displays mobility security associations for Mobile IP.	No	No
show ip route vrf	Displays the routing table information corresponding to a VRF.	No	No
show ip mobile redundancy	Displays the redundancy status of the Home Agent.	No	No
show ip mobile secure	Displays mobility security associations for Mobile IP.	No	No
show ip mobile ipc	Displays ipc information for CP-TP interface	No	No
debug ip mobile advertise	Displays advertisement information.	No	No
debug aaa authentication	Displays information on AAA/TACACS+ authorization.	No	Yes
debug aaa pod	Displays debug information for Radius Disconnect message processing at AAA subsystem level.	No	Yes
debug ip mobile [advertise | dfp | host | local-area | redundancy | router | upd-tunneling | vpdn-tunneling [events | detail]| ipc | mib]	Displays IP mobility activities.	No	No
debug ip mobile host [*acl* **| nai | mac** *H.H.H*]	Displays mobility event information.	No	No
debug ip mobile redundancy {**events | error | detail | periodic-sync**}	Displays IP mobility events.	No	No
debug radius [accounting | authentication | brief | elog | failover | periodic-sync | retrans-mit | verbose]	Displays information associated with RADIUS.	No	Yes
debug tacacs [**accounting | authentication | authorization | events | packet**]	Displays information associated with TACACS.	No	Yes

Only for the **show ip mobile binding** [**nai** string | ip address] command and the **show ip mobile host** [**nai** *string* | *ip address*] command, the CP will use a Pull mechanism to get the current counters from the TPs. The interval for the counters displayed in these **show** commands is too long to make them irrelevant.

Note The **clear mobile ip binding all load** command is no longer available for the Home Agent product. This is replaced by the requirement to perform a reload rather than using this command.

Show CLI Enhancements for Chassis Management

Table 3-5 lists the **show** commands are added to support the chassis-wide management interface for the Single IP Home Agent. Refer to the section for further details.

Table 3-5 Chassis Management-related Show Commands

CLI Command	Purpose	Does it collect info from the TPs? (Yes/No)
show ip mobile binding fa [*coa-ip*]	Displays the mobility binding table on the home-agent with the matching care-of-address.	No
show ip mobile binding fa [*coa-ip*] **summary**	Displays the summary of mobility binding table on the home-agent with the matching care-of-address.	No
show ip mobile binding granted-lifetime greater [*time*]	Displays the of mobility binding table on the home-agent with the granted-lifetime greater than *time*.	No
show ip mobile binding granted-lifetime greater [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the granted-lifetime greater than *time*.	No
show ip mobile binding granted-lifetime equals [*time*]	Displays the of mobility binding table on the home-agent with the granted-lifetime equal to *time*.	No
show ip mobile binding granted-lifetime equals [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the grated-lifetime equal to *time*.	No
show ip mobile binding granted-lifetime less [*time*]	Displays the mobility binding table on the home-agent with the granted-lifetime less than *time*.	No
show ip mobile binding granted-lifetime less [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the granted-lifetime less than *time*.	No
show ip mobile binding remaining-lifetime greater [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime greater than *time*.	No
show ip mobile binding remaining-lifetime greater [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime greater than *time*.	No

Table 3-5 Chassis Management-related Show Commands (continued)

show ip mobile binding remaining-lifetime equals [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime equals to *time*.	No
show ip mobile binding remaining-lifetime equals [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime equals to *time*.	No
show ip mobile binding remaining-lifetime less [*time*]	Displays the mobility binding table on the home-agent with the remaining-lifetime less than *time*.	No
show ip mobile binding remaining-lifetime less [*time*] **summary**	Displays the summary of mobility binding table on the home-agent with the remaining-lifetime less than *time*.	No

Network Management and MIBs

One focus of the Single IP design is to provide single MIB access per service blade. The result is that a number of MIBs will now have six entries, one per processor, rather than a single entry. This applies specifically to the CISCO-PROCESS-MIB and the CISCO-ENHANCED-MEMPOOL-MIB.

The other MIBs used for Home Agent management, RFC 2002 MIB, CISCO-MOBILE-IP-MIB, CISCO-IP-LOCAL-POOL-MIB, RADIUS Authentication Client MIB are not affected by this system design.

Here is a list of MIBs that are used as a source of key performance indicators (KPIs):

- RFC 2002 MIB
- CISCO-MOBILE-IP-MIB
- RFC 2618 RADIUS Authentication Client MIB
- IF-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-MEMORY-POOL-MIB - Replaced by ENHANCED-MEMPOOL-MIB
- CISCO-ENHANCED-MEMPOOL-MIB

Both the CISCO-PROCESS-MIB and the CISCO-MEMORY-POOL-MIB are required to provide a single MIB report per service blade. Both of these MIBs contain per-processor content. Because the design requires that the information for all six application processors is reported with one SNMP GET, each MIB will contain six entries, one per application processor.

The IF-MIB will contain information for interfaces of the Traffic Plane processors in addition to the interfaces of the Control Plane processor.

The CISCO-PROCESS-MIB already contains a facility to provide information for one or more CPUs. The CISCO-MEMORY-POOL-MIB does not support this capability. Nor does the the Home Agent currently support the CISCO-ENHANCED-MEMPOOL-MIB.

The RADIUS Authentication Client MIB is not currently supported in the Home Agent image and is required.

Table 3-6 lists the supported MIBs:

Table 3-6 Single IP MIBs for HA Release 5.0

MIB	Description	Does it need info from TP?	If Yes, Mechanism
RFC2006-MIB	This uses the definitions defined in RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*	No, there are no traffic counters.	
CISCO-MOBILE-IP-MIB	This allows you to monitor the total number of HA mobility bindings and the total number of FA visitor bindings using an NM	No, it has only counters for control messages.	
RFC2618 RADIUS Authentication Client MIB	This uses the definitions defined in RFC 2618.	No, there are no traffic counters.	
IF-MIB	This contains information for interfaces of the Traffic Plane processors in addition to the interfaces of the Control Plane processor	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. TP sends update to CP every minute.
CISCO-IP-LOCAL-POOL-MIB	This MIB defines the configuration and monitoring capabilities relating to local IP pools.	No, there are no traffic counters.	
CISCO-ENHANCED-MEMPOOL-MIB	This is for monitoring the memory pools of all physical entities on a managed system.	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. Each TP sends update every second to CP.
CISCO-PROCESS-MIB	This describes the statistic of active system processes on processors running IOS, the six processor on the two daughter cards.	Yes	Data Aggregator on CP, Data Provider on TP, follows PUSH paradigm. CPU stats from TP are sent every second, other stats are sent every minute to CP.
CISCO-ENTITY-MIB	The MIB module for representing multiple logical entities supported by a single SNMP agent	Yes	Data Aggregator on CP, Data Provider on TP

Resource Requirements and Limitations

The re-architecture from a six "do-everything" processor model to a one control, multiple traffic plane model imposes some new resource constraints:

- Calls per Second figure will be bounded by the capability of a single CPU versus the previous six
- The number of supported Mobile IP bindings is limited by the memory available to the control plane processor. Home Agent 4.0 currently supports 235,000 subscribers per processor based on a memory limitation of 1Gigabyte. SAMI platform support of the Single IP Home Agent will provide 2 Gigabytes of memory per processor. Given that I/O memory does not need to be duplicated when combining the session capacity of two processors into one, HA Release 5.0 supports 500,000 subscribers per blade and does not require memory requirements in excess of 2 Gigabytes.
- Reducing the number of processors supporting user traffic from 6 to 5 requires a corresponding increase in throughput per processor of 20%. This is achieved as a result of the CEF/MFI rewrite activities of Home Agent 5.0.
- Decoupling of the control and traffic planes significantly reduces the inter-dependency of calls per second ratings and throughput achieved. The decoupling is not complete though.
- Establishing and and releasing mobile IP bindings requires inter-processor messaging between the control plane processor and the traffic plane processor chosen to provide packet routing for the user.
- The push/pull nature of the control plane to traffic plane interactions for MIB population on the control plane processor impacts both calls per second and throughput.
- The per-chassis features that require periodic retrieval of information from the service blade will impact the calls per second rating. Throughput is also affected as variables relevant to the per-chassis statistics collection are provided from the traffic plane in either a Push or Pull model.
- A tradeoff in performance occurs between Supervisor processing and service blade processing to support the various **show subscriber** command combinations.

Features Not Supported

The following features are not supported on the Home Agent 5.0 Single IP software release:

- MIP-LAC
- Mobile Router
- Home Agent as LNS
- Hotlining

Chassis Managment

The Single IP functionality depends on chassis management to provide a single OAM viewpoint for a defined set of functionality. This allows you to see whole chassis as a single black box without worrying about the multiple service blades having multiple processors, and separate active/standby configurations.

In order to get or set the right information on the right HA instance, the management commands check all the modules in the chassis, figure out the right module (active SAMI blades) and the HA instance(s) on these active blades. The Home Agent 5.0 release allows only one HA instance per service blade.

The following commands provide chassis management information, and are initiated from the active SUP card.

- **Show Subscriber**
- **Monitor Subscriber**
- **Show Subscriber Session**
- **Statistics Collection**

Restrictions

The Single IP model places some restrictions on packet routing configurations, both internal and external to the chassis.

Note You should perform all configuration change in a maintenance window.

Note After a reload, reboot the card to make sure things are working properly.

Note You must configure the **no auto-sync all** command for an inter-chassis SR setup. For inter-chassis, the "unit1/unit2" style of configuration commands do not apply.

Note
- Dynamic routing protocols for advertizing routes for mobile subnets run at the supervisor.

Note
- OSPF runs on the CP only of each SAMI blade for the purpose of advertizing mobile subnets to the Supervisor only.

Note
- Dynamic route updates are not propagated from the CP to the TP.

Note
- Static routes must be configured from the SAMI blade to the Supervisor.

Note
- All MN-sourced traffic will be routed from the same blade to the Supervisor. This applies to both MN-Network traffic and MN-MN traffic.

Note
- Routing MN-MN traffic within a TP on a SAMI blade is not possible.

Note
- An HSRP Virtual IP Address is no longer used as the IP address of the Mobile IP tunnel termination of the Home Agent.

Note
- You must configure a loopback address at the Home Agent for use as the Mobile IP tunnel termination address.

Note
- You must configure a loopback address for interfaces to external servers such as DHCP and Radius servers. Do not use the HSRP virtual IP address.

Note
- The Standby Home Agent does not advertize routes to the Supervisor.

Note
- The Supervisor routes packets to the Home Agent blade on the SAMI using the HSRP Virtual IP address and associated HSRP Virtual Mac address.

Note
- Any physical interface used for external routing of packets must have the IP address assigned using the **redundancy ip address** command so that the active and standby have the correct address assigned when using the config-sync feature.

CHAPTER 4

Assigning a Home Address on the Home Agent

This chapter discusses how the Cisco Mobile Wireless Home Agent assigns home addresses to a mobile node, the different address types, and provides configuration details and examples.

This chapter includes the following sections:

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.

Address Assignment Feature

The Address Assignment with session overwrite feature removes a stale session to allow a new session to be established for a device. The MAC address of the device remains the same, but the NAI (which may be obtained from outer EAP identity) and HoA may change.

The NAI realm (i.e., not the Home Address field in the RRQ) determines if static IP pool or dynamic IP pool address management is used.

In Home Agent Release 5.0, both CMIPv4 and PMIPv4 are supported. The address management performed is based on the MAC address in the registration.

The following conditions apply for a RRQ with and without MAC address (provided in the PMIPv4 Device ID Extension):

- If RRQ does not contain MAC address (CMIP), the session is managed based on R4.0 matrix
- If RRQ contains MAC address (PMIP), the session is managed based on R5.0 matrix.
- There is no handoff between CMIP and PMIP.
- Domain of CMIP users and PMIP users are not same.
- Home Addresses of CMIP users and PMIP users are not same. If VRF is used and CMIP users and PMIP users are in different VRFs, the HoA address may be same.

Client-based Mobile IPv4

CMIPv4 is based on HA Release 4.0 address assignment method. Configuration examples are illustrated below.

Static IP Pool:

```
ip mobile host nai @domain static-address local-pool pool_001
```

AAA assigns the HoA, and the HoA is set in the MIP RRQ for the initial registration.

Dynamic IP Pool Allowing Static Access:

```
ip mobile host nai @domain static-address local-pool pool_002 address pool local pool_002
```

If HoA is sent in the MIP RRQ for the initial registration, the HA establishes a session with the HoA. If HoA is not sent in the MIP RRQ for the initial registration, the HA assigns a HoA and establishes a session.

Dynamic IP Pool:

```
ip mobile host nai @domain address pool local pool_003
```

The HA assigns the HoA. The HoA is not set (0.0.0.0) in the MIP RRQ for the initial registration. The existing address management is described below using following pool types:

Proxy Mobile IPv4

PMIPv4 is based on the HA Release 5.0 address assignment method. The Address Assignment with HoA Overwrite feature removes a stale session to allow a new session to be established for a device. The MAC address of the device remains the same, but the NAI (which may be obtained from outer EAP identity) and HoA may change.

The NAI realm (not the Home Address field in the RRQ) determines if static IP pool or dynamic IP pool address management is used. The configuration examples are illustrated below:

Static IP Pool:

```
ip mobile host nai @domain static-address local-pool pool_001
```

AAA assigns the HoA. The HoA is set in the MIP RRQ for the initial registration.

Dynamic IP Pool:

```
ip mobile host nai @domain address pool local pool_003
```

The HA assigns the HoA. The HoA is either set or not set (0.0.0.0) in the MIP RRQ for the initial registration.

To enable the deletion of stale bindings, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent binding-overwrite`	Enables or disables the deletion of a stale binding identified by the Home Address, MAC address, and NAI information in the registration request.
Step 2	`router#debug ip mobile host mac H.H.H`	Enables MAC Address-based debugging.

Note The revocation message does not need to include NAI extension because multiple HA IP addresses are used for VRF support.

Here are three configuration examples to illustrate how to use the Address Assignment feature. :

MAC-based Session Using Static IP Pool HA Configuration

HA Config

```
ip local pool cisco-static-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com static-address local-pool
cisco-static-pool interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 1
    description ctc-mac-static
    registration lifetime 65535
    registration retries 0
    registration flags 42
    revocation flags 00
    home-agent 81.81.81.81
    home-address 5.1.0.1
    secure home-agent spi 100 key ascii cisco
    nai cisco-%f@cisco.com
    pmip skip subtype 2 idtype mac
    no extension fa-challenge
    no extension mn-fa
    no extension nat traversal
    extension revocation
```

MAC-based Session Using Dynamic IP Pool

HA Config

```
ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 1
  description ctc-mac-static
  registration lifetime 65535
```

```
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.1.0.1
  secure home-agent spi 100 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension fa-challenge
  no extension mn-fa
  no extension nat traversal
  extension revocation
```

Overwrite Existing Binding

HA Config

```
ip mobile home-agent binding-overwrite

ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 3
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation

simulator mip mn profile 4
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.0.0.2 0
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai pepsi-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation

simulator mip scenario 3
  mn profile 3
  fa 2.2.2.200
  mn id 20

  simulator mip scenario 4
```

```
mn profile 4
fa 2.2.2.200
mn id 21
```

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 Home Agent Assignment

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

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

The Home Agent sends a Registration Reply, and places it’s own IP address in the Home Agent field. At this point, any re-registration 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.

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 it's binding by sending a RRQ with either the allocated address, or 0.0.0.0 as it's 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 mippool 10.0.0.5 10.0.0.250
router (config)# ip mobile host nai @localpool.com address pool local mippool
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 you 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 used to return a specific address, the home address can be configured either 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”

Note The Framed-IP-Address attribute is also supported

Configuration Examples

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 10.0.0.1 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby priority 110
 standby preempt delay sync 100
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.8 255.255.0.0
 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
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
ip mobile virtual-network 10.0.0.0 255.0.0.0
```

```
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
radius-server host 172.16.0.2 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 10.0.0.2 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 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
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
!
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
```

CHAPTER 5

User Authentication and Authorization

This chapter discusses User Authentication and Authorization, and how to configure this feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

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 is used if no MN-AAA extension is present, and CHAP is always 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 the 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. This default password is a locally defined string such as “vendor”.

The HA 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. You can configure the Home Agent to communicate with a group of AAA servers; the server is chosen in round-robin fashion from the available configured servers.

To configure authorization and authentication on the HA, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile host {lower [upper] | nai string {static-address {addr1 [addr2] [addr3] [addr4] [addr5] | local-pool name} | address {addr | pool {local name | dhcp-proxy-client [dhcp-server addr]} {interface name | virtual-network network_address mask} [skip-chap | aaa [load-sa [permanent]] [authorized-pool pool name] [skip-aaa-reauthentication] [care-of-access acl] [lifetime seconds]`	Configures the mobile host or mobile node group on the HA. If the **aaa load-sa** option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration. If **aaa load-sa skip-aaa-reauthentication** is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration. The **aaa load-sa permanent** option is not supported on the Mobile Wireless Home Agent, and should not be configured.

The HA supports 3GPP2 and Cisco proprietary security extension attributes in RADIUS access accept packet. Sending 3GPP2 MN-HA SPI in Access Request to RADIUS server and processing the MN-HA Secure Key Received from RADIUS server is configurable on HA.

Cisco IOS provides a mechanism to authorize subscribers based on their realm. This can be done using a feature called “Subscriber Authorization”, the details of which can be found here: http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463.

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

Authentication Configuration Extension

The Home Agent allow you to configure when external authentication with AAA occurs for specific mobile IP events. Handoffs across foreign agents is treated as a registration and a de-registration event, and there is no specific configuration for handoff.

In the event that a re-registration request is received with a different SPI than used for a previous registration or re-registration for that session, the configuration options **enable | disable** for authentication on re-registration are ignored for this user.

Applying or modifying any configuration occurs at the next event for a given binding.

The following configuration is for the re-registration and de-registration events that may be on a per-realm (VRF) basis.

ip mobile host nai *string* aaa **load-sa skip-aaa-reauth** [*reregistration* | *deregistration*]

The default configuration is that authentication occurs for all three events (**ip mobile host nai** *string* **aaa load-sa**).

Here are some examples that assume the default configuration is in place:

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** results in AAA authentication occurring for registration only.

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *deregistration* results in AAA authentication occurring for registration and reregistration.

ip mobile host nai *string* **aaa skip-chap** results in no authentication occurring for initial registration, reregistration, and deregistration events.

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *reregistration* results in AAA authentication occurring for registration and deregistration only.

The **load-sa** keyword causes the HA to download and locally store the security attributes for mobile-home authentication during the entire session. Without this parameter the HA does not locally store the security attributes for mobile-home authentication, and must retrieve them from AAA for subsequent re-registration or de-registration.

3GPP2 RRQ Without MHAE

Currently, the HA treats the MN-HA authenticator extension in RRQ as mandatory. If an RRQ is received by the HA without the MHAE extension, that RRQ is ignored.

But 3GPP2 PMIP RRQs may not have MHAE extensions since they are not mandatory according to the standard/RFC. In Cisco HA Release 5.1, you can configure the HA to allow 3GPP2 PMIP RRQs without the MHAE extension provided it succeeds FA-HA authentication.

To configure this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent options mhae optional`	When configured, if the HA receives a 3GPP2 RRQ without an MHAE but with a valid FHAE, the HA processes the RRQ.

Note If a CMIP RRQ is received without MHAE, but with valid FHAE and the command is configured, the HA will still process the RRQ. It does not reject this RRQ, because the HA cannot differentiate between PMIP RRQs and CMIP RRQs. To avoid this situation, ensure that the FA checks for the CMIP RRQ, and makes sure it does not forward a CMIP RRQ without MHAE to the HA.

Local Authentication for 3GPP2

The existing HA 5.0 allows you to authenticate a user either using a downloaded SA from AAA, or on locally configured HA. This can be provisioned using the **aaa** keyword in the **show ip mobile host nai** command.

The HA 5.0 functionality can be configured per user/nai but not per access-type.

In HA Release 5.1, this feature along with NAI Authentication with local MN-HA SPI and Key, provides you the flexibility of authenticating a user using a downloaded SA or local SA based on access-type.

This feature addresses the requirement of authenticating a user using local SA for 3gpp2 access-type, and authenticating the same user using AAA SA for Wimax access-type. During 3gpp2 access-type, no Access-Request is sent to the AAA.

When enabled, the Access-Request is not sent to AAA even if the RRQ has an MN-AAA extension.

To configure the HA to perform local authentication for 3GPP2, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent options`	Enables a sub-mode that allows you to configure local authentication for 3GPP2.
Step 2	`Router(config)#access-type 3gpp2 suppress aaa access-request`	Allows configuration to suppress access-requests to AAA.

This configuration, when used with **ip mobile host nai aaa**, and **ip mobile secure host nai**, addresses the requirement of authenticating a user using local SA for 3gpp2 access-type, and authenticating the same user using AAA SA for Wimax access-type.

NAI Authentication with Local MN-HA SPI and Key

HA R5.0 supports local configuration for MN-HA security association (SA) or MN-HA SA downloaded from AAA, but not both together.

In HA Release 5.1, the HA supports both the local configuration of a MN-HA SA, as well as an SA downloaded from AAA. Regardless of whether an SA is configured locally or not, if the HA receives an SA in the access-response message from AAA, then only the SA downloaded from AAA is used for MN-HA authentication.

Limitations and Restrictions

- When the **ip mobile host** command is configured for a full-NAI, the SA(s) configured locally for the corresponding realm are not applied. If the local SA needs to be applied, then the SA(s) needs to be configured separately for the full-NAI.

  For example, consider the following case:

  - **ip mobile host nai** *@cisco.com* **virtual-network** *ip1 mask1* **aaa**
  - **ip mobile host nai** *user1@cisco.com* virtual-network ip2 mask2 **aaa**
  - **ip mobile secure host nai** *@cisco.com* **spi** *100* **key ascii** *CISCO*

  Here, the configured SA for *@cisco.com* is not applied to *user1@cisco.com*. If a local SA needs to be applied for this user, an SA needs to be configured separately:

  ip mobile secure host nai *user1@cisco.com* **spi** *100* **key ascii** *YAHOO*
- This feature is supported only for 3GPP2 users, and not for Wimax users.

No Authorization for Re-Reg / De-Reg

With the NAI Authentication with local MN-HA SPI and Key feature, both locally configured SA and SA downloaded from AAA are supported.

But when you configure the following command, the re-authentication and re-authorization are prevented only when the SA for MN-HA is received in an access-accept:

```
router (config)# ip mobile host nai realm virtual-network ip mask aaa load-sa
skip-aaa-reauth [rereg | dereg]
```

If the MN-HA authentication uses local SA during registration, even with the above configuration, the re-authentication/re-authorization is not skipped because the **load-sa** only caches the SA downloaded from AAA.

This feature supports caching SA even when using locally configured SA, if **load-sa** is configured. With **load-sa** configured, re-authorization is prevented even when using a locally configured SA. Additionally, when **skip-aaa-reauth** is configured, re-authentication with AAA is prevented when using a locally configured SA.

The [**rereg** | **dereg**] options, if specified, gives you the flexibility to prevent re-authentication and re-authorization for either re-registration or de-registration only.

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.

You can configure this feature on the HA using the **ip mobile host** command, noted above.

Configuration Examples

The following example configures a mobile node group to reside on virtual network 10.99.1.0 and retrieve and cache mobile node security associations from a AAA server. The cached security association is then used for subsequent registrations.

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached permanently until cleared manually.

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

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	Allowed In 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: • Outbound sent for PAP • Framed sent for CHAP • Framed received in both cases	Yes	Yes
Framed-Protocol	7	NA	4	integer	Framing protocol user is using. Sent for CHAP, received for PAP and CHAP. Supported values: • PPP	Yes	Yes
Framed Compression	13	NA	4	integer	Compression method Supported values: • 0 - None	No	Yes
Framed-Routing	10	NA	4	integer	Routing method Supported values: • 0 - None	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: • 0 - Async	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	Allowed In 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 **ip mobile secure host** *addr* 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

CHAPTER 6

Home Agent Redundancy

This chapter discusses several concepts related to Home Agent redundancy, how Home Agent redundancy works, and how to configure redundancy on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

Overview of 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 the 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.

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 the Cisco 7600 series platform, the backup Home Agent image is configured on a different SAMI 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.

Note In Cisco Home Agent Release 5.0 and above, the supported redundancy features that are the same as those supported in Release 4.0, except for the MIP-LAC, Mobile Router, VRF, Home Agent as LNS, and Home Agent Accounting features. The Change of Authorization and Packet of Disconnect features are still supported as they are independent of the accounting feature. The active / standby redundancy interaction is between the control processors of the active and standby service blades. There is no need for inter-traffic processor redundancy as the Home Agent accounting feature is not supported in this release.

Note HA Release 5.0 and above supports both intra-chassis and inter-chassis redundancy.

Home Agent Session Redundancy Infrastructure

Limitations of Home Agent Session Redundancy

Home Agent stateful session redundancy till release 4.0 was implemented over HSRP. In that implementation the transport between active and standby HA was implemented by home agent application. The UDP/IP-based transport implementation posed the following limitations:

- Inconstancies in bulk sync scenarios. For example while bulk sync is going on, if bindings are deleted on the active, then at the end of bulk sync completion the number of bindings seen on active and standby is inconsistent.
- Inability to sync multi packet sync data. This is seen during syncing hot-lining rules. When hot lining rules are large in number, the length of data required to be synced is larger to contain in one packet. The ability of syncing such data which is fragmented in multiple packets is inconsistent due to lack of packet sequencing, fragmentation and de-fragmentation support implemented in redundancy transport.

In the Session Redundancy infrastructure enhancement, the previously mentioned limitations are eliminated. In the Home Agent 5.0 release, HA SR infrastructure is implemented over a Component Cluster Manager (CCM). CCM software is built on top IOS High Availability infrastructure which contains (Redundancy Framework) RF/RF-Interdev and CF (Check-Pointing Facility)/SCTP (Stream Control Transport Protocol). RF/RF-Interdev take care of redundancy control signaling and CF/SCTP provides transport mechanism. This HA SR rework brings the advantages of the IOS High Availability feature such as robust transport, inter-chassis/intra-chassis redundancy support.

Supported Redundancy Events

The existing HA 4.0 redundancy events are discussed below. New redundancy events that occur as a result of new features implemented by 5.0 features are discussed in the section appropriate to that feature.

Dynamic Sync Events

Binding Creation

This sync is conveyed by using IPMOBILE_BINDUPDATE_REQ message from active to standby. Standby acknowledges successful recreation of binding using PMOBILE_BINDUPDATE_ACK.

Binding Deletion

This sync is conveyed by using IPMOBILE_BINDDELETE_REQ message from active to standby. Standby acknowledges successful deletion of bindings using IPMOBILE_BINDDELETE_ACK message to active.

Binding Update

Due CoA as a result of hotline status update. When the active HA receives a CoA message in which the hotline status of binding is updated, then the update in the existing binding date is conveyed to standby using IPMOBILE_BINDINTERIM_REQ message. The standby receives the above message, updates the existing binding, and conveys the update status using IPMOBILE_BINDINTERIM_ACK.

Binding Update as a Result of Accounting Counter Sync

When accounting counters are updated during the lifetime of a call then every accounting update message triggers IPMOBILE_BINDSYNC_REQ message to standby which contains updated counters to standby. Standby updates the counters for the bindings on it, and updates the status of updation using IPMOBILE_BINDSYNC_ACK message.

Table 6-1 lists the new sync events implemented for dynamic sync events mentioned above.

Table 6-1 Dynamic Sync Events

Current Event Name	New Event Name	Comment
IPMOBILE_BINDUPDATE_REQ, IPMOBILE_BINDUPDATE_ACK	IPMOBILE_BIND_CREATE	Used to sync Binding creation.
IPMOBILE_BINDINTERIM_REQ, IPMOBILE_BINDINTERIM_ACK	IPMOBILE_BIND_HOTLINE_UPDATE	Used to sync binding update due CoA processing.
IPMOBILE_BINDDELETE_REQ, IPMOBILE_BINDDELETE_ACK	IPMOBILE_BIND_DELETE	This event is synced in presence of De-Registration, PoD, or Revocation. Binding deletion is conveyed using this message.
IPMOBILE_BINDSYNC_REQ, IPMOBILE_BINDSYNC_ACK	Not supported in this release	This event is used to sync accounting counters. But HA accounting counter synchronized is not going to be supported in 5.0.
IPMOBILE_BINDINTERIM_EXTND_REQ	Not Supported	This request is used to sync when the sync message size is large and needs to be sent in multiple packets. This will not be needed new SR

Bulk Sync Events

When a router comes up as the standby it sends IPMOBILE_BINDINFO_REQ to existing active to retrieve all the existing bindings. Active replies in IPMOBILE_BINDINFO_RSP messages which contains binding information. Standby processes IPMOBILE_BINDINFO_RSP messages to recreates bindings on it and replies the status of recreation in IPMOBILE_BINDINFO_ACK message to active. The number of bindings which active can host are to the tune of 500K. Hence during bulk sync process multiple IPMOBILE_BINDINFO_RSP and IPMOBILE_BINDINFO_ACK messages are exchanged between active and standby. In the new implementation active is going to sync IPMOBILE_BIND_CREATE event for each binding to standby which contains bind sync information.

The CCM software implements the bulk sync process through bundling mode during sync of binding from active to standby. This process is completely transparent to HA application. In bundling mode, CCM sends more than one binding info per sync packet to standby CCM. Also CCM provides a CLI to control the bulk sync process. Should the bulk sync process hog cpu operator can make use of CLI redundancy rate

subscriber redundancy rate *# of Sessions Per Unit Time*

This command controls the bulk sync process. In case of number of bindings to be synced during bulk sync process is large then no more than #Sessions Per unit time will be synced. This command ensures that the CPU is not overloaded by the bulk sync process.

Sync Event Behavior

In the new SR Infrastucture, the standby acts as a receiver of the events and messages from the active. The standby does not send any status or acknowledgement message to the active to convey the status of processing any sync event from the active. Hence IPMOBILE_BINDUPDATE_ACK, IPMOBILE_BINDINTERIM_ACK, IPMOBILE_BINDDELETE_ACK messages from standby are discontinued in new framework. This is a significant change from HA 4.0 release. The active HA assumes that the standby is successfully able to decode sync messages, and able to recreate, update, or delete a binding.

Single IP Considerations

With the Home Agent single IP architecture, the SAMI blade is divided in to two logical entities namely Control Plane (CP) and Traffic Plane (TP). Physically, the CP functionality resides on the first of the 6 PPCs on the SAMI blade with the following 5 PPCs taking care of TP processing. The CP processor takes care of all the control signaling (registration, de-registration, CoA, PoD, etc. associated with all the bindings), while the Traffic-Plane Processors (TP) handle traffic distributed across 5 PPCs.

From the SR perspective, redundancy contexts are present on the CP on both the active and standby. So redundancy control signaling and SCTP channel occurs between two CP on the active and standby. It is the responsibility of the CP on the active to dynamically sync binding creation, updates and deletion, on the CP on standby. Upon receiving sync messages it is the responsibility of the CP on the standby to propagate the binding on the TP similar to the way the active CP propagates bindings to the TP.

Although the Single IP feature is built into the HA software, it is tied to the architecture and is a platform specific feature. The Mobile IP redundancy design is agnostic to any architecture-specific aspects.

Geographical Redundancy

Home Agents in a redundant pair can be placed at geographically separate locations using a VPN solution (such as one based on MPLS) instead of a LAN/VLAN between Home Agent pairs. Such a deployment needs to implement correct routing logic in the network to route traffic to one of the Home Agents in the pair. If there is a network failure, both the HAs could transition to HSRP active state in such a deployment. The Home Agent Redundancy feature recovers from such a failure gracefully with minimal loss of bindings. The following scenario describes the failure recovery process:

1. HA1 (high priority) and HA2 (low priority) are deployed in redundant mode over a WAN link. HSRP is running between the home agents over the WAN link.
2. HA1 is active and HA2 is standby.
3. WAN connectivity to HA1 is lost, due to a network fault, so the HSRP link between HA1 and HA2 is lost.

4. HA2 does not receive hello packets, and transitions to active. HA1 remains active as well, for the same reason (the box itself is functional). If this feature is enabled, both HA1 and HA2 lower their priority.
5. Mobile traffic and signaling messages are routed to HA2. HA2 updates its binding table accordingly and if the feature is enabled, increases its priority back to the original value. But the changed home agent state information on HA2 do not get synched to HA1 (which is unreachable).
6. Network fault is corrected, and hello packets exchanged between HA1 and HA2.
7. Without this feature, HA1 remains active and HA2 moves to become standby, leading to loss of latest state information as created on HA2 at step #5. If this feature is enabled, HA1 moves to become standby and HA2 remains active. Hence latest information on HA2 gets synched to HA1. Once state information is replicated, HA1 moves back to its normal priority. This leads to HA1 becoming active and HA2 becoming standby.

As described above, the latest state information is maintained after network fault is corrected. To enable this feature, following commands should be configured on the HA:

track *tracking object id* **application home-agent**

This command creates a tracking object to track the home-agent state.

standby track *tracking object id* **decrement** *priority*

This command enables lowering priority as required by step #4 in the above failure scenario.

Note If preemption is configured, the *priority* value should be greater than the difference in priorities of the active and standby Homeagents.

Redundancy with Radius Downloaded Pool Names

The Cisco Mobile Wireless HA supports AAA downloadable pool names for address allocation. The radius pool-name attributes returned in an access accept for address allocation are “ip-pool” for dynamic address allocation, and “static-ip-pool” for static address authorization. The pool name returned in an access accept to the Home Agent will be synched to standby Home Agent during normal and bulk sync operation. This enables address allocation from the same pool on the standby Home Agent as well.

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:

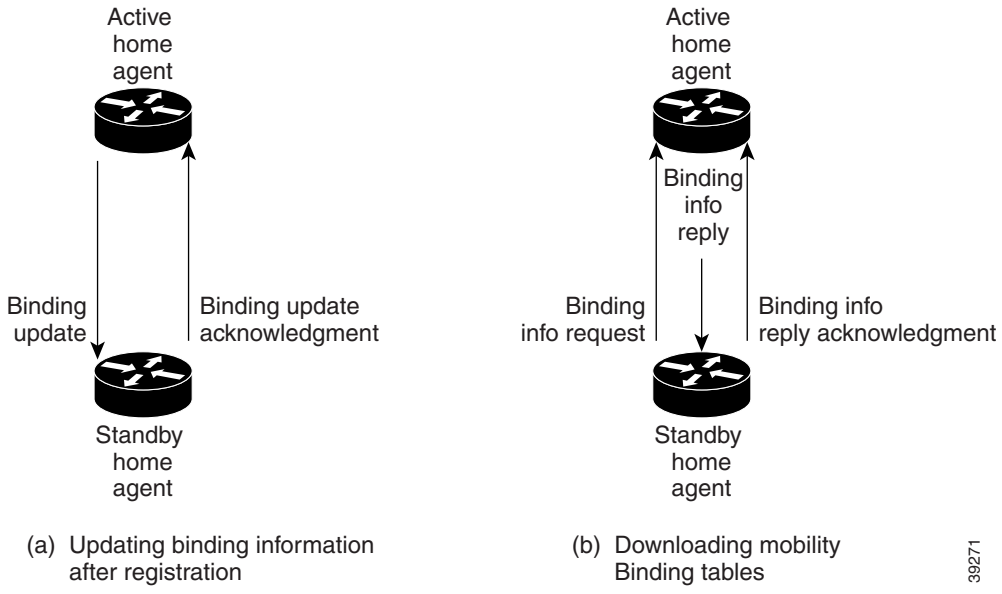
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN.
- An MN that requires the HA interface to be on the same subnet as the MN; that is, the HA and the MN must be on the same home network.

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 1 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 1 Overview of HA Redundancy and Mobility Binding Process



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

Physical Network Support

For MNs on physical networks, the HAs are configured in the active HA-standby HA configurations as shown in Figure 2 and Figure 3. 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 2 Virtual Network Support Using One Physical Network (Peer HA-Peer HA)

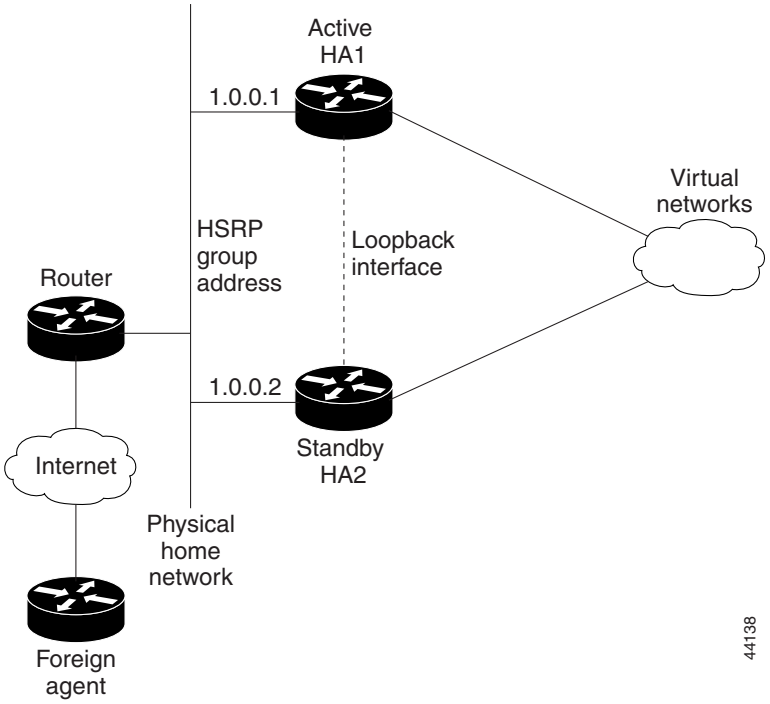
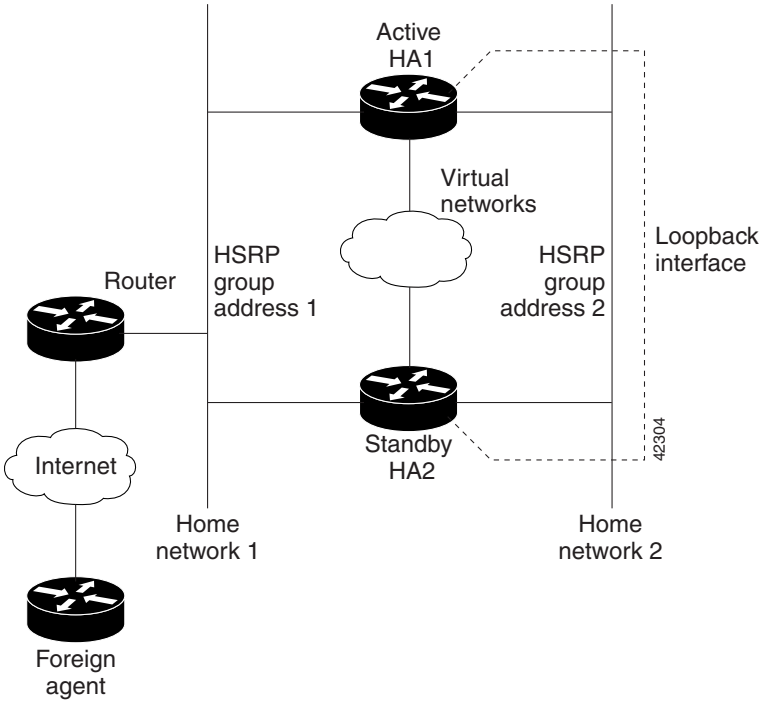


Figure 3 Virtual Network Support Using Multiple Physical Networks (Peer HA-Peer HA)



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 10.0.0.0 255.255.255.0 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 discontiguous 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 10.1.1.1 1.1.1.250
ip local pool pool1 10.1.2.1 1.1.2.250

ip mobile home-agent
ip mobile virtual-network 10.1.1.0 255.255.255.0
ip mobile virtual-network 10.1.2.0 255.255.255.0
ip mobile host nai @xyz.com address pool local pool1 virtual-network 10.1.1.0
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.

Priority Metric for Local Pool

In order to support the ability to change addressing schemes dynamically, a priority metric on a local address pool is introduced. This allows you to create a high priority address pool with the new address scheme. New bindings utilize this new address pool. Existing subscribers continue to use their current address until they disconnect, and upon reconnect they are allocated an address from the new pool. When all subscribers age out of the old address pool, it can be removed.

Currently, different addressing schemes (range of addresses) are configured under the same pool name, and the IP address will be assigned from the pool in the order of configuration. Initially, the first configured range of addresses is used to assign the IP Address, and when all the addresses have been utilized, the subsequent range is then used to assign IP Address, and so on.

To override the above default behavior and configure subscribers to have different address scheme, a priority value is introduced with the pool. This allows you to use the higher priority pool over the lower priority one so that when a new registration request comes, the IP address is assigned from the desired pool.

By default, a priority value of 255 (high priority) is assigned to a newly created local pool. The pool priority value takes a value of 1 to 255, where 0 is less, and 255 is the higher priority.

Here is an example:

```
ip local pool hapool 1.0.0.0 1.0.0.255
ip local pool hapool 2.0.0.0 2.0.0.255
```

This example creates local pools with the priority of 255. An IP address is assigned in the order of configuration if more than one address scheme has the same priority. Initially, all 255 hosts are assigned from the first pool, and the second one will be used for subsequent requests.

```
ip local pool hapool 1.0.0.0 1.0.0.255 priority 200
ip local pool hapool 2.0.0.0 2.0.0.255 priority 100
```

This example creates local pools with the priority of 255. In this case, the IP address is assigned in the order of priority. Initially all 255 hosts are assigned from the second pool (which has a higher priority 100), and the first pool (priority 200) is used for subsequent requests.

Configuring Local Pool Priority Values

To configure a priority value for a local pool, perform the following task:

	Command	Purpose
Step 1	`Router(config)#ip local pool {default | poolname} [low-ip-address [high-ip-address]] [group group-name] [cache-size size] [priority 1-255] [theshold low-threshold high-threshold]`	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, to generate traps when pool utilization reaches a high or low threshold in percentage. The new option **priority** *1-255* is allows you to assign a priority to a newly created pool, and this priority is used to assign IP addresses.

Configuring HA Redundancy

Home Agent Redundancy Tasks (Required for Mobile IP)

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

- Enabling Mobile IP, page 6-11 (Required)
- Enabling HSRP, page 6-11 (Required)
- Configuring HSRP Group Attributes, page 6-12
- Enabling HA Redundancy for a Physical Network, page 6-12 (Required)
- Configuring Geographical Redundancy, page 6-13
- Configuring HA Load Balancing, page 6-13

Enabling Mobile IP

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

	Command	Purpose
Step 1	`Router(config)#router mobile`	Enables Mobile IP on the router.

Enabling HSRP

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

	Command	Purpose
Step 1	`Router(config-if)#standby [group-number] ip ip-address`	Enables HSRP.

Configuring HSRP Group Attributes

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

	Command	Purpose

Step 1	`Router(config-if)#`**`standby`** `[`*`group-number`*`]` **`priority`** *`priority`* `[`**`preempt`** `[`**`delay`** `[`**`minimum`** | **`sync`**`]` *`delay`*`]]`
	
	or
	
	`Router(config-if)#`**`standby`** `[`*`group-number`*`]` `[`**`priority`** *`priority`*`]` **`preempt`** `[`**`delay`** `[`**`minimum`** | **`sync`**`]` *`delay`*`]`
		Sets the Hot Standby priority used in choosing the active router. By default, the router that comes up later becomes standby. When one router is designated as an active HA, the priority is set highest in the HSRP group and the preemption is set. Configure the **preempt delay min** 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.

Step 2	`Router(config-if)#` **`standby`** *`group-number`* **`follow`** *`group-name`*	Specifies the number of the follow group and the name of the primary group to follow and share status. We recommend that the specified group number is the same as the primary group number.

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
Step 1	`Router(config-if)#`**`standby`** `[`*`group-number`*`]` **`ip`** *`ip-address`*	Enables HSRP.
Step 2	`Router(config-if)#` **`standby name`** *`hsrp-group-name`*	Sets the name of the standby group.
Step 3	`Router(config)#`**`ip mobile home-agent redundancy`**	Enables the Home Agent for redundancy.
Step 4	`Router(config)#` **`redundancy inter-device scheme standby`** *`hsrp-group-name`* **`ipc zone default`** **`association 1`** **`no shutdown`** **`protocol sctp`** **`local-port`** *`local-port-no`* **`local-ip`** *`local-ip-address`* **`remote-port`** *`remote-port-no`* **`remote-ip`** *`remote-ip-address`*	Configures RF-Interdev on the HA. HA redundancy is built on top of RF-Interdev.

Configuring Geographical Redundancy

To enable Geographical redundancy on the Home Agent, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# track` *tracking object id* `application home-agent`	Creates a tracking object to track the home-agent state.
Step 2	`Router(config)# standby track` *tracking object id* `decrement` *priority*	Enables HAs to lower their priority as required in a failure scenario.

Configuring HA Load Balancing

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

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent dynamic-address` *ip address*	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to *ip address*.

Home Agent Redundancy Configuration Examples

Active-HA Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
scheme standby cisco
!
!
!
redundancy
no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
association 1
no shutdown
protocol sctp
local-port 5000
local-ip 10.0.0.2
remote-port 5000
remote-ip 10.0.0.3
!
!
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
no auto-sync all
!
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby priority 110
standby preempt delay min 100
standby name cisco
!
interface GigabitEthernet0/0.172
description to AAA
encapsulation dot1Q 172
ip address 172.16.1.8 255.255.0.0
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.254
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
!
radius-server host 172.16.0.2 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 GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 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
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
prefix-suffix
!
radius-server host 172.16.0.2 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
```

Note For HA Release 5.0 and above, it is not neccesary to configure the **ip mobile secure home-agent** command for redundancy.

Redundancy Support for Hotlining

Note Home Agent Release 5.1 supports redundancy only for Hotlining of WiMax bindings.

Redundancy Support for QoS

HA release 4.0 and above does not support flow-based QoS policing involving continuous updates of dynamic runtime policymap information between active and standby HA. Since the HA only supports normal and bulk sync, any periodic updates of policing data or counter statistics will not be accurate.

Redundancy Support for Call admission Control (CAC)

At present there is no requirement to support redundancy for Call admission control (CAC). However, the backup Home Agent maintains its own state.

Redundancy Support for Framed-pool Standard

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for Priority-metric for Local Pool

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for Mobile IPv4 Host Configuration Extensions

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for WiMAX AAA Attributes

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

When HA redundancy is enabled, all attributes included in Access-Request and Accounting messages from the active are also present in the corresponding messages from the standby after switchover. Additionally, interim accounting messages are sent from the standby in the same interval as they are sent from the active. In order to achieve this, the values of the following attributes are synced to the standby.

- Chargeable User Identity (89)
- Acct-Multi-Session-Id (50)
- Acct-Interim-Interval (85)

Redundancy Support for SAMI Migration

It is necessary to have redundancy set up for seamless migration, and to prevent disruption in service. Please refer to the User Migration section in Planning to Configure the Home Agent chapter for details on how to migrate to the SAMI plarform.

CHAPTER 7

Configuring Load Balancing on the Home Agent

This chapter discusses concepts and configuration details regarding Server Load Balancing on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

HA Server Load Balancing

Note The HA-Server Load Balancing (HA-SLB) feature is not available on the Cisco 7301 Series Router

The 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/products/ps5940/products_white_paper0900aecd802921f0.shtml

The HA-SLB feature is available on the Cisco 7600 series platforms. This feature allows a set of real Home Agents, each running on an SAMI, to be identified by a single virtual server IP address residing on the Cisco 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 The 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 Note that the packet is not sent to virtual IP address (HA-SLB)

Step 6 The Real HA sends Mobile IP RRP to the PDSN/FA. The HA-SLB does not intercept this packet. The 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 reals 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 RRPs are 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.

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

- Configuring HA Load Balancing, page 7-3
- Configuring Server Load Balancing, page 7-3

Configuring HA Load Balancing

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

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent dynamic-address ip address`	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to *ip address*. This command is configured on the HA.

Configuring Server Load Balancing

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

	Command	Purpose
Step 1	`Router(config)# ip slb vserver name` `Router(config-slb-vserver)# virtual ip address udp 434 service ipmobile`	Enables the Mobile IP SLB feature. The *ip address* is the virtual Home Agent address to which registration requests from PDSN/FA will be sent. This is configured on the SLB Supervisor.

HA-SLB Configuration Examples

The following examples illustrate various HA-SLB configurations, including how to verify details of the 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 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  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. Optionally, the **idle ipmobile request** *idle-time-val* command configures the duration for which the session object exists.

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

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 10.1.1.10 255.255.255.0
```

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 10.1.1.51
```

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 number 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-7600#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-7600#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-7600#
```

Show Output on HAs:

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

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

Dispatched mode with DFP

Configuration on SLB:

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

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  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 MIPSLB
 virtual 10.1.1.10 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 10.1.1.51 500
 agent 10.1.1.52 500
!
```

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 10.1.1.10 255.255.255.0
!
```

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 10.1.1.51
```

Show Output on SLB:

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

```
SLB-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

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-7600#show ip slb reals

real                  farm name        weight  state          conns
--------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-7600#
```

Show output on HAs:

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

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

Currently, the number of bindings and memory usage are considered for calculating the load balancing in HA-SLB. The existing DFP (dynamic feedback protocol) weight calculation equation can be modified by considering the CPS (frequency of calls per second), and throughput parameters on each real server (HA).

The CPS on the HA calculated for every minute is called the Usage CPS, and can be configured to some maximum value (Available CPS) that can be handled by the HA. If the Usage CPS reaches the available CPS then the HA real server will return less weight to the SLB.

It is difficult to calculate throughput on a router, and it can be solved by usage of interrupt CPU for packet handling.

From the above two parameters, the equation looks like,

dfp_weight = (Maxbindings - NumberofBindings)*(cpu+mem)*

(Available cps - Usage cps) *dftp_max_weight / (Maxbindings*32*Available cps)

Note Currently a MIB item that contains metrics is not available.

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 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice

ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

Show Output on SLB:

The following example 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 4 MIP sessions which the HA-SLB load balanced equally across two real HAs (2 connections to each HA).

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51            HAFARM           1       OPERATIONAL    2
10.1.1.52            HAFARM           1       OPERATIONAL    2
```

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

```
SLB-7600#show ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
-------------------------------------------------------------------------------
MIPSLB          A984DF0A00000000 15.1.1.51       10.1.1.52               IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       10.1.1.52               IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       10.1.1.51               IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       10.1.1.51               IPMOBILE_ESTAB

SLB-7600#
```

Show Output on HAs:

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

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

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

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*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= 10.1.1.51, NAT= S
*Apr 21 15:26:03: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
SLB-7600#
```

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 10.1.1.51
  inservice
 !
 real 10.1.1.52
  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 MIPSLB
 virtual 10.1.1.10 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 10.1.1.51 500
 agent 10.1.1.52 500
```

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-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

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-7600#show ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-7600#
```

Show Output on HAs:

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

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

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

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 10.1.1.51, 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= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 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= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 1DC0E31400000000
```

Direct Mode of Operation and Crypto Transform Mode is Tunnel

```
Configuration on SLB:
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  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 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 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 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

Configuration on PDSN:

```
The following commands configure IPSEC on PDSN:
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 10.1.1.51 host 10.1.1.10
```

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-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     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.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
```

```
     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-7600#
```

Show Output on SLB:

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

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   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.: 10.1.1.51
      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: l2tpmap
         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: l2tpmap
         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: l2tpmap
         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: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4608000/3581)
         replay detection support: Y

      outbound pcp sas:

SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                 state
---------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12          IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12          IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11          IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11          IPMOBILE_ESTAB
SLB1-7600#
SLB1-7600#sh ip slb
SLB1-7600#sh ip slb rea
SLB1-7600#sh ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.99.11.11          FARM1            1       OPERATIONAL    2
10.99.11.12          FARM1            1       OPERATIONAL    2
SLB1-7600

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:

```
SLB1-7600#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 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 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 10.1.1.51
!
!
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 10.1.1.51
 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 unreachables
 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 10.1.1.15
!
!
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 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 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-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
```

```
    current_peer: 10.1.1.15
      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.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
      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-7600#
```

Show Output on SLB:

```
SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
------------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
```

```
SLB1-7600#
SLB1-7600#sh ip slb rea
SLB1-7600#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
SLB1-7600#
SLB1-7600#
```

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

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     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: l2tpmap
        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: l2tpmap
        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: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3527)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
```

```
        slot: 0, conn id: 11030, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3524)
        replay detection support: Y

    outbound pcp sas:


SLB1-7600#
```

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#
```

CHAPTER 8

Terminating IP Registrations

This chapter discusses how the Cisco Mobile Wireless Home Agent terminates IP registrations and how to configure the Home Agent to perform this function.

This chapter includes the following sections:

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 a registration revocation acknowledgement message to the HA. Additionally, if the PDSN/FA needs to terminate the session administratively, the FA sends a registration revocation message to the HA. The HA deletes the binding for the mobile, and sends a 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 MHAE. 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 a 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 a registration request to the HA.

Step 6 The HA sends a registration response to PDSN/FA (2).

Step 7 The HA sends a Mobile IP resource revocation message to the PDSN/FA (1).

Step 8 PDSN/FA (1) sends a Mobile IP resource revocation acknowledgement to the HA, and terminates the mobile IP data session for the mobile.

The following sample 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

During the registration revocation phase, the I (Inform) bit notifies the mobile node (MN) of the revoked data service in cases where the mobile node has more than one MobileIP flow. 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 also sets the I-bit to **1**, and the I-bit can be used during the revocation phase. When the HA initiates revocation (and if the I bit was negotiated), it sets the I bit to **1** in the Revocation message if a binding is administratively released, and sets it to **0** if a 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 also sets the I-bit to **1** in the revocation ACK message.

Configuring MIPv4 Registration Revocation

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

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent revocation`	Enables support for MIPv4 Registration Revocation on the HA.
Step 2	`Router(config)# ip mobile home-agent revocation timeout` *5* `retransmit` *6*	(Optional) Sets the retransmit count and timeout value for revocation messages.

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

```
Router(config)# ip mobile home-agent revoc timeout ?
  <1-100>  Wait time (default 3 secs)
Router(config)# ip mobile home-agent revoc retransmit ?
  <0-100>  Number of retries for a transaction (default 3)
```

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.

Simultaneous Bindings

The Home Agent does not support simultaneous bindings for the following reason:

- When multiple flows are established for the same NAI, a different IP address is assigned to each flow. Therefore, simultaneous binding is not required because its function is to maintain more than one flow to the same IP address.

Radius Disconnect

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

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

The following events occur when a Disconnect Request is received on the HA:

Step 1 Find the user session corresponding to the username (NAI).

Step 2 If the Framed-IP-Address attribute is received in the Disconnect Request, terminate the binding with corresponding to the address.

Step 3 If Framed-IP-Address is not received in the Disconnect Request, terminate all bindings for the user (NAI).

Configuring RADIUS Disconnect Client

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

Command	Purpose
`Router(config)# aaa server radius dynamic-author client a.b.c.d server-key hakey`	Enables POD and CoA processing on the HA..
`Router(config)#ip mobile radius disconnect`	Enables the functionality of processing RADIUS disconnect messages on the HA.

Command	Purpose
`Router(config)#radius-server attribute 32 include-in-access-req`	This command is required to include the optional NAS-Identifier attribute in Access-Request to the home AAA.
`Router# debug aaa pod`	Displays debug information for Radius Disconnect message processing at AAA subsystem level.

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.

Support for Binding Synch and Deletion

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 or a RADIUS disconnect message, are synched to the standby HA, or the peer HA. Also, the additional extensions and attributes for Revocation and Radius Disconnect are relayed to the standby. Registration Revocation and Radius Disconnect (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, or a Radius Disconnect message) 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 or a Radius Disconnect message), 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.

Binding Synch

The following call flow shows the sequences and message exchange among various network entities used to bring up the Mobile IP flow and synch the information to the standby Home Agent.

1. The MS originates a call and a PPP session is up.
2. The PDSN receives a MIP RRQ from the MN and authenticates the MN by FA-CHAP. The STC VSA with the appropriate value (2 or 3) is included in the Access-request message to the AAA. After successful authentication, the PDSN forwards the RRQ to the HA and includes the revocation support extension after the MHAE.
3. The HA, upon receiving the MIP RRQ containing a revocation extension, includes a revocation support extension in the MIP RRP sent back to PDSN. During HA-CHAP to authenticate the MS, the STC VSA with appropriate value (2 or 3) is included in the Access-request message sent to the AAA. The binding at the HA is now considered revocable.
4. The PDSN receives the MIP RRP containing a revocation extension. The binding at the PDSN is revocable as the MIP RRP contained a revocation extension
5. Since the Home Agent is configured in redundant mode, a Bind Update message is sent to the standby with the additional information (revocation support extension and STC NVSE).
6. The standby Home Agent regenerates the binding using the information received in the Bind Update message, and sends back a Bind Update Ack message with code “accept” on successful creation of a binding on the standby.

Binding Deletion

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 sample 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. The MS originates a call, a PPP session is up and a Mobile IP flow is setup on the active Home Agent with Registration revocation capability enabled and negotiated. The same is synched to the standby Home Agent.
2. When a user issues administrative clear command, the PDSN sends a Revocation message to the active Home Agent, 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 the resources associated with the binding for the Revocation message that 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 can now send and receive revocation messages.

Selective FA Revocation

In a 3GPP2 environment, when a subscriber roams between their service provider's network and another partner service provider's network, the PDSN gateway sends a Resource Revocation message to the Home Agent to remove the subscriber. This causes timing problems, so Selective FA Revocation selectively ignores these "remove subscriber" requests. Revocation is done on a Foreign Agent basis. Thus, a given HA will statically configure a list of Foreign Agents from which to ignore the "remove subscriber" messages.

Here is a detailed call-flow for Selective FA Revocation:

1. A dual 1x/DO handset registers with RF and establishes a data call on DO. Unlike a voice call, the RF network does not register this data call with the VLR, as it has no knowledge of EVDO networks (as per standards).
2. The handset goes dormant (35 seconds on Samsung, 30 seconds on RIM, 40 seconds on Sierra).
3. The handset does a physical transition from a DO coverage area to a 1x coverage area. As part of this transition, the handset informs the 1x RF via the MTX that it has an active Data Session, but has no data to send, as it's dormant (DRS bit is set to 0). A new session is established to the PDSN through the MTX PCF.
4. Based on the events in Step **3**, the 1x PCF queries the VLR for this active Data Session mentioned by the Handset, and because of Step **1**, cannot find such session.
5. As part of the events in Step **3**, the PCF now sends the PDSN (through the OpenRP interface) a message with the Mobility Event Indicator (MEI) set to **0**. To the PDSN, this event, as part of a call-setup is for a brand new session, does the following check
   - if **MEI=0** and IMSI is a new IMSI not currently assigned to an existing session, proceed and establish the new session.
   - if **MEI=0** and IMSI is currently assigned to a session, consider this session old, and tear down the session.
6. Since **MEI=0** and IMSI is currently assigned to a session (as this is a Hybrid PDSN, handling both DO and 1X sessions at the same time), the PDSN will send a PPP TermReq to the handset and send a Resource Revocation to the Home Agent.
7. The Mobile Node, which was dormant, does not see the TermReq. The MTX RF will buffer the message for a while.
8. The Mobile Node becomes active and has data to send. It still acts as if it has a valid Mobile IP session, receives the TermReq (buffered), and Acks the message, followed by an immediate RF setup/RRQ. The RRQ contains previously assigned values such as assigned IP address for the Handset, IP address of the HA and so on.
9. The PDSN regards this as a new session (**MEI=0** and IMSI is a not currently assigned to a session) and sends the RRQ to the HA.
10. The HA now sees a RRQ with no existing binding (as it was revoked in step (6)), and with parameters in the RRQ and considers it a static-assigned MN.
11. The HA sends a Code-139 (administrative prohibited) back to the MN.

With Selectable FA Revocation, the Hybrid PDSN/FA will go through the above conditions and send the revocation to the Home Agent. However, in this case the HA ignores the revocation, but sends a RR response to the PDSN.

As a result, the MN and Home Agent still have a binding state but the PDSN/FA no longer has a PPP session/visitor table entry. Eventually, the mobile goes active and has Data Ready to Send, where the 1x RF channel **DRS=1** is included. In this scenario, the VLR is not queried and the OpenRP message to the PDSN has **MEI** set to 1. Regardless of the MEI value, the PDSN will initiate PPP, and send a RRQ with the previously assigned home address. In this case HA will accept the Re-registration.

Configuring Selective FA Revocation

Perform the following tasks to configure Selective FA Revocation:

Command	Purpose
`Router(config)# ip mobile home-agent revocation ignore` *fa acl*	Enables the HA to send a revocation acknowledgement to the PDSN/FA but not delete the binding. *fa-acl* is either a acl number *1-99*, or a name.

Here is an example of the **ip mobile home-agent revocation ignore** command:

You can ignore revocation from the FA by specifying the **standard** access-list number or **standard** access-list name.

Configuring access-list name to ignore the requests from COA 5.1.1.4

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard fa_acl1
Router(config-std-nacl)#permit 5.1.1.4
```

Configuring access-list number to ignore the requests from COA 5.1.1.5

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit 5.1.1.5
```

Configuring access-list name to selectively ignore requests from FA 5.1.1.4 . This is to associate the above created acl with the **ip mobile home-agent revocation ignore** command.

```
Router((config)#ip mobile home-agent revocation ignore ?
  <1-99>  fa Access-list number
  WORD    fa Access-list name
Router(config)#ip mobile home-agent revocation ignore fa_acl1
```

Configuring the access-list number to selectively ignore requests from FA 5.1.1.5

```
Router(config)#ip mobile home-agent revocation ignore 1
```

Note **ip mobile home-agent revocation ignore** currently does not support using *1300-1999* (Standard IP access-list number (expanded range).

CHAPTER 9

Dynamic Domain Name Server Updates

This chapter discusses DNS update methods and Server Address assignment, and provides configuration details of those features.

This chapter contains the following sections:

IP Reachability

TIA/EIA/IS-835-D describes dynamic DNS update method by the home AAA server and the Home Agent. DNS update by AAA is applicable to both Simple IP and Mobile IP service, while DNS update by the Home Agent is only applicable to Mobile IP service. The following describes the IP Reachability feature on Home Agent.

When the HA receives an initial Registration Request it sends a RADIUS Access-Request to the Home RADIUS server. If the RADIUS server is configured to request Home Agent-based DNS updates, the Home RADIUS server will include the DNS-Update-Required attribute in the RADIUS Access-Accept message returned to the HA. If the initial Mobile IP registration is successful, the HA sends a DNS Update message to the DNS server to add an A Resource Record for the MS. The HA sends a DNS Update message to the primary and secondary DNS server, if present.

When the HA receives a Mobile IP RRQ with lifetime timer set to zero, or the Mobile IP lifetime expires, or administrative operations invalidate the mobility binding for the MS, the Home Agent will send a DNS Update message to DNS server to delete the associated Resource Record. The following commands will enable the IP Reachability feature on Home Agent for the specified realm.

Note DNS updates are not sent for each Re-registration.

Note This feature is supported for Proxy Mobile IP flows as well.

The following call flow describes the IP Reachability on Home Agent - mobile registration scenario:

1. Home Agent receives a registration request from the PDSN/FA.
2. Home Agent sends an access request to RADIUS Server. The HA includes DNS Server Update Capability VSA.
3. The RADIUS server sends access accept with DNS Update Required VSA.
4. The HA sends Registration response to the PDSN/FA. If the HA is configured for redundancy, the active Home Agent will sync the binding creation to the standby Home Agent.
5. The HA creates a binding, and sends DNS Update request message to DNS Server
6. The DNS Server creates a DNS entry for the NAI, and sends DNS Update response message to the HA.

The following call flow describes the IP Reachability on Home Agent - Mobile deregistration scenario:

1. Home Agent receives a registration request with lifetime zero from PDSN/FA.
2. Home Agent sends an access request to RADIUS Server, if SA is not stored locally (optional).
3. RADIUS Server sends access accept (optional).
4. Home Agent deletes the binding. Home Agent sends Registration response to PDSN/FA. If Home Agent is configured for redundancy, the active Home Agent will sync the binding deletion to standby Home Agent.
5. Home Agent sends DNS Update request message to DNS Server, to delete the DNS entry.
6. DNS Server deletes the DNS entry for the NAI. DNS Server sends DNS Update response message to Home Agent.

Configuring IP Reachability

To enable this feature for the specified realm, issue the following commands:

	Command	Purpose
Step 1	`Router(config)# ip name-server x.x.x.x`	Specifies the address of one or more name servers to use for name and address resolution.
Step 2	`Router(config)# ip mobile realm @ispxyz1.com dns dynamic-update method word`	Enables the DNS Update procedure for the specified realm. *word* is the dynamic DNS update method name.
Step 3	`Router(config)# ip mobile realm realm dns server primary dns server address secondary dns server address`	Enables you to locally configure the DNS Server address.

To verify that this feature is enabled for a binding, use the following command:

	Command	Purpose
Step 1	`Router# show ip mobile binding`	Displays the mobility binding table.

The following example illustrates the realm configuration for IP reachability:

```
ip ddns update method sit-ha2-ddns2
 DDNS both
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
```

DNS Server Address Assignment

IS835D defines a method to push the home DNS server address to a mobile as an NVSE in a mobileip registration response. This procedure allows the Mobile Station to learn the primary and secondary DNS server address of its home domain.

The RADIUS server will include DNS Server VSA in an access response to the HA during mobile authentication. The HA forms a DNS server NVSE from the DNS Server VSA and adds it to mobileip registration response. If the DNS Server VSA is not received at the time of authentication, and DNS server address is configured locally on the Home Agent will form a DNS server NVSE from the local configuration and add it to mobileip registration response.

The DNS Server VSA and DNS Server NVSE carry primary and secondary DNS IP addresses.

DNS Server VSA will be synced to the standby if the HA is deployed in redundant mode.

To enable this feature for the specified realm, issue the following commands:

ip mobile realm *realm* **dns server assign**

ip name-server x.x.x.x

To locally configure the DNS Server address, issue the following command:

ip mobile realm *realm* **dns server** *primary dns server address secondary dns server address*

To verify that this feature is enabled for a binding, use the **show ip mobile binding** command.

Note If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

Support DNS Remapping on Home Agent

In Cisco Mobile Wireless Home Agent Release 5.0, the Home Agent supports Stateful NAT capability with scaling to the number of subscribers supported by the Home Agent. This involves matching to a specific protocol and port so that DNS requests from a user can be recognized. Once recognized, the destination IP address is modified so that the DNS request is sent to the IP address defined by the operator. Similarly, the response has a source IP address of the DNS server that responded to the request. This is then mapped back to the original address used by the subscriber.

MN is initially configured with a DNS server IP address of the visited network during session setup. Later, MN tries to resolve hostname by sending DNS message to this IP address which cannot reach the destination via the home network (i.e. reverse tunneled to the HA). In order to address this issue, in HA 5.0, “DNS remapping” feature is added.

DNS Redirection with Monitoring

One problem with DNS remapping is when the primary DNS server fails, the DNS query is not redirected on the secondary DNS server configured on the HA. Additionally, the HA does not use a NAT configuration for remapping the destination address of the DNS query to the configured DNS address on the HA.

The DNS Redirection feature, on the top of the existing DNS Remapping functionality, enables the Home Agent to support Stateful NAT capability with scaling to the number of subscribers supported by the Home Agent.

As part of this feature support, the HA now takes care of remapping the destination address as well as DNS servers monitoring for their availability. The HA rewrites the destination IP address of the DNS messages from the MN to a configured IP address of the primary or secondary DNS server, depending on which one is available. If both primary and secondary DNS are available, the primary will play the role of active DNS. If the primary DNS server is unavailable, the HA starts remapping the destination IP address to the secondary DNS server configured on the HA.

This solution solves the potential problem of when a primary DNS server fails; the DNS query needs to be redirected on the secondary DNS server configured on the HA.

The HA uses the functionality of IP SLA to detect the availability of the primary and secondary DNS server from the Home Agent. Since the IP SLA only informs the CP about the connectivity of the monitored node, the CP informs all of the TPs (through IPC) about the connectivity which the CP has received from IP SLA.

If the HA finds the primary DNS server is available, the primary DNS server is used as an active DNS server and used for remapping the DNS queries coming from the FA on the tunnel. If primary DNS server is down, the secondary DNS server is used as an active DNS server for remapping DNS queries. In case when both primary and secondary DNS servers are reachable from the Home Agent, the primary server is used for DNS remapping. Additionally, if the secondary DNS server is the active DNS server, and the primary DNS server comes up or connectivity resumes with the Home Agent, the primary DNS server takes over the role of active DNS server again.

Here are some important considerations about this feature:

- When switchover occurs, all pending DNS queries that are awaiting responses at the HA from the DNS server are lost on the new, active HA. Mobile nodes need to resend DNS query in this scenario.
- If the destination address of the DNS query matches with the addresses of the DNS servers configured on the HA, DNS redirection does not come into picture, and the HA treats this packet as a normal data packet.
- There is no need to use a NAT configuration for DNS redirection.

To enable realm-based DNS Redirection perform the following tasks;

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *word* `dns server` *primary DNS ip secondary DNS ip*	Configures the primary and secondary DNS server for a realm.
Step 2	`Router(config)# ip mobile realm` *word* `dns server redirect {all}`	Enables the DNS redirection feature for this realm.

Behavior of Above Two Commands:

- If **ip mobile realm** *word* **dns server redirect {all}**is configured before **ip mobile realm** *word* **dns server** *primary DNS ip secondary DNS ip*, the HA will display the following error message.

Error Message `Error: Primary and Secondary DNS not configured for realm`

- Since DNS redirection feature is realm based therefore only "@" or "@domain" will be valid realm. E.g xyz@domain, xyz or xyz@ will not be a valid realm option. In case of an error, the HA will display the following error message:

Error Message `DNS Redirection is allowed for realm only (e.g. @word)`

- If no command to unconfigure the primary DNS server and secondary DNS server is run for a particular realm, this will automatically disable DNS redirection for that realm.
- When unconfiguring the DNS redirection feature using the **no** version of the **ip mobile realm** *word* **dns server redirect** command, it will not remove the existing binding for that realm from the HA. Only the DNS redirection feature will be disabled

To enable DNS servers monitoring for their availability, configure the following IP SLA CLIs. This set of IP SLA configuration commands are required for all the DNS server nodes which need to be monitored by the HA. These IP SLA commands are existing commands that are available in all 7600 series routers.

	Command	Purpose
Step 1	`Router(config)# ip sla` *`ipsla-number`* `icmp-echo` *`ip-addr`* `frequency` *`freq`*	Assigns a IPSLA number, and configures and IP address that needs to be monitored.
Step 2	`Router(config)# ip sla reaction-configuration` *`ipsla-number`* `react timeout threshold-type immediate action-type trapAndTrigger`	Configures the IP sla to notify if the above configured DNS server is not available.
Step 3	`router(config)#ip sla reaction-configuration` *`ipsla-number`* `react connectionLoss threshold-type immediate action-type trapAndTrigger`	Configures ip sla to notify if the above configured DNS server is available.
Step 4	`router(config)#ip sla enable reaction-alerts`	Configures the ip sla to generate notification for availability and unavailability of DNS servers configured above.
Step 5	`router(config)#ip sla sch` *`ipsla-number`* `start-time now life forever`	Configures the ip sla to start monitoring configure DNS server configured above.

Where:

- ipsla-number—IP SLA number that has been assigned for checking the DNS server.
- ip-addr—The IP address of the DNS server.
- freq—The frequency of the probe in seconds (default 60).

DNS Query Matching PDNS or SDNS

This section explains the redirection behavior when the DNS query matches either the configured PDNS or SDNS.

Requests matching PDNS:

If the DNS request matches the PDNS and if it is alive, then that request is skipped. But if PDNS is down, then the request is redirected to SDNS, if it is active. Otherwise the request is ignored (treated as a normal data packet).

Requests matching SDNS:

The behavior pertaining to requests matching SDNS is controlled through the configuration CLI. The following is the CLI used to configure DNS redirect:

ip mobile realm *@realm* **dns server redirect** {**all**}

When **redirect** alone is configured, the requests that are sent to SDNS are not redirected, if it is up. They are sent to SDNS server only. Other DNS requests are redirected to PDNS.

When **redirect all** is configured, all the DNS requests (including the requests that are matching the configured SDNS IP) are redirected to PDNS.

Monitor DNS servers Through IP SLA

Whenever IP SLA detects a connection loss or a connection up event with any of the configured primary and secondary DNS servers, it invokes the registry API on the CP. When the CP gets the notification, it notifies all of the TPs through IPC about this event. When the TPs get this notification from the CP, it sets the active DNS between the primary DNS and secondary DNS.

DNS Redirection supports redundancy. After a switchover, when HA becomes active, it starts monitoring the configured DNS servers for their availability. When any DNS query comes it is remapped to the configured DNS server on the HA.

The only limitation is when a switchover occurs, all pending DNS queries that are awaiting DNS responses at the HA will be lost on the new, active HA. The mobile nodes need to resend a DNS query in this scenario.

Examples

The following example illustrates how to configure a User profile for DNS:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-DNS-Server-IP-Address = 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
    CDMA-DNS-Update-Required = "HA does need to send DNS Update"
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

Here is a sample configuration of the DNS server address assignment realm:

```
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
```

The following example illustrates how to configure the same in AR user profile:

```
set  CDMA-DNS-Server-IP-Address 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
```

The ones marked in **bold** text are primary and secondary DNS server address.

Here is a sample configuration of both IP Reachability and DNS Server Address Assignment:

```
ha2#show run
Building configuration...

Current configuration : 10649 bytes
!
! Last configuration change at 22:45:21 UTC Fri Nov 11 2005
```

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
!
hostname tb1-6513-ha2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius MOT
 server 150.2.0.1 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group MOT
aaa authorization config-commands
aaa authorization ipmobile default group MOT
aaa authorization network default group MOT
aaa authorization configuration default group MOT
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 3
aaa accounting network ha start-stop group MOT
aaa accounting system default start-stop group MOT
!
aaa server radius dynamic-author
 client 150.2.0.1
 server-key cisco
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
ip dfp agent ipmobile
 port 400
 interval 15
 inservice
!
ip ftp source-interface GigabitEthernet0/0.10
ip ftp username root
ip ftp password pdsnmwg
no ip domain lookup
ip name-server 10.77.155.10
ip name-server 1.1.1.1
ip name-server 6.6.6.6
no ip dhcp use vrf connected
no ip dhcp conflict logging
ip dhcp ping packets 0
!
ip dhcp pool Subnet-Pool1
   utilization mark high 75
   utilization mark low 25
   origin dhcp subnet size initial /30 autogrow /30
!
```

```
!
ip vrf forwarding
!
ip vrf ispxyz
!
ip vrf ispxyz-vrf1
 rd 100:1
!
ip vrf ispxyz-vrf2
 rd 100:2
!
!
ip ddns update method sit-ha2-ddns1
 DDNS both
!
ip ddns update method sit-ha2-ddns2
 DDNS both
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group testsip1-l2tp
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 l2tp tunnel hello 0
!
username user-ha2 password 0 cisco
!
!
!
interface Tunnel10
 no ip address
 ip access-group 150 in
!
interface Loopback0
 ip address 20.20.225.1 255.255.255.0
!
interface Loopback1
 description address of the LNS server
 ip address 20.20.206.20 255.255.255.0
!
interface Loopback2
 ip address 170.12.0.102 255.255.0.0
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/0.10
 description TFTP vlan
 encapsulation dot1Q 10
 ip address 10.77.155.5 255.255.255.192
 no ip route-cache
 no snmp trap link-status
 no cdp enable
!
interface GigabitEthernet0/0.172
 description HAAA interface
```

```
 encapsulation dot1Q 172
 ip address 170.2.0.20 255.255.0.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 170.2.0.102
 standby 2 follow sit-ha2
!
interface GigabitEthernet0/0.202
 description PI interface
 encapsulation dot1Q 202
 ip address 20.20.202.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.202.102
 standby 2 ip 20.20.204.2 secondary
 standby 2 ip 20.20.204.3 secondary
 standby 2 ip 20.20.204.4 secondary
 standby 2 ip 20.20.204.5 secondary
 standby 2 ip 20.20.204.6 secondary
 standby 2 timers msec 750 msec 2250
 standby 2 priority 130
 standby 2 preempt delay minimum 180
 standby 2 name sit-ha2
!
interface GigabitEthernet0/0.205
 description REF interface
 encapsulation dot1Q 205
 ip address 20.20.205.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.205.102
 standby 2 follow sit-ha2
!
interface Virtual-Template1
 description To be used by VPDN for PPP tunnel
 ip unnumbered Loopback1
 peer default ip address pool LNS-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool LNS-pool 7.0.0.1 7.0.0.255
ip local pool ispxyz-vrf1-pool 50.0.0.1 50.0.0.255
ip local pool mobilenodes 40.0.0.1 40.0.100.255
ip default-gateway 10.77.155.1
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.202
ip route 10.77.139.29 255.255.255.255 10.77.155.1
ip route 150.2.0.0 255.255.0.0 170.2.0.1
no ip http server
!
!
```

```
ip mobile debug include username
ip mobile home-agent template Tunnel10 address 20.20.202.102
ip mobile home-agent revocation timeout 5 retransmit 4
ip mobile home-agent dynamic-address 20.20.202.102
ip mobile home-agent accounting ha broadcast lifetime 3600 replay 8 suppress-unreachable
unknown-ha deny
ip mobile home-agent redundancy sit-ha2 virtual-network address 20.20.202.102
periodic-sync
ip mobile radius disconnect
ip mobile virtual-network 50.0.0.0 255.0.0.0
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai mwts-pmp-r20sit-base-user1@ispxyz1.com virtual-network 40.0.0.0
255.0.0.0 aaa load-sa lifetime 600
ip mobile host nai @ispxyz2.com address pool local mobilenodes virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 180
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server 10.77.155.10 1.1.1.1
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server assign
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns dynamic-update method
sit-ha2-ddns1
ip mobile realm @ispxyz2.com vrf ispxyz-vrf2 ha-addr 20.20.204.6
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
ip mobile secure foreign-agent 20.20.201.10 20.20.201.100 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
ip mobile secure foreign-agent 20.20.210.10 20.20.210.100 spi 100 key ascii cisco replay
timestamp within 5 algorithm md5 mode prefix-suffix
ip mobile secure home-agent 20.20.202.10 20.20.202.95 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
!
ip radius source-interface Loopback2
no logging trap
logging source-interface GigabitEthernet0/0.201
access-list 150 permit ip host 40.0.0.1 host 20.20.205.220 log
access-list 150 permit ip host 20.20.205.220 host 40.0.0.1 log
access-list 150 deny   ip any any log
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 150.2.0.100 version 2c private
snmp-server host 150.2.0.100 public
no cdp run
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server host 150.2.0.1 auth-port 1645 acct-port 1646 key 7 121A0C041104
radius-server host 150.2.0.100 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 4
radius-server timeout 2
radius-server deadtime 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
alias exec shc sh cdma pdsn
alias exec ua undebug all
alias exec ui undebug ip packet
```

```
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
line vty 5 15
 exec-timeout 0 0
!
!
end

ha2#
```

CHAPTER 10

Per User Packet Filtering

This chapter discusses Per-User Packet Filtering and its implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

Mobile-User ACLs in Packet Filtering

The Home Agent supports per user packet filtering. This feature provides that for a successfully authenticated registration request, the RADIUS server will return “inACL” and “outACL” attributes in an access response to the HA. “inACL” and “outACL” attributes identify the pre-configured ACLs on the HA that are applied to mobility bindings. An input ACL will apply to traffic from the user leaving the tunnel. An output ACL will apply to traffic sent to the user using the tunnel. The attributes will be synched to the standby HA during normal sync and bulksync operation.

ACLs applied to a mobility binding can be displayed by **show ip mobile binding** command. Only the ACLs downloaded at the time of initial authentication will be applied. An ACL downloaded at the time of mobile re-authentication, for lifetime renewal, will not be applied.

The HA will accept one input ACL name and one output ACL name for each user.

Only named extended access-lists are supported for this feature

Note There is significant performance degradation when mobile user ACLs are applied to a large number of mobility bindings.

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.

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)# interface tunnel 10`
`ip access-group 150 in -------> apply access-list 150`
`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`
 	
`ip mobile home-agent template tunnel 10 address 10.0.0.1`
	Configures a tunnel template.
	Configures the ACL.
	
	Configures a Home Agent to use the template tunnel.

Verifying ACLs are Applied to a Tunnel

Here is example output of the **show ip mobile binding** command:

ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
user1-flow8@abc.com (Bindings 1):
    Home Addr 30.0.0.5
    Care-of Addr 7.0.0.2, Src Addr 7.0.0.1
    Lifetime granted 00:03:20 (200), remaining 00:03:03
    Flags sBdmg-T-, Identification CB32792C.A7E22A29
    Tunnel0 src 7.0.0.242 dest 7.0.0.2 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Acct-Session-Id: 0x0000009D
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes
```

In/Out Access List Per NAI/Realm

HA R5.0 supports upstream/downstream (in/out) ACLs for a mobile user if the HA receives the ACL names in the access-response message from AAA. But, if AAA does not send ACL names in the access-response, it is not possible to have in/out ACL applied for a mobile user. HA R5.1 supports in/out ACLs per tunnel using tunnel template, but this is applied on all users on the tunnel. It is not possible to apply ACLs only to specific users or to a set of users.

- This feature supports configuration of in/out ACL names per realm/NAI. The ACLs corresponding to the ACL names are configured by using the **ip access-list extended** *acl-name* command.
- If the ACL is modified/updated/created/deleted after associating the ACL name to realm/NAI, the modifications are applied immediately to the mobile users that are using this particular ACL.
- If the in/out ACL name associated with a realm/NAI is modified/added, then the new ACL will be applied to all the current bindings that belong to the realm/NAI.
- If the in/out ACL name associated with a realm/NAI is deleted, then the deleted ACL will not be applied to the current bindings that belong to the realm/NAI.
- Irrespective of whether in/out ACL name is configured for a realm/NAI, if the HA receives in/out ACL names in an access-response message, then the ACL names received from AAA are applied to the mobile user.

Configuring the In/Out Access List Per NAI/Realm Feature

To enable the In/Out Access List per NAI/Realm feature in Cisco HA Release 5.1, perfrom the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *nai* | *realm* `in-acl` *in-acl-name* `Router(config)# [no] ip mobile realm` *nai* | *realm* `out-acl` *out-acl-name*	?????

Limitations and Restrictions

- Only named extended ACLs are supported for configuring the in/out ACLs per realm/NAI.
- Only ACL names received in the first successful access-response for the session are applied. ACL names from the subsequent access-responses are not considered.

CHAPTER 11

Home Agent Security

Security

This chapter discusses the concepts that comprise the Security features in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

3 DES Encryption

The Cisco Home Agent includes 3DES encryption, which supports IPSec on the HA. On the Cisco 7600 platform, the SAMI utilizes the Cisco VPN-SPA 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.

Note This feature is only available on the 7301 Router platform.

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 The Cisco IOS IPSec feature is available on the Cisco 7600 switch platform. 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 platform requires the support of the Cisco IPSec Services Module (VPN-SPA), a blade that runs on the Catalyst 7600 router. VPN-SPA does not have any physical WAN or LAN interfaces, and utilizes VLAN selectors for its VPN policy. For more information on the Cisco 7600 Internet Router visit: http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.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.

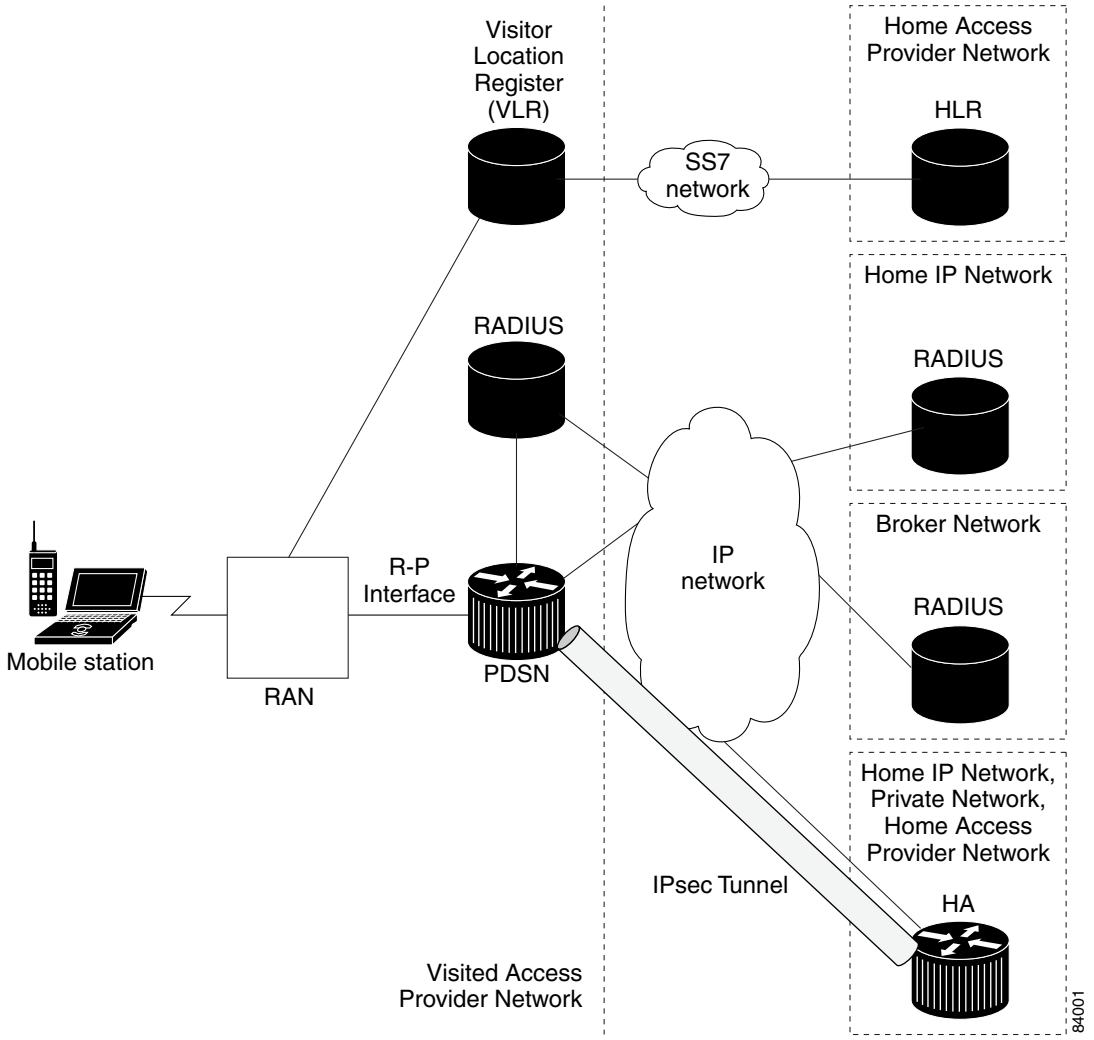
In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy for the MN to the HA.

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 11-1 illustrates the IS835 IPSec network topology.

Figure 11-1 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.

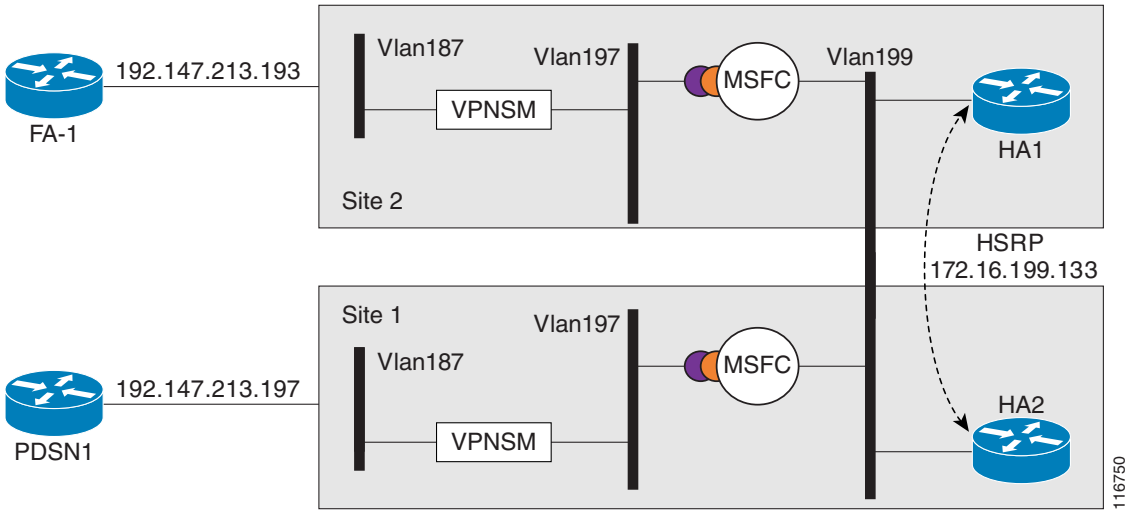
The change in the configuration allows for IPSec connections for the Home Agent IP address but still terminated by the VPNSM.

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 11-2 illustrates a possible configuration:

Figure 11-2 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 10.0.0.0 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 10.0.0.1
 set transform-set mobile-set1
 match address 131
!

interface Loopback21
 description corresponds to ha-on-proc3
 ip address 10.0.0.50 255.255.255.255
!
```

```
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 10.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap
!
interface Vlan137
 description internal vlan to HA3
 ip address 10.0.0.1 255.255.0.0
!
interface Vlan139
 no ip address
 crypto connect vlan 136
!

access-list 131 permit ip host 10.0.0.1 host 10.0.0.50
access-list 131 permit ip host 10.0.0.50 host 10.0.0.1
access-list 131 permit ip 10.0.0.0 0.0.0.255 10.0.0.0 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 10.0.0.2
!
```

IPSec Support on the Cisco 7600 with 6 CPUs of SAMI

An IPSec tunnel may be required to be established over the mobile IP tunnel between the PDSN and the HA. The PDSN resides in the foreign network and the HA in the home network. As per IS-835B specification, IPSec connections are always initiated from the PDSN towards the HA. The IPSec tunnel endpoints are thus, the PDSN IP address and the HA IP address.

In Cisco's 7600 HA solution, IPSec is terminated at the SUP, while the actual HA application resides on the SAMI card(s). Each SAMI card has 6 CPUs, each running one HA instance. Each HA has its own IP address. If different IP addresses are used in the SUP as IPSec endpoints, and in SAMI for HA endpoints, IKE messages generated from the PDSN with HA IP addresses are dropped at the SUP.

To avoid this issue, the above requirement is achieved by letting the SUP own the same IP address that is configured as the HA IP address on SAMI. The requirement is to split the IPSec traffic for different HA IP addresses across separate IPSec VLANs so that each PDSN-HA pair is handled appropriately. This configuration will allow the SUP to support all the 6 CPUs on the SAMI card running the HA application, each owning an IP address that is the IPSec endpoint.

The VRF IPSec feature on the SUP720 is used in this case. All traffic coming from the PDSN will be put on different VLANs based on the HA IP address. Each VLAN corresponds to one VRF and one VRF exists per HA instance on the SUP. Thus, the VRF mode of IPSec is used in this case to split traffic between the 6 different HA instances present on the SAMI. Once the packets are decrypted by the crypto VLAN, packets are then policy routed using an internal VLAN that corresponds to the particular HA to the correct HA CPU on SAMI.

IPSec redundancy across chassis and within a single chassis is supported for this.

The following call flow describes this behavior:

1. IPSec security association (SA) is opened between each PDSN and HA IP address pair on the SUP. IKE messages are sent from the PDSN with its IP address and peer IP address as the particular HA IP address. Based on the PDSN IP address and the HA IP address in the IKE message, the correct ISAKMP profile is selected for the PDSN-HA pair that indicates the VRF for the pair. This establishes different SPIs corresponding to the PDSN-HA pair.
2. One VLAN per HA IP address is defined and it belongs to a VRF that is defined for that IP address on the SUP. Thus, the SUP owns the HA IP address and it is the IPSec terminating point for PDSN.
3. Once an IPSec SA is established between each PDSN-HA IP address pair, encrypted packets are put on to the correct VRF based on the SPI of the incoming packet.
4. Once the encrypted packets are decrypted at the IPSec VLAN corresponding to the HA address, the packets are then policy routed to the corresponding CPU on the MWAM card that hosts the HA IP address using the internal VLAN present between SUP and the HA instance on MWAM.
5. In the return path, packets from HA instances on SAMI are placed on the internal VLAN and put on to the corresponding IPSec VLAN for the HA. This enables the packet to get encrypted and then send out to PDSN via the outgoing interface.

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.

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.

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
Step 1	`Router(config)# ip mobile secure {host | visitor | home-agent | foreign-agent | proxy-host} {lower-address [upper-address] | nai string} {inbound-spi spi-in outbound-spi spi-out | spi spi} key {hex | ascii} string [replay timestamp [number] algorithm md5 mode prefix-suffix]`	Specifies the security associations for IP mobile users.

Configuring IPSec for the HA

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

	Command	Purpose
Step 1	`Router(config)# crypto map map-name seq-num ipsec-isakmp`	Creates a a crypto map entry for one HA in one Crypto-map set.

	`set peer ip address of ha`
	`set transform-set transform-set-name`
	`match address acl name`
		The Crypto Map definition is not complete until:
		1. ACL associated with it is defined, and
		2. The Crypto-Map is applied on the interface. You can configure Crypto MAP for different HAs by using a different sequence number for each HA in one crypto-map set.

	`crypto map map name local-address interface`	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.

	Command	Purpose

Step 2	`Router# access-list acl-name deny udp host HA IP addr eq mobile-ip host PDSN IP addr eq mobile-ip`
	
	`access-list acl-name permit ip host PDSN IP addr host HA IP addr`
	
	`access-list acl-name deny ip any any`
		Defines the access list.
		
		The ACL name "acl-name" is same as in the crypto-map configuration.

Step 3	`Router# Interface Physical-Interface of PI interface`
	
	`crypto map Crypto-Map set`
		Applies the Crypto-Map on Pi Interface, as the HA sends/receives Mobile IP traffic to/from PDSN on this interface.

Creating Active Standby Home Agent Security Associations

The following IOS command displays active standby Home Agent security associations:

	Command	Purpose

Step 1	`Router(config)#show ip mobile secure ?`
	
	`foreign-agent`
	`home-agent`
	`host`
	`summary`
		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:

```
Router# 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#
```

Configuration Examples

Home Agent IPSec Configuration

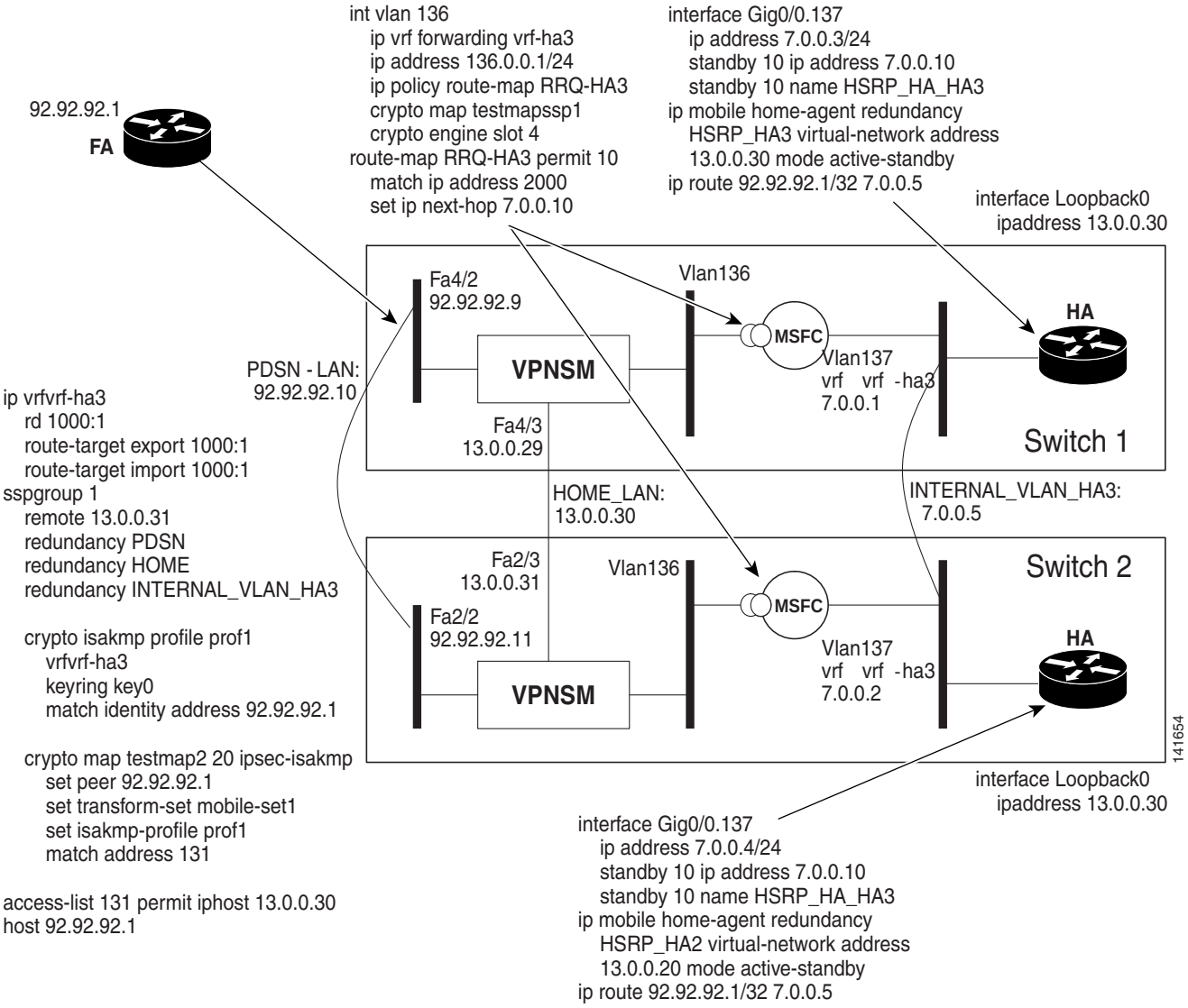
Note Once you permit the hosts/subnets you want encrypted, ensure that you put in an explicit deny statement. The deny statement states do not encrypt any other packets.

Note IPSec on the Cisco Catalyst 6500 amd the 7600 is configured on the Supervisor, rather than on the Home Agent.

Configuration - SUP720 / VRF-IPSec for 6 HA Instances

The following example provides detail of the SUP720 / VRF-IPSec configuration, as illustrated in Figure 11-3.

Figure 11-3 SUP720 / VRF-IPSec Configuration



SUP Configuration - Switch 1:

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
```

```
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.31
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
```

```
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet4/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet4/4
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet4/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet4/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet4/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet4/2
 ip address 92.92.92.9 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet4/2
 standby 1 track FastEthernet4/3
 standby 1 track FastEthernet4/4
 standby 1 track FastEthernet4/7
 standby 1 track FastEthernet4/9
 standby 1 track FastEthernet4/11
 standby 1 track GigabitEthernet6/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan147
 standby 1 track Vlan156
```

```
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan200
 crypto engine slot 6
!
interface FastEthernet4/3
 ip address 13.0.0.29 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet4/2
 standby 3 track FastEthernet4/3
 standby 3 track FastEthernet4/4
 standby 3 track FastEthernet4/7
 standby 3 track FastEthernet4/9
 standby 3 track FastEthernet4/11
 standby 3 track GigabitEthernet6/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan147
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/4
 ip address 12.0.0.29 255.255.255.0
 duplex half
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet4/2
 standby 2 track FastEthernet4/3
 standby 2 track FastEthernet4/4
 standby 2 track FastEthernet4/7
 standby 2 track FastEthernet4/9
 standby 2 track FastEthernet4/11
 standby 2 track GigabitEthernet6/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan147
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/5
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
```

```
!
interface FastEthernet4/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
 speed 100
 duplex half
!
interface FastEthernet4/7
 ip address 14.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet4/2
 standby 4 track FastEthernet4/3
 standby 4 track FastEthernet4/4
 standby 4 track FastEthernet4/7
 standby 4 track FastEthernet4/9
 standby 4 track FastEthernet4/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet6/1
 standby 4 track Vlan146
 standby 4 track Vlan147
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet4/9
 ip address 15.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet4/2
 standby 5 track FastEthernet4/3
 standby 5 track FastEthernet4/4
 standby 5 track FastEthernet4/7
 standby 5 track FastEthernet4/9
 standby 5 track FastEthernet4/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet6/1
 standby 5 track Vlan146
 standby 5 track Vlan147
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
```

```
 standby 5 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet4/11
 ip address 16.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet4/2
 standby 6 track FastEthernet4/3
 standby 6 track FastEthernet4/4
 standby 6 track FastEthernet4/7
 standby 6 track FastEthernet4/9
 standby 6 track FastEthernet4/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet6/1
 standby 6 track Vlan146
 standby 6 track Vlan147
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet6/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
```

```
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 6
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.1 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet4/2
 standby 12 track FastEthernet4/3
 standby 12 track FastEthernet4/4
 standby 12 track FastEthernet4/7
 standby 12 track FastEthernet4/9
 standby 12 track FastEthernet4/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet6/1
 standby 12 track Vlan146
 standby 12 track Vlan147
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 6
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.1 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet4/2
 standby 13 track FastEthernet4/3
 standby 13 track FastEthernet4/4
 standby 13 track FastEthernet4/7
 standby 13 track FastEthernet4/9
 standby 13 track FastEthernet4/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
```

```
 standby 13 track GigabitEthernet6/1
 standby 13 track Vlan146
 standby 13 track Vlan147
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 6
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.1 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet4/2
 standby 14 track FastEthernet4/3
 standby 14 track FastEthernet4/4
 standby 14 track FastEthernet4/7
 standby 14 track FastEthernet4/9
 standby 14 track FastEthernet4/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet6/1
 standby 14 track Vlan146
 standby 14 track Vlan147
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 6
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.1 255.255.0.0
 standby 15 ip 9.0.0.5
```

```
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet4/2
 standby 15 track FastEthernet4/3
 standby 15 track FastEthernet4/4
 standby 15 track FastEthernet4/7
 standby 15 track FastEthernet4/9
 standby 15 track FastEthernet4/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet6/1
 standby 15 track Vlan146
 standby 15 track Vlan147
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 6
!
interface Vlan167
 description internal vlan to HA6
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.1 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet4/2
 standby 16 track FastEthernet4/3
 standby 16 track FastEthernet4/4
 standby 16 track FastEthernet4/7
 standby 16 track FastEthernet4/9
 standby 16 track FastEthernet4/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet6/1
 standby 16 track Vlan146
 standby 16 track Vlan147
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.2 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
```

```
 standby 250 track FastEthernet4/2
 standby 250 track FastEthernet4/3
 standby 250 track FastEthernet4/4
 standby 250 track FastEthernet4/7
 standby 250 track FastEthernet4/9
 standby 250 track FastEthernet4/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet6/1
 standby 250 track Vlan146
 standby 250 track Vlan147
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
!
ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
```

```
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

SUP Configuration - Switch 2:

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.29
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
```

```
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet2/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet2/5
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet2/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
```

```
!
crypto map testmap5 local-address FastEthernet2/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet2/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet2/2
 ip address 92.92.92.11 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex full
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet2/2
 standby 1 track FastEthernet2/3
 standby 1 track FastEthernet2/5
 standby 1 track FastEthernet2/7
 standby 1 track FastEthernet2/9
 standby 1 track FastEthernet2/11
 standby 1 track GigabitEthernet4/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan147
 standby 1 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/3
 ip address 13.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet2/2
 standby 3 track FastEthernet2/3
 standby 3 track FastEthernet2/5
 standby 3 track FastEthernet2/7
 standby 3 track FastEthernet2/9
 standby 3 track FastEthernet2/11
 standby 3 track GigabitEthernet4/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
```

```
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan147
 standby 3 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/4
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet2/5
 ip address 12.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet2/2
 standby 2 track FastEthernet2/3
 standby 2 track FastEthernet2/5
 standby 2 track FastEthernet2/7
 standby 2 track FastEthernet2/9
 standby 2 track FastEthernet2/11
 standby 2 track GigabitEthernet4/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan147
 standby 2 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
!
interface FastEthernet2/7
 ip address 14.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet2/2
 standby 4 track FastEthernet2/3
 standby 4 track FastEthernet2/5
 standby 4 track FastEthernet2/7
 standby 4 track FastEthernet2/9
 standby 4 track FastEthernet2/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet4/1
 standby 4 track Vlan146
```

```
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan147
 standby 4 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet2/9
 ip address 15.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet2/2
 standby 5 track FastEthernet2/3
 standby 5 track FastEthernet2/5
 standby 5 track FastEthernet2/7
 standby 5 track FastEthernet2/9
 standby 5 track FastEthernet2/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet4/1
 standby 5 track Vlan146
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan147
 standby 5 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet2/11
 ip address 16.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet2/2
 standby 6 track FastEthernet2/3
 standby 6 track FastEthernet2/5
 standby 6 track FastEthernet2/7
 standby 6 track FastEthernet2/9
 standby 6 track FastEthernet2/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet4/1
 standby 6 track Vlan146
```

```
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan147
 standby 6 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet4/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 4
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.2 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet2/2
 standby 12 track FastEthernet2/3
 standby 12 track FastEthernet2/5
 standby 12 track FastEthernet2/7
 standby 12 track FastEthernet2/9
 standby 12 track FastEthernet2/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet4/1
```

```
 standby 12 track Vlan146
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan147
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 4
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.2 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet2/2
 standby 13 track FastEthernet2/3
 standby 13 track FastEthernet2/5
 standby 13 track FastEthernet2/7
 standby 13 track FastEthernet2/9
 standby 13 track FastEthernet2/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet4/1
 standby 13 track Vlan146
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan147
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.2 255.0.0.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 4
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.2 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
```

```
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet2/2
 standby 14 track FastEthernet2/3
 standby 14 track FastEthernet2/5
 standby 14 track FastEthernet2/7
 standby 14 track FastEthernet2/9
 standby 14 track FastEthernet2/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet4/1
 standby 14 track Vlan146
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan147
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 4
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.2 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet2/2
 standby 15 track FastEthernet2/3
 standby 15 track FastEthernet2/5
 standby 15 track FastEthernet2/7
 standby 15 track FastEthernet2/9
 standby 15 track FastEthernet2/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet4/1
 standby 15 track Vlan146
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan147
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.2 255.255.255.0
 no ip redirects
```

```
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 4
!
interface Vlan167
 description internal vlan to HA2
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.2 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet2/2
 standby 16 track FastEthernet2/3
 standby 16 track FastEthernet2/5
 standby 16 track FastEthernet2/7
 standby 16 track FastEthernet2/9
 standby 16 track FastEthernet2/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet4/1
 standby 16 track Vlan146
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan147
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.1 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet2/2
 standby 250 track FastEthernet2/3
 standby 250 track FastEthernet2/5
 standby 250 track FastEthernet2/7
 standby 250 track FastEthernet2/9
 standby 250 track FastEthernet2/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet4/1
 standby 250 track Vlan146
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
 standby 250 track Vlan147

ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
```

```
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

HA Configuration - Switch 1:

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.3 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 track GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.4 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.83 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
```

```
 encapsulation dot1Q 137
 ip address 7.0.0.3 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.14 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.3 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.24 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
```

```
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.3 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.34 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.3 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.44 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 99.99.99.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA Configuration - Switch 2:

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.4 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
```

```
 standby 10 name HSRP_HA_HA2
 standby 10 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.6 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.33 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.4 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.16 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
```

```
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.4 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.26 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.4 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.36 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.4 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
```

```
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.46 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

CHAPTER 12

Home Agent Accounting

This chapter discusses concepts related to Accounting on the Cisco Mobile Wireless Home Agent, and provides details about how to configure this feature.

This chapter includes the following sections:

Overview of 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.

This release supports the following Accounting features:

- Home Agent Accounting in a Redundant Setup
- Packet count and Byte count in Accounting Records
- Additional Attributes in the Accounting Records
- Additional Accounting Methods—Interim Accounting is Supported.

As byte count and packet count is performed on the HA, this accounting feature does not need the SSG in the network to generate full accounting information.

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
- Start-stop, and Interim accounting methods will be supported

- When a mobileip registration reply with an error code is sent for an authenticated NAI (due and if a binding does not exit for the NAI), an accounting stop record will be sent.
- A Watchdog message will be sent with an appropriate reject code for an authenticated NAI if Re-registration fails for an existing binding.

The following attributes are sent in Accounting Records:

- NAI in Username attribute (1)
- MN IP Address in Framed IP Address attribute (8)
- Home Agent IP Address (26/7, 3gpp2 attribute)
- Care-of-address in Tunnel End Point (66)
- Network Access Server (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)
- Acct-Input-Octets (42)
- Acct-Output-Octets (43)
- Acct-Input-Packets (47)
- Acct-Output-Packets (48)
- Acct-Input-Gigawords (52)
- Acct-Output-Gigawords (53)
- Registration flags in “mobileip-mn-flags” cisco-avpair attribute
- Vrf name in “mobileip:ip-vrf” cisco-avpair attribute

Single IP Home Agent Accounting Support

The Single IP Home Agent design supports the underlying ability to run AAA services on the Traffic Processor of the Single IP model. For accounting services, the Radius Accounting executes on the traffic processors. Each traffic processor uses a unique UDP source port when originating Radius traffic. The Radius response has this port as the UDP destination port which is used to identify the Traffic Processor that originated the Radius message.

These messages include **Start**, **Update** and **Stop**.

This feature is only supported on the Cisco 7600 Switch with SAMI blade.

To configure the Single IP HA Accounting support, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# sami balance ports start-port end-port`	This configuration is effective after reload only. It configures the port for a particular processor and sets a port to send accounting messages to AAA. If this command is not configured, then the default ports from 45000 to 46535 get set for the card. The range mentioned in this command should be a multiple of six. **Note** We recommend that you use the default configuration.
Step 2	`router#show sami port-range`	This show command displays the port range that is currently configured. It also shows the port range that will be effective after reload.
Step 3	`router#debug radius`	This debug enables the radius debugs to check whether the accounting packets are being sent to AAA on the desired port.
Step 4	`router#debug aaa accounting`	Enables accounting debug messages.

Here are some configuration examples:

```
Slot4#show sami port-range
Current Start Port range 30000 End port range 35999 Range Per PPC 1000
 Port ranges for
    Processor 3: 30000 to 30999
    Processor 4: 31000 to 31999
    Processor 5: 32000 to 32999
    Processor 6: 33000 to 33999
    Processor 7: 34000 to 34999
    Processor 8: 35000 to 35999

After Reload Start Port range 30000 End port range 35999 Range Per PPC 1000


aaa authentication login default local
aaa authentication ppp default group radius
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa accounting update periodic 1
aaa accounting network default start-stop group radius

ip local pool fasim-pool-82 16.82.0.1 16.82.100.254
ip forward-protocol nd
ip mobile home-agent revocation
ip mobile home-agent dynamic-address 48.48.48.48
ip mobile home-agent accounting default
ip mobile host nai @fasim48.com address pool local fasim-pool-82 virtual-network
16.82.0.0 255.255.0.0 aaa load-sa lifetime 7400

radius-server host 12.1.3.2 auth-port 1645 acct-port 1646 key lab
radius-server vsa send accounting
```

Per Domain Accounting

The Home Agent VRF feature allows you to configure accounting groups, authentication groups and whether accounting is enabled or not as part of the VRF definition. In Cisco Mobile Wireless Home Agent Release 5.0 it is now possible to define the accounting interim update interval timer as part of the per-realm configuration within a VRF.

To enable this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)#` **ip mobile realm** `@xyz.com` **ha-addr** *ip-address* [**aaa-group** [**accounting** *aaa-acct-group* | **authentication** *aaa-auth-group*]] **periodic** *minutes*	Enables a per-realm configuration independent of VRF.
Step 2	`Router(config)#` **ip mobile realm** *@xyz.com* **vrf** *vrf-name* **ha-addr** *ip-address* [**aaa-group** [**accounting** *aaa-acct-group* | **authentication** *aaa-auth-group*]] **periodic** *minutes*	The VRF configuration command is enhanced to include accounting support. The **periodic** keyword defines how interim accounting records are sent at an interval corresponding to the *minutes* value.

Note The per-VRF configuration takes precedence over per-realm configuration, which takes precedence over **aaa accounting update periodic** configuration

The **show** command now includes the periodic minutes parameters in addition to those previously displayed.

Here is an example router configuration for per Domain Accounting:

```
ip mobile host nai @yahoo.com address pool local mypool virtual-network 60.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @cisco.com address pool local hapool virtual-network 65.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @xyz.com address pool local nextpool virtual-network 61.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @abc.com address pool local vrf-pool1 virtual-network 55.1.1.0
255.255.255.0 aaa load-sa
ip mobile realm @yahoo.com aaa-group accounting mylist authentication mylist periodic 2
accounting
```

Accounting Interim Sync

In Home Agent Release 5.0, the following per-session fields are periodically synchronized to the standby Home Agent.

- Input octets
- Output octets
- Input bytes
- Output bytes
- Input octets gigawords
- Output octets gigawords
- Input packet gigawords
- Output packet gigawords

- Data Path Idle Timer

The update interval is configurable in minutes, and is independent of the configuration to send interim accounting update Radius messages.

The information is only sent to the standby if there is a change in value for any of the Input/Output counts.

To enable this feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# redundancy periodic-sync interval` *minutes* `limit cpu` *Percentage cpu Threshold* `rate` *rate*#	Enables periodic updates between the active and standby for accounting counters, and is used to spread the sync messages and uniformly distribute the load over a configured period of time. The default value is **5** minutes. Entering **0** minutes causes redundancy sync to be disabled. When the CPU threshold exceeds the CPU limit, HA will start throttling by sending 500 bindings every 5 seconds. The default threshold is 70 %. It is possible that the rate specified cannot be met due to CPU load or memory thresholds being exceeded. We recommend that you choose an interval that matches well with the max bindings in order to be able to achieve the default sync rate. So choosing **1** minute interval for 500K bindings will not be honored in the calculated rate (the required rate is 8500/s, but max is 5000/s) unless a rate is also specified in the CLI.
Step 2	`Router# show redundancy inter-device`	Displays redundancy statisitics, including • Input octets • Output octets • Input bytes • Output bytes • Input octets gigawords • Output octets gigawords • Input packet gigawords • Output packet gigawords • Data Path Idle Timer
Step 3	`Router#debug redundancy periodic-sync`	Displays Mobile IP stateful session redundancy related periodic-sync debugging information.

Basic Accounting Messages

Home Agent Release 2.1 and above 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 an Accounting Update message, if periodic accounting update message is configured, and when the mobile node changes its point of attachment (POA). For a Mobile IP session, this corresponds to a successful re-registration from a mobile node when it changes its care-of address (CoA). The CoA is the current location of the mobile node on the foreign network. Additionally, the HA sends an accounting update message with correct reject code when re-registration fails for an existing binding.
- Accounting Stop: The HA sends an Accounting Stop message when RRP with error code is sent for an authenticated NAI (except for MobileIP error code 136), due and if binding does not exist for the NAI.

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 the 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).

System Accounting in HA

An accounting-on is sent while a home agent is brought into the service (in other words, at the time of initialization after reloading a box), and if there is no active home agent at that time.

An accounting-off could be sent when the active home agent is taken out of service (graceful or otherwise), and if there is no standby home agent to provide the home agent service. Note that, accounting-off is not guaranteed.

An accounting-off is not sent when the standby home agent is taken out of service (graceful or otherwise).

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

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
Step 1	`Router(config)# ip mobile home-agent accounting list`	Enables HA accounting, and applies the previously defined accounting method list for Home Agent. *list* is the AAA Accounting method used to generate HA accounting records.
Step 2	`Router(config)# redundancy periodic-sync interval`	Controls the periodic sync of binding statistics and remaining idle time for the bindings in a redundancy setup (between the active and standby).
Step 3	`Router(config)# aaa accounting network method list name start-stop group group name`	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.
Step 4	`Router(config)# aaa accounting update newinfo`	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.
Step 5	`Router(config)# aaa accounting system default start-stop group radius`	Enables the HA to send system messages.
Step 6	`Router(config)# ip mobile homeagent switchover aaa swact-notification`	Sends Switchover-Action (swact) Notification after a switchover in Accounting watchdog/stop messages for each MIP session
Step 7	`Router# debug aaa accounting`	Enables debugging of HA Accounting messages.
Step 8	`Router# debug radius` `Router# debug tacacs`	Enables debugging of security protocol specific messages.
Step 9	`Router# debug ip mobile`	Enable Mobile IP related debug messages. Accounting will print debug messages only in case of errors.

HA Accounting Configuration Examples

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 10.3.3.1
ip mobile host 10.3.3.2 3.3.3.5 interface Ethernet2/2
ip mobile secure host 10.3.3.2 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 172.16.162.173 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.

Here is a sample HA Accounting configuration:

ACTIVE HA:

```
router#
router#show run
Building configuration...

Current configuration : 4927 bytes
!
! Last configuration change at 05:12:03 UTC Thu Oct 13 2005
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco7600
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
```

```
!
aaa session-id common
!
resource manager
!
no ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
ip dhcp-server 99.107.0.13
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
!
username cisco7600 password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 description "LINK TO HAAA.................!"
 ip address 150.2.13.40 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 4 ip 150.2.0.252
 standby 4 priority 110
 standby 4 preempt delay reload 300
 standby 4 name cisco1
!
interface FastEthernet1/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.10 255.0.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby 2 ip 7.0.0.2
 standby 2 priority 110
 standby 2 preempt delay reload 300
 standby 2 name cisco
!
interface FastEthernet3/0
```

```
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
 bridge-group 4
 bridge-group 4 spanning-disabled
!
interface Ethernet6/0
 description ""LINK TO REFLECTOR...."
 ip address 99.107.0.19 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 99.107.89.67
 standby 3 priority 110
 standby 3 preempt delay reload 300
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.10 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/4
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/5
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
```

```
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/6
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/7
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Virtual-Template1
 no ip address
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent ip mobile home-agent redundancy
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.67 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
access-list 120 deny   ip 40.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255
access-list 120 permit ip any any
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
dial-peer cor custom
!
!
gatekeeper
```

```
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 password 7 0507070D
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end

router#
```

STANDBY HA:

```
router#
router#show run
Building configuration...

Current configuration : 3995 bytes
!
! No configuration change since last restart
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname cisco7600
!
boot-start-marker
boot system tftp /auto/tftpboot-users/tennis/c7600-h1is-mz.123-3.8.PI2 171.69.1.129
boot-end-marker
!
enable password 7 00445566
!
no spd enable
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
```

```
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
ip subnet-zero
!
!
no ip cef
ip ftp username pdsn-team
ip ftp password 7 pdsneng
ip host PAGENT-SECURITY-V3 32.68.10.4 38.90.0.0
ip name-server 11.69.2.133
no ip dhcp use vrf connected
!
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
username mwt13-7600b password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
 no ip route-cache
!
interface FastEthernet0/0
 ip address 4.0.10.2 255.0.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 no ip address
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet2/0
 description "LINK TO HAAA.................!"
 ip address 15.2.13.20 255.255.0.0
 no ip route-cache
 duplex full
 no cdp enable
 standby 4 ip 15.2.0.252
 standby 4 name cisco1
!
interface FastEthernet5/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.67 255.0.0.0
```

```
 no ip route-cache
 duplex full
 standby 2 ip 7.0.0.2
 standby 2 name cisco
!
interface Ethernet6/0
 description "LINK TO REFLECTOR....!"
 ip address 22.107.0.12 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 22.107.89.67
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.2 255.255.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent ip mobile home-agent redundancy
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.10 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
```

```
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane

!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end
```

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: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm disabled
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist
    NAT UDP Tunneling support enabled
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Standby groups
        cisco (virtual network - address 7.0.0.2)
    Virtual networks
        40.0.0.0 /8

Foreign Agent is not enabled, no care-of address
```

```
0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
Radius Disconnect Capability disabled

router#
```

CHAPTER 13

Multi-VPN Routing and Forwarding on the Home Agent

This chapter discusses the functional elements of the Multi-VPN Routing and Forwarding (VRF) CE network architecture, and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

VRF Support on HA

The HA supports overlapping IP addresses 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.

Figure 13-1 VRF-Lite in the Cisco PDSN/Home Agent Architecture

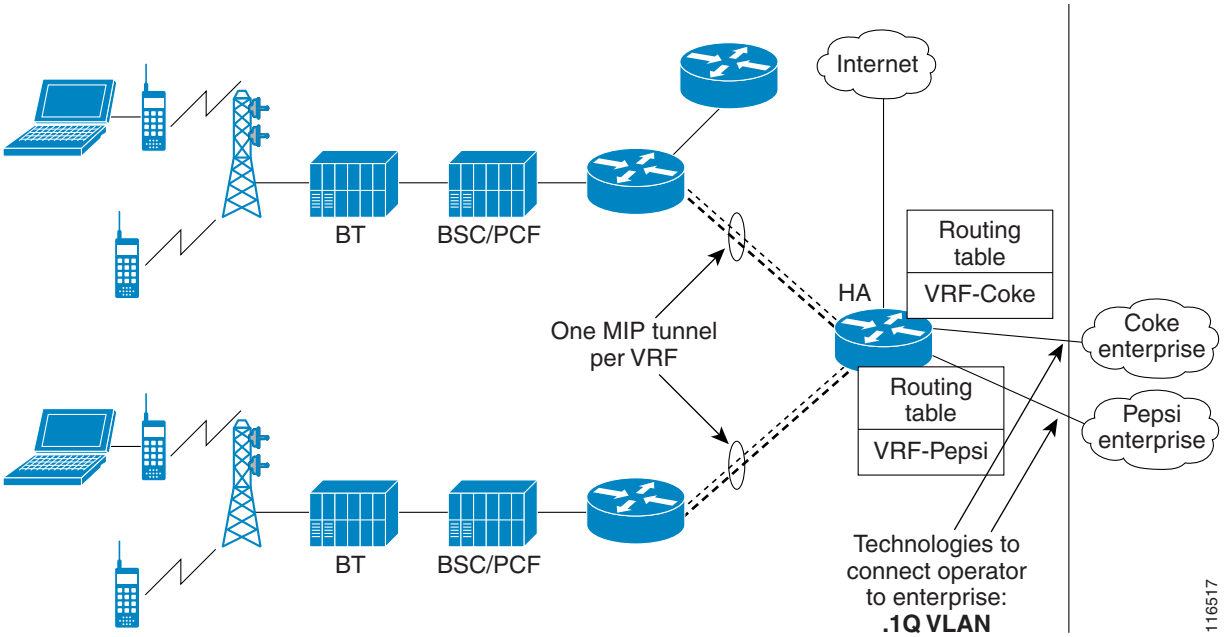


Figure 13-1 illustrates the PDSN architecture and how the VRF-lite solution is applied to the Home Agent for different realms/enterprises, thus segregating data between the enterprises.

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, the 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 Mapping on the RADIUS Server

In Release 3.0, the VRF feature is enhanced to configure the NAI to VRF mapping on the RADIUS server. Mobile to VRF mapping will be learned as follows with this enhancement. When a mobileip registration request is received, the HA sends a radius access request. The AAA server sends access accept with VRF name, in radius attribute “cisco-avpair = mobileip:ip-vrf”, and the corresponding home-agent address in RADIUS attribute “cisco-avpair = mobileip-vrf-ha-addr” to the HA. The Home Agent uses this information to open the binding and associates it with the correct VRF. If the above attributes are not downloaded from AAA server, then the locally configured VRF, if any, is used.

Additionally, an option is provided to send a registration reply with code 136 and a new home agent address, if the HA has to assign a different address than requested by the PDSN/FA. Upon receiving a registration reply with code 136, the mobile sends one more registration request with a new address. The HA will process the request, open a binding, and send a registration reply (success) thus completing the registration process

VRF Feature Restrictions

The following list identifies restrictions for the VRF feature:

- A maximum of 130 VRFs per Home Agent is supported.
- The 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.

Configuring VRF for the HA

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

	Command	Purpose
Step 1	`Router(config)#`**`ip mobile realm`** *`@xyz.com`* **`vrf`** *`vrf-name`* **`ha-addr`** *`ip-address`* [**`aaa-group`** [**`accounting`** *`aaa-acct-group`* | **`authentication`** *`aaa-auth-group`*]]	Defines the VRF for the domain *@xyz.com*. The IP address of the Home Agent that corresponds to the VRF is also defined at the point that the MOIP tunnel will terminate. The IP address of the Home Agent should be a routable IP address on the box. Optionally, the AAA accounting and/or authentication server groups can be defined per VRF. If AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group. If AAA authentication server group is defined, HA-CHAP (MN-AAA authentication) is sent to the server(s) defined in the group.

Step 2	`Router(config)#` **`ip vrf`** *`vrf-name`*
	`description VRF for domain1`
	`rd 10:1`
		Defines the VRF on the box.
		Description of the VRF.
		Router descriptor for VRF. Creates a VRF table by specifying a route distinguisher.
		Note One VRF per domain should be configured on each HA CPU.

Step 3	`router#` **`interface Loopback1`**
	`ip address 192.168.11.1 255.255.255.0 secondary`
	`ip address 192.168.10.1 255.255.255.0`
		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.
		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.

Here is an example of how to configure the User profile for VRF:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    cisco-avpair = mobileip-vrf-ha-addr=20.20.204.2
    cisco-avpair = ip:ip-vrf#0=ispxyz-vrf1
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

VRF Configuration Example

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 172.16.11.1 255.255.255.0 secondary
 ip address 172.16.10.1 255.255.255.0
!
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 10.82.82.2 255.255.0.0
```

```
!
router mobile
!
ip local pool vrf-pool1 10.5.5.1 5.5.5.254 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.1 5.5.5.254 group vrf-pool-grp2
ip classless
ip route 10.15.47.80 255.255.255.255 GigabitEthernet0/1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.1.0.0 255.255.0.0 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 172.16.11.1 aaa-group accounting
vrf-auth-grp1 authentication vrf-auth-grp2
ip mobile realm @cisco.com vrf moip-vrf-grp1 ha 172.16.10.1 aaa-group accounting
vrf-auth-grp2 authentication vrf-auth-grp1
!
!
!
radius-server host 10.15.100.1 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 Example

The following is a sample configuration on a Cisco 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 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 priority 130
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip classless
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
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 10.92.92.3 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 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 10.15.100.1 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 10.15.100.1 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 10.92.92.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
...
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
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 10.92.92.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix ignore-spi
ip mobile secure home-agent 172.16.12.1 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 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
...
end
```

CHAPTER 14

Home Agent Quality of Service

This chapter discusses concepts related to Quality of Service on the Cisco Mobile Wireless Home Agent, and provides details about how to configure this feature.

This chapter includes the following sections:

Overview of HA QoS

Currently, the Home Agent does not support the ability to limit traffic based on rate specified on a per-user basis for various user-subscribed services such as Voice over IP (VoIP), Push-to-Talk (PTT) etc. The per-binding flow policing feature provides the ability to forward packets at rates enforced by a NAI-based user and appropriate for each binding registered on the Home Agent.

Note Per-binding flow means one binding per NAI.

The key benefits of this feature include the following:

- Utilizes the robust Modular QoS CLI (MQC) for performing QoS actions.
- Ensures the original DSCP options are preserved in the downstream packets originated from the internet to the MN, by copying the DSCP from the inner to the outer tunnel header.
- Identifies, classifies, and polices traffic for individual or all users in a realm registered on the Home Agent. This is done for upstream and downstream traffic. The use of MQC allows operators to group user traffic according to a classmap and policymap, and dynamically specify bandwidth requirements at the time of binding flow identification.

QoS Policing

On the Cisco HA, QoS policing is enabled as follows:

Step 1 A user attaches a service-policy to an APN virtual interface recognized by the QoS infrastructure. This is done using the extended **ip mobile realm** command for convenience of performing policing for a group of NAI-based users (on a per-realm basis). This allows a user-configured policymap to be applied to the APN interface, which helps to classify Mobile IP data packets through the HA. Also the peak-rate can be specified to MQC in either input (downstream) or output (upstream) directions.

Step 2 Using MQC classmap/policymap commands, a "match flow pdp" filter is configured that classifies packets for individual flows (bindings) and informs the HA to send police parameters during flow identification. Police rate pdp peak-rate pdp commands, along with the burst values and the various actions needed, are configured under the policy-map, for the class-map for which the match type is flow **pdp**. Peak-rate values for the upstream and downstream are configured using the **ip mobile realm** command.

After the initial RRQ processing, when a binding is registered on the Home Agent, the first packet corresponding to a binding is intercepted in CEF path and policing rules are applied to it. Based on this behavior, police action is invoked on subsequent packets according to configured peak rate, conform burst, and exceed burst values. MQC QoS determines when a user police request has exceeded the configured rate and accordingly permits or drops the packet. For every active binding, a QoS flow exists and a run time state is stored on the HA.

Restrictions

Please note following restrictions:

- Only single-rate policing is allowed. There is no bandwidth reservation, so policing is done based on a maximum bandwidth rate specified by user.
- Once the service policy attachment and police actions are configured they cannot be modified. To modify policy or associated parameters, the existing service policy needs to be removed and a new one configured in its place.
- Policing can be applied only to users registering using a NAI username.
- In the MQC command set when **match flow pdp** is configured for a class only the police command can be configured. Other actions are not allowed.
- There is no traffic shaping feature implemented.

Configuring HA QoS

To enable the HA QoS feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)`**`ip mobile realm`** [*nai* | *realm*] [**service-policy** {**input** *policy-name* [**peak-rate** *rate*] |**output** *policy-name* [**peak-rate** *rate*]}]	Configures a policy and associated rate for one or more user bindings belonging to that policy on the basis of NAI/realm. This can be configured for both upstream and downstream traffic.
Step 2	`Router(conf t)#` **class-map** *class-name*	Specifies a class map name and enters global classmap mode.
Step 3	`Router(config-cmap)#`**match flow pdp**	Classifies HA packets for each binding belonging to a class of MN users with a specified rate.
Step 4	`Router(config-pmap-c)#` **police rate pdp** [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]	Invokes a specified police action on a binding flow. **peak-rate pdp** keywords ensure that policing is done based on the rate specified for each binding flow.

The above configuration details have the following restrictions:

- You cannot remove one of the policies (either input or output) if both policies are configured.
- You cannot modify the existing service-policy for a realm without unconfiguring and then configuring it.
- You cannot configure output-policy first, and then input policy.

QoS Configuration Examples

Here is a configuration example for the QoS feature on the Cisco Mobile Wireless HA:

```
class-map match-all class-mip
 match flow pdp

policy-map policy-mip-flow
 class class-mip
   police rate pdp burst 1400  peak-rate pdp peak-burst 1700
     conform-action transmit
     exceed-action drop
     violate-action drop

ip mobile realm @cisco.com service-policy input policy-mip-flow peak-rate 9000 output
policy-mip-flow peak-rate 8000
```

Verifying the Configuration

To dislay various statistics for the HA QoS feature, perform the following tasks:

	Command	Purpose
Step 1	Router#**show ip mobile binding police nai** *@example.com*	Displays when QoS policing is enabled, statistics for each individual binding, and is provided as an extension to the existing **show ip mobile binding** command. Details such as police rate in bps, and the packets that have conformed, exceeded, or violated the rate are displayed.
Step 2	Router# **show policy-map apn realm** *string*	Displays aggregate statistics on a per-realm basis.

Show Command Examples

The following examples display QoS binding statistics and aggregate statistics:

```
Router#sh ip mob bind police nai mip-qos-user1@cisco.com:
Mobility Binding List:
Total number of QoS bindings is 1
mip-qos-user1@cisco.com:
Downlink Policing

      police:
          rate 8000 , bc 1400 bytes
         peak-rate 9000, be 1700 bytes
        conformed 3000 packets, 312000 bytes; actions:
          drop
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
Uplink Policing

      police:
          rate 8000 , bc 1400 bytes
         peak-rate 8000, be 1700 bytes
        conformed 6000 packets, 516000 bytes; actions:
          drop
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
Router#

Router#sh policy-map apn realm cisco.com
 APN 566497294

  Service-policy input: toMN

    Class-map: HA4.0 (match-all)
      1 packets, 118 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: flow pdp
      police:
          rate pdp, bc 1400 bytes
         peak-rate pdp, be 1700 bytes
        conformed 0 packets, 0 bytes; actions:
```

```
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          violated 0 packets, 0 bytes; actions:
            drop

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: any

    Service-policy output: fromMN

      Class-map: HA4.0 (match-all)
        1 packets, 100 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: flow pdp
        police:
            rate pdp, bc 1400 bytes
           peak-rate pdp, be 1700 bytes
          conformed 1 packets, 100 bytes; actions:
            transmit
          exceeded 0 packets, 0 bytes; actions:
            drop
          violated 0 packets, 0 bytes; actions:
            drop

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Match: any
  Router#
```

CHAPTER 15

Monitoring User Traffic

This chapter discusses how to monitor upstream and downstream user traffic using the Hotlining feature, and provides details on how to configure the feature on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

Hot-lining

Hot-Lining provides a wireless operator with the capability to efficiently address issues with users that would otherwise be unauthorized to access packet data services. When a problem occurs such that a user may no longer be authorized to use the packet data service, a wireless operator using this feature may Hot-Line the user, and upon the successful resolution of the problem, return the user's packet data services to normal once the hot-lined condition is resolved. When a user is Hot-Lined, their packet data service is redirected to a Hot-Line Application which may notify (if feasible) the user of the reason(s) that they have been Hot-Lined and offers them means to address the reasons for Hot-Lining, meanwhile blocking access to normal packet data services.

HA support Profile based hot-lining with Filter/IPRedirection/HTTPRedirection by using Active and New session hot-lining for 3gpp2/wimax environment subscribers.

HA Release 5.1 does not deal with Rule based hot-lining for both 3gpp2/Wimax environment with Active and New session hotlining. HA5.1 does deal with IS835-D and NWG 1.3.1 Stage 2 standards for Hot-lining support.

In HA Release 5.1, there is one style of hot-lining is supported on HA which will be triggered by the HAAA to indicate that a user be hot-lined:

- In profile-based hot-lining, IP or HTTP, or both redirection rules are configured under a profile on the HA. The HA performs hot-lining after it receives the Filter-Id from the home AAA in either an Access-Accept, or a COA. The HA sends the hot-line capability parameter in the Access-Request message.

Note The Filter-ID matches one of the profiles on the HA.

Additional Hot-Lining Features

On the Home Agent, the hot-lining policy is applied only when the policy is downloaded during HA CHAP. The Home Agent will reject the RRQ if Reverse-Tunnel is not requested by the user and hot lining policy is downloaded for the user.

Note There is no MIB support planned for this feature.

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.

New Session Hot-Lining

Here is the process by which a new session is hot-lined.

Step 1 The HAAA receives a signal from the hot-lining application to hot-line a user's packet data service.

Step 2 The HAAA records this information in its user profile store. If the user is not active, the HAAA waits until the user initiates the packet data service, which causes the user to be hot-lined immediately. Meanwhile, it is possible for the hot-line application to change the user's hot-line status back to normal, in which case the HAAA updates the user profile, and stores it accordingly.

Step 3 When the user who is to be hot-lined initiates a packet data session, a RADIUS access-request is received by the HAAA that indicates the hot-line capability of the HA.

Step 4 In the HAAA, the local policies and received hot-line capability parameter is used to determine which HA receives the hot-lining VSAs. The HAAA signals the hot-lining device of the user's hot-line status by sending hot-lining VSA(s) in the RADIUS Access Accept message. The HAAA may include the hot-line accounting indication VSA in the RADIUS access-accept message.

Step 5 If accounting is enabled on the HA, the HA generates a RADIUS accounting-request (start) packet and includes the hot-line accounting indication VSA if it was received in the RADIUS access-accept message. If the HA is unable to honor the hot-lining VSA(s) received in the RADIUS access-accept packet, it treats the RADIUS access-accept packet as a RADIUS access-reject packet, and terminates session setup.

Step 6 Once a hot-line session starts, traffic is blocked and/or directed to the hot-line application.

Active Session Hot-Lining

The following procedure lists the events for active session Hot-lining:

Step 1 The user is currently engaged in a packet data session that is not hot-lined.

Step 2 The HAAA starts the active session hot-lining procedure when it receives a hot-line signal from the hot-line application for a user that has already started a packet data session.

Step 3 The HAAA stores the hot-line state of the user in the user's profile.

Step 4 In the HAAA, the local policies and received hot-line capability is used to determine which HA receives hot-lining VSAs. The HAAA signals the HA of the user's hot-line status by sending hot-lining VSA(s) or RADIUS filter-id (11) attribute in the RADIUS change of authorization (COA) message. The HAAA may include the hot-line accounting indication VSA in the RADIUS COA message for 3gpp2 environment users.

Step 5 If the HA can honor the request then it responds with a COA ACK packet. If the HA cannot honor the hot-lining request, then the HA responds with a COA NAK message. Based on local policy, upon receiving a COA NAK message with error-cause (101) indicating "Administratively Prohibited (501)", the HAAA may either retry sending the hot-lining signal to the HA, or send a RADIUS disconnect-request message to the HA, or to another device to instruct it to drop the session.

Step 6 An HA capable of generating accounting packets (if accounting is enabled) also generates a RADIUS accounting-request (stop) message to close the current accounting session. The release indicator (F13) is set to 14 (hot-line status changed) for only 3gpp2 environment users.

Step 7 An HA capable of generating accounting packets also generates a RADIUS accounting-request (start) message that includes the hot-line accounting indication VSA received in the COA packet.

Step 8 The hot-lining device then immediately invokes the hot-lining profiles as specified in the COA packet.

Step 9 Once the user has been hot-lined, the hot-line application might notify the user of their hot-lined state, and will interact with the user to rectify the issue that caused the hot-lining. If the hot-lining application is not satisfied with the results, it may maintain the hot-lining status of the user, or it may terminate the users session. If the problem has been rectified the hot-lining application will return the user's session back to a normal mode.

Step 10 The hot-line application will indicate the return to normal status to the HAAA. The interaction of the hot-line application with the user is beyond the scope of this document.

Step 11 The HAAA updates the user's profile.

Step 12 If the session is active, the HAAA sends a COA packet to the HA that is currently applying the hot-line rule. This may not be the same device that initially implemented the hot-line state for the session (a handoff may have happened). If the received notification, of Step 9 indicated session termination from the hot-line application, the HAAA records the termination status of the user in the user's policy store. And if the session is still active, it sends a RADIUS disconnect-request message to an appropriate device. This device may not be applying any hot-line rule. Upon receiving the RADIUS disconnect-message, the device terminates the session. If the device is capable of generating accounting messages, it generates a RADIUS accounting-request (stop) message with release indicator (F13) set to 6 (termination due to resource management).

Step 13 Upon receiving the signal to return the user back to normal mode, if the HA is unable to honor the request it responds with a COA NAK packet. Upon receiving a COA NAK, the HAAA may send a RADIUS disconnect-request message to terminate the use's session. The RADIUS disconnect-request message may be sent to the hot-lining device or to another device that is capable of terminating the session. But, if the hot-lining device is able to return the user back to normal state, it sends a COA ACK packet.

Step 14 If the hot-lining device is capable of generating accounting messages it generates a RADIUS accounting-request (stop) message indicating that the hot-lining session has been terminated, and includes the hot-line-accounting indication VSA if received in the COA message. The release indicator (F13) is set to 14 (hot-line status changed).

Step 15 The RADIUS accounting-request (stop) message is followed by a RADIUS accounting-request (start) message indicating the start of the normal packet data session.

Step 16 The user's session is now returned back to normal.

Redundancy Support for Hotlining

In HA Release 5.0 Redundancy framework/infrastructure is modified to be under CCM and Redundancy Framework Inter-device (RF-Interdev).

HA Release 5.1 supports hotlining by downloading a Hotline profile from AAA server using RADIUS attribute 11. HA 5.1 supports hotlining of both new-session and active-session. HA 5.1 also supports hotlining using Change of Authorization messages (COA).

Additionally, HA Release 5.1 supports redundancy for all the above.

The following Hotlining information of binding is synced to standby:

- Hotlining Status—Specifies the current status (Active/Normal) of the binding.
- Hotline Profile(s)—Specifies the hot-lining profile(s) downloaded from AAA using either Radius attribute 11.
- Session-Timeout—Indicates the maximum number of seconds of service to be provided to the user under hotlining.

Additionally, the following information is also synced:

- User-Name—NAI of the user
- Bind address—HoA of the binding.
- Accounting-Session-Id—Accounting Session ID generated by the HA. A new accounting Session ID is generated whenever the user changes the state (from Active to Normal and vice versa).

If the failover occurs and the standby becomes active, it applies the hotline profile to the user. The standby also uses the same Accounting-Session-Id that was synced before failover.

Restrictions and Limitations

The following restrictions and limitations apply to this feature:

- ACL rules that match counters under hotlining are not synced to the standby

Requirements for Hot-Line Capable HA

This section describes the requirements of HA that can be applied to process hot-lining information for MIP flow of a subscriber during Registration/Re-Registration and COA.

1. HA should support both New-Session Hot-Lining and Active-Session Hot-Lining.
2. Hot-Lining should not interfere with the establishment of a packet data session. HA should allow completion of the packet data session and shall allow MIP signaling re-registration. HA shall apply the Hot-Lining rules to DNS traffic and DHCP traffic through relay agent functionality.
   a. During registration of MIP subscriber, if any invalid hot-lining information received by Home-Agent, then HA can reject the RRQ by sending Registration-Reject with "HA-CHAP Failure".
   b. During re-registration of MIP subscriber, HA should retain subscriber MIP Session and as well hot-lining session though the invalid information received in Access-Accept. And, It should reject the RRQ with “HA-CHAP Failure”.
3. HA should include the Hot-line Capability VSA in the RADIUS Access-Request message indicating its ability to support Hot-Lining for MIP subscriber.
4. 4.HA shall treat a RADIUS Access-Accept message as Access-Reject message or shall respond with a COA NAK message with Error-Cause (101) indicating “Administratively Prohibited”(501) when it receives a RADIUS Access-Accept message or COA message that contains:
   a. A RADIUS Filter-Id(11) attribute that it cannot decode.
5. Upon receiving RADIUS Filter-Id(11) attribute(s) in a RADIUS Access-Accept message, HA shall immediately apply the locally provisioned Hot-Line rules that match the one specified by the RADIUS Filter-Id(11) attribute(s).
6. Upon receiving a COA message containing RADIUS Filter-Id(11) attribute(s), HA will locate the Hot-Line rules that match the profile(s) specified by the RADIUS Filter-Id(11) attribute(s). If HA is successful, it should reply to the HAAA with a COA ACK message. HA should remove any previously specified RADIUS Filter-Id(11) attribute(s) and begin applying the rules associated with the newly received RADIUS Filter-Id(11) attribute(s). HA should send accounting messages accounting stop and start messages. If HA is not successful at matching the newly received RADIUS Filter-Id(11) attribute(s) with corresponding rules, it shall send a COA NAK with Error-Cause (101) indicating “Administratively Prohibited”(501). In this case, the Hot-Line state and all existing rules shall remain unchanged.
7. If the HA receives the Session-Timeout (27) attribute it shall terminate the session after the time specified for the session (in seconds) has expired. If HA is capable of RADIUS accounting it shall send a RADIUS Accounting-Request (Stop) message and shall containing the Hot-Lining Accounting Indication VSA if one was received in a RADIUS Access-Accept or COA message.
8. The HA will give priority for the rules that are configured under Profile in the order of HTTP Pass, HTTP Redirection, IPRedirection, IPFilter Rules

9. A Home-Agent that receives the HTTP-Redirection VSA shall monitor the IP flows. When an IP flow matches the "src" and "dst" fields, HA shall apply the rule as specified in the HTTP-Redirection. If the action in the rule is to redirect, HA shall block the traffic and respond to every HTTP request it sees with an HTTP Redirect response (RFC 2616) specifying the URL of the matching HTTP-Redirection Rule VSA.

Limiting the Hot-Lining Duration

Hot-Lined sessions can still utilize expensive network resources, therefore AAA may wish to limit the period over which a session is to be Hot-Lined by sending Session-Timeout atttibute value in either COA or Access-Accept. There are two methods that are available to the operator.

First, a (Hot-Lined or not Hot-Lined) session can be terminated immediately by sending a Disconnect Message. The Disconnect Message is not required to target HA .

Second, the Home RADIUS server should be configured to include the Session-Timeout (27) attribute when it sends the Hot-Lining indication to HA . The Session-Timeout will contain the length of time in seconds varies from 1- (232-1) sec that the user would be allowed to remain in the session. If Session-Timeout expires, the packet data session shall be terminated. This feature will be supported for both profile and rule-based hot-lining.

IP Redirect for Non-Hotlined Users

This feature allows you to configure IP-redirect rules on a per realm basis so that upstream packets can be redirected to the specified IP address. A non-hotlined profile is created and associated with a realm. Under the non-hotlined profile, IP redirect rules are configured.

Once configured, the HA tries to match the packet contents with configured ACL values till Layer-4, and tries to redirect the packets to the configured IP address and port by modifying the destination-ip and destination-port. The destination-port is modified, if the value is configured under profile.

To enable hontlining for non-hotline users, perform the following task:

Command	Purpose
`router(config)# ip mobile home-agent non-hotline profile` *profile-id* `router(non-hotline-rules)# redirect ip access-group {`*100-199 | 2000-2699 | WORD*`} in redirect-ip` *redirect-ip-address* `[redirect-port` *redirect-port*`]`	Enables hotline capability for non-hotline users.

Note This feature is applicable for upstream (MN->Network) traffic only.

Note This functionality is only available for non-hotlined users.

Note NAT functionality must be supported as part of this feature for redirected traffic. This particular functionality is common for both hotlined and non-hotlined user traffic.

Restrictions for Hot-lining

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

- In case of upstream traffic, the HA will intercept the traffic and apply HTTP, IP Redirection and IP Filter Rules for the user. In case of downstream traffic, the HA suppports IP Redirection and IP Filter Rules verification. There is no support for HTTP Redirection on the HA for downstream traffic.
- To enable hot-lining on a router, the router should support mobileip and Home Agent functionality. If the router does not, you can enable **router mobile** on the router, and configure **ip mobile home-agent** in global configuration mode.
- Hot-lining capabilities and configuration for any particular user can be overwritten depending on the order in which the Hot-lining CLIs are entered with the latest hot-lining CLI, taking precedence over the previous one. For example, a user "mip1@cisco.com" may have been configured for Profile-based hot-lining. Later, that can be over-written by Rule-based hot-lining configuration.
- Initially a realm configured with hot-lining capabilities that is applicable to all users falls into that realm. Later, that realm can be overwritten to particular user by configuring the user with hot-lining capabilities.
- IOS has restrictions on CLI configuration and deconfiguration. While configuring the CLI the maximum allowed length is 249 characters. For deconfiguring the CLI, the maximum allowed length is 252 characters.

Note The Home Agent MIB is not updated with the Hot-lining information.

Configuring Hot-Lining

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

Command	Purpose

`Router(config)# [no] ip mobile home-agent hotline ?`
`  profile  defines hotline profiles`
`Router(config)# [no] ip mobile home-agent hotline profile word`
`Router(hotline-rules)#`
 	
`Router(hotline-rules)#?`
`  exit  Exit from hotline profile configuration mode`
`  firewall  Defines Firewall filter Rules`
`  no  Negate the hotline rules`
`  redirect  Redirection Rules`
	Enables you to configure and distinguish profile or rule based hot-lining for each user (MN).
	The **profile** keyword acts as sub-configuration mode to configure a set of rules.

`Router(hotline-rules)# [no] Redirect ip access-group {acl-no | word} {in|out} {redirect ip-addr [port]}`	Specifies that IP is the redirected profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.
`Router(hotline-rules)# [no] Redirect http access-group {acl-no | word} {redir-url url}`	Specifies that HTTP is the redirected profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.

Command	Purpose
`Router(hotline-rules)#[no] firewall ip access-group {acl-no | word} {in|out}`	Specifies that IP firewall is the Profile-based configuration. The configured ACL should be an extended ACL. The acl number ranges from 100-199 and 2000-2699.
`router(config)# ip mobile home-agent non-hotline profile profile-id` `router(non-hotline-rules)# redirect ip access-group {100-199 | 2000-2699 | WORD} in redirect-ip redirect-ip-address [redirect-port redirect-port]`	Enables hotline capability for non-hotline users.

`Router(config)#[no] ip mobile realm {realm | nai} hotline ?`
`capability Hotlining Capability of the mobile hosts`
`redirect Redirect ip address for upstream traffic`
 	
`Router(config)#[no] ip mobile realm { realm | nai} hotline capability ?`
`all Support all Hotline Capabilities`
`httpredir HTTPRedir Rule-based Hot-Lining`
`ipfilter IPFilter Rule-based Hot-Lining`
`ipredir IPRedir Rule-based Hot-Lining`
`profile Profile-based Hot-Lining`
	Configures the hotlining capability of the mobile hose.
	
	Configures either profile, or rule-based hotlining, or all forms of hotlining. The *word* should be specified as **nai | realm**, and in the format of *@cisco.com|username@cisco.com*. Otherwise, this command will give an error message.
	
	At least one form of hot-lining must be selected. There is no default rule to activate rule-based hot-lining for the user. Unconfiguring the command will erase the rule-based hot-lining capability for the user. The values in this configuration are mentioned as flags.
	1 The flag values are explained below.

`Router(config)# ip mobile realm realm hotline capability ipredir`	Configures a profile-based hot-lining for users with IP-redirection rules. Here, the realm can be nai/realm.
`Router(config)#ip mobile realm realm hotline capability httpredir`	Configures a profile-based hot-lining for users with HTTP-redirection rules. Here, the realm can be nai/realm.
`Router(config)# ip mobile realm realm hotline capability rule-based flag`	Configures rule-based hot-lining for users. Here, the realm can be nai/realm.
`router# clear ip mobile traffic`	Clears all ip-mobile related counters for traffic, and clears hotline related counters.

1 The flag values are explained below.

0x00000001 Profile-based Hot-Lining is supported (Using RADIUS Filter-Id attributes)

0x00000002 Rule-based Hot-Lining is supported using Filter Rule

0x00000004 Rule-based Hot-Lining is supported using HTTP Redirection Rule.

0x00000008 Rule-based Hot-Lining is supported using IP Redirection Rule.

For more information related to dynamic ACL configuration, please check the following URL:

http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080430e5b.html

Verifying the Configuration

Perform the following tasks to display various information regarding hotlining on the HA:

Command	Purpose
`Router# show ip mobile hotline[profile profile-id] | summary | users [nai id]`	Displays the hotlined user information for a particular user, or all users eligible for hot-lining.
`Router# show ip mobile hotline users ?` `  nai  MN identified by NAI`	Displays the hot-lined user information for a particular user, or all users eligible for hot-lining.

`Router# show ip mobile hotline profile ?`
`  WORD  Profile-Id`
`  Output modifiers`
	Displays the list of hotline profiles, or particular hotline profile.

`router# show ip mob hot summary`	Displays the list of current statistics of hotline subscribers. This command displays the counters if at least one MIP session should be hot-lined.
`router# show ip mobile traffic [since]`	Incorporates counters for hot-lining sessions (i.e., cumulative counters for number of sessions hotlined, number of active sessions hotlined, number of new session hotlined).

The following is the sample output for hotline user information:

```
HA#show ip mobile hotline users nai mip1@cisco.com
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

HA#show ip mobile hot-lined users
Hotline Binding List:
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

blrmip2@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com
```

The following is sample output for hotline profile information:

```
HA#Show ip mobile hotline profile cisco
Hotline Profile List:
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

HA#show ip mobile hotline profile
Hotline Profile List:
Total 2
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
```

```
    Redirected Url - cisco.com

 Profile: ht-prof1 (Rules 3)
    RuleType IPRedir, Extended ACL Name ht-acl1
    Direction - in
    Redirected IPAddr 16.1.1.102

    RuleType IPRedir, Extended ACL Number 100
    Direction - in
    Redirected IPAddr 1.1.1.1

    RuleType IPFilter, Extended ACL Name cisco
    Direction - out
    HA#
```

The following is sample output for hotline statistics information:

```
HA#sh ip mob hot summary
HomeAgent Hotlining Summary:
    Number of Sessions Hotlined 2
    Number of Profile-Based Hotlined 0
    Number of Rule-Based Hotlined 2
HA#
```

The following is sample output for counters for hot-lining session:

```
HA# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 1351, denied 0, ignored 0, dropped 0, replied 1
    Register requests accepted 1351, No simultaneous bindings 0
    Register requests rcvd initial 149, re-register 1132, de-register 70
    Register requests accepted initial 149, re-register 113, de-register 7
    Register requests replied 1281, de-register 70
    Register requests denied initial 0, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 0, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 14, sent 0 total 0 fail 1351
    Binding Update acks received 0 sent 14
    Binding info requests received 0, sent 1 total 2 fail 1
    Binding info reply received 1 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 1
    Binding Delete Req received 0, sent 0 total 0 fail 0
    Binding Delete acks received 0 sent 0
    Binding Sync Req received 0, sent 0 total 0 fail 0
    Binding Sync acks received 0 sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
    Total incoming registration requests using NAT detect 0
```

```
    Total VPDN Tunnel sessions attempted: 1 success: 1 fail: 0 pending: 0
                               PPP SW IDBs: 1 no resource: 0 deleted: 0


Change of Authorization:
  Request rcvd 0, accepted 0
  Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS 0
    Session Cxt Not Found 0, Session Cxt Not Removable 0
    Unsupported Service 0
Dynamic DNS Update (IP Reachability):
Number of DDNS Update Add request sent 0
  Number of DDNS Update Delete request sent 0
Home Agent Hotlining:
    Number of Hotline Sessions 6
    Number of Active-Session Hotlined 0
    Number of New-Session Hotlined 6
    Number of Active-Sessions Reconciled 0
    Number of New-Sessions Reconciled 0
```

CoA for WiMAX Hotlining

Hot-lining can be applied to a new session through an Access-Accept message. Also, an existing session can be hotlined through a change of Authorization (CoA) packet received from the AAA server.

When a CoA (Change of Authorization) packet is received from the AAA server to the HA with in/out ACLs, the In/Out ACL received in the packet is applied to the Subscriber session that could have commands like allow, deny, or re-direct.

In HA5.0, there is no Hot-lining support for Wimax subscribers. Both rule and profile-based hot-lining applied for 3gpp2 subscribers.

The following table illustrates Hot-Lining support for HA Release 5.0 and HA Release 4.0

Technology	Home-Agent Version	Hot-Lining Type Supported	Hot-Lining Style Supported	Redundancy Support
3G (CDMA)	HA4.0	New & Active Session Hot-Lining	Profile and Rule based Hot-Lining	Available
	HA5.0	No	No	No
4G (Wimax)	HA4.0	No	No	No
	HA5.0	No	No	No

In HA Release 5.1, the Home Agent provides support Hot-Lining of Wimax subscribers. The following sub-sections describe detailed call flows for these scenarios.

- This feature supports Wimax new-session and active-session Hot-lining by downloading one or more filter-id [11] attributes from AAA as part of Access-Accept or COA.
- The downloaded filter-id attribute is mapped to one of the profile-ids that is configured locally on the HA. This profile-id consists one or more IP redirection rule and firewall (filter) rules.
- The HA sends Hotline capability in Wimax-capability as sub TLV to the AAA server.

- The HA supports the standard RADIUS attribute Session-Timeout [27] for maintaining the Hotline session, and this approach is downward compatible with HA 4.0 functionality. The user session is restricted to remain hotlined for the duration specified by the hotline-session-timer.
- Whenever the hotline status is modified for subscriber, the HA sends an Accounting Stop and Start for the session. The HA sends and Accounting Stop message with a previously generated/utilized Accounting-Session-Id before the hotline status is modified. The HA generates a new Accounting-Session-Id for sending Accounting Start after modifying the hotline status for the user.
- The Hot-lined MN session is reconciled by downloading the filter- id [11] as “Hot-Line Normal”, either in an Access-Accept during re-registration, or a CoA.
- Since this feature exists on a Single IP architecture, the CP processes the CoA and sends the “InterimUpdate” to the corresponding TP.

Call Flows for Wimax Hot-Lining

The following call flows explain the New-Session and Active-Session Hot-Lining for WiMAX bindings.

New-Session Hot-Lining for WiMAX bindings

1. HA has to send Wimax capability type from the configured value in Access-Request message to AAA server. Required configuration for this is: **ip mobile realm** *realm* **hotline capability** { *ipredir ipfilter httpredir profile all* }
2. During New-Session Hot-lining, HA can receive one or multiple filter-ids [11] with profile-id values that are configured locally on HA. Profile can be configured locally on HA with below CLI: **ip mobile home-agent hotline profile** *profile-id*
3. If HA receives “session-timeout [27]” as part of Access-Accept, then the user will be allowed to remain in the hotline state for the hotline session timer duration mentioned by this attribute. After that, the user will be disconnected.
4. HA will send Accounting Stop and Start whenever hotline status is modified.

Active-Session Hot-Lining for WiMAX bindings

1. During Active-Session Hot-lining, the HA receives one or multiple filter-ids [11] with profile-id values in a CoA message that are configured locally on the HA using the **ip mobile home-agent hotline profile** *profile-id* command.
2. If the HA downloads “session-timeout [27]” as part of the Access-Accept, users can remain in the hotline session only for the hotline session timer duration.
3. The HA sends an Accounting Stop and Start whenever the hotline status is modified.

Re-Conciliation of WiMAX Hotline Session

The term Re-Conciliation represents when a hot-lined user returns back to a normal state. That means the downloaded profiles are no longer applicable for users.

The hot-lined MN session is reconciled by downloading the filter- id [11] value as “Hot-Line Normal”, either in an Access-Accept during re-registration, or in a CoA.

After reconciling the hotline session, the HA sends and Accounting Stop for the previous generated Accounting-Session-Id, and initiates an Accounting-Start by generating a new Accounting-Session-Id.

Note In HA 4.0, in order to reconcile the hotline session, the HA expects the “3GPP2 Hot-Line Normal” string. In Release 5.1, the string value is modified to “Hot-Line Normal”.

Limitations

The following software limitations are noted:

- Configuring HTTP redirection rules under the hot-lining profile configuration is not applicable for Wimax hot-lining support. You can only use the IPFilter and IPRedirect Rule configuration for Wimax hot-lining. As part of this feature support, configuring the HTTP redirection rule is not supported under profile configuration.
- There is no support for Wimax Hotline-Accounting-Indicator as part of this feature.
- For Wimax hot-lining, Rule-based Hot-Lining Rules and Profile-Id, as defined in NWG R1.1 Stage 3, is not supported.
- The Hot-lined MN session can be reconciled by downloading the filter- ids [11] as “Hot-Line Normal”, either in an Access-Accept during re-registration, or in a CoA.

NAT Translations for Hotlining / Non-Hotlining Redirection

The HA has to maintain the mapping between actual destination IP address of the hot-lined or non-hotlined IP redirected user’s data packet and redirected IP address. Whenever a response is received from the redirected server, the HA modifies the response packet src IP address to an actual destination IP address of the request packet.

To perform the mapping between the actual destination IP address/port to the redirect IP address/port, the HA utilizes the NAT Functionality to maintain the NAT Translations during upstream path.

Packet Processing of Upstream Packets

For upstream packets, the HA intercepts the packets after de-capsulation of the tunnel header, and modifies the packet destination IP address to redirected IP address as defined hotline/non-hotline profile information. In case of TCP or UDP Packets, part from modifying the destination IP-address, the HA may modify the destination port address to redirected port address based on availability of redirect port information in hotline/non-hotline profile information. Before finding the adjacency for modified destination IP-address, the HA maintains the NAT translations between the redirected IP-address and actual destination IP-address of the packet. And, the translations also consists of the redirect port and actual destination port information along with **ip**-addresses.

Packet Processing of Downstream Packets

In the downstream path, when a response is received from redirected packets from the redirect server, the HA first finds the adjacency, and based on idb, it hands over the packet to the Home Agent application. The HA looks into NAT translations based on packet information (for example - source IP-address, source port (incase of TCP or UDP packets), ICMP ID (for icmp packets)). The HA fetches the corresponding NAT translation, and modifies the packet source IP-address to the actual destination IP-address. The packets need to be subjected to NAT translations before applying in/out acl, tunnel template and QOS, Hotline/Non-Hotline rules. Later, the HA encapsulates the packet and routes it towards the FA after inspecting the packets with the Home Agent applications.

This functionality can be achieved with NAT support. Here, the HA maintains NAT translations between redirect IP address, the redirect port to destination IP address, and the destination port. The port information is applicable for UDP and TCP packets only.

Create and Maintain the NAT Translations:

- None of the interfaces can be marked as “nat inside” and “nat outside” to maintain the NAT Translations for redirected packets.
- Creating the NAT translations are applicable for upstream hot-lined/non-hot-lined IP redirected packets only.
- TP will only own to create and maintain the NAT translations, CP does not get NAT translations information from individual TPs.

Timeout for NAT Translations

- The HA will internally trigger timer values for NAT translations by invoking NAT APIs during interception of redirected packets for creating translations.
- The timeout values are initialized during configuration of **ip mobile home-agent ipredirect nat-enable** command. The timeout values are not visible on the CP in the **show running-config**, but the TP will display these values.

The following are the Timeouts for different form of packets.

  - For TCP packets, the FIN/RST timeout is 30 Seconds.
  - For TCP packets, the SYN timeout is 30 Seconds.
  - For TCP packets, the timeout is 60 Seconds.
  - For UDP packets, the timeout is 30 Seconds.
  - For ICMP packets, the timeout is 5 Seconds.

- The NAT translation of ICMP packet is timeout after 5 seconds of creation of NAT translations irrespective of response sent by redirected server for translated packet. If the response packet is received from the redirect server within NAT translations expiry (i.e., 5 seconds), the HA re-translates the packet with packet src IP address actual destination IP address.
- For TCP packets, if there is no syn and ack for NAT translated packet on the HA, the HA will timeout for NAT Translations after 20 Seconds.
- For TCP Packets, the HA clears the NAT translations for received FIN or RST packet after 30 seconds.
- For TCP Packets, the HA clears the NAT translation entries after 60 seconds if there is no packet with TCP flags FIN or RST for TCP connection.
- For UDP Packets, the HA clears the NAT translation entries after 30 seconds if there are no packets for corresponding NAT entries.

Redundancy support

There is no redundancy support for updating the NAT translations between the HA redundant peers. During the transition time after switchover between redundant peers, the current active-HA may fail to translate the response packets from redirected server, since it does not have NAT entries for actual requested packets with destination IP-address and redirect IP-address.

Restrictions and Limitations

- Un-configuring this feature CLI command is not permitted when there are active sessions on the Home Agent.
- NAT translations will be cleared on the HA when the timer expiry occurs for each NAT translations, or by removing the translations using the **clear ip nat translations** command. Clearing the MIP sessions and un-configuring the **ip mobile home-agent ipredirect nat-enable** command does not clear the NAT translations.
- CP doesn't show the **ip nat translations** timeout values in the **show running-config**. But, the TP does show these values since data path is supported on TP. For these timer values “write memory” is not required. These values are initiated when is configured with "ip mobile home-agent ipredirect nat-enable" feature.
- HA will take 360bytes of memory to maintain each NAT Translation. From the theoretical calculations,
  - On the 1GB card, each TP can create maximum of 50k translations
  - On the 2GB card, each TP can create maximum of 100k translations.
- Due to deep inspection of packets to create NAT translations and maintain NAT translations, the HA is impacted with a 15-20% of CPU utilization for processing hot-lined redirected packets.

CHAPTER 16

Other Configuration Tasks

Other Configuration Tasks

This chapter discusses important concepts and provides configuration details for the following features in the Cisco IOS Mobile Wireless Home Agent software:

HA - Realm Case-Insensitive Option

NAI contains two parameters, username and realm written as username@realm. In HA 5.0, both username and realm are case sensitive. When an RRQ with NAI is received from the FA, the HA has to find a match with the configured commands. HA 5.0 tries to find a case sensitive match for both username and realm.

The Realm Case Insensitive feature enables you to match the configured commands against RRQ NAIs with case insensitive realm parameters. However, the username is still considered to be case sensitive.

Example 1:

Local Configuration

```
router(config)#ip mobile host nai @sprintpcs.com interface Null0
```

The following NAIs (with different cases of the same realm) are a match is the above configuration.

- mobile1@sprintpcs.com
- mobile2@sprintPCS.com
- mobile3@sprintPCS.COM
- mobile4@SPRINTPCS.COM
- mobile5@sPrInTpCs.cOm

Example 2:

Local configuration

```
router(config)#ip mobile host nai mobile6@sprintpcs.com interface Null0
```

The following NAIs (with different cases of same username) are not a match with the above configuration CLI:

- Mobile6@sprintpcs.com
- MoBiLe6@SPRINTPCS.COM
- MOBILE6@sprintpcs.com

Configuring the Realm Case Insensitive Feature

To enable the Realm Case Insensitive feature, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)# ip mobile options`	Provides a sub configuration mode for entering MobileIP options.
	`Router(config)# realm case-insensitive`	Enables the Realm Case-Insensitive feature.

Here is an example:

```
HA(config)#ip mobile options
HA(config-ipmobile-options)#realm case-insensitive
```

Here is an example of how to verify the command:

```
router#show ip mobile options
IP Mobility Options information:

Realm (Domain) match is case insenstive
```

Limitations and Restrictions

Following are the limitations and restrictions for this feature:

- RRQs having NAI with realm case insensitive are considered to be from the same MN. For example, "user1@cisco.com" and "user1@CISCO.COM" are considered to be from the same MN.
- Realm Case Insensitive enable/disable cannot be modified when active sessions are present.
- Realm case insensitive does not work for conditional debugging with username **debug condition username** *nai*. To enable conditional debugging for a user, you must use a case sensitive NAI.

FA-HA Auth Extension Mandatory

The HA must be able to force the HA to require the FA-HA Authentication Extension in the MIP RRQ, or otherwise reject the RRQ. This feature rejects any RRQ that does not have an appropriate **ip mobile secure foreign-agent** command configured. Currently if you send an RRQ to the HA and omit the FA-HA Auth Extension, and do not configure the **ip mobile secure foreign-agent** command for this FA IP Address, the RRQ is accepted. This is considered to be a security risk.

Currently, the HA allows the FHAE extension received in an RRQ or revocation messages from Wimax FAs based on local configuration of the **FA Access-Type** command. The HA supports the following command that allows the FHAE in a received MIP RRQ for Wimax FAs:

ip mobile home-agent foreign-agent *fa-address mask* **access-type wimax {enable-fhae | disable-fhae}**

The above command is modified for 3gpp2 access-type by having the keywords **enable-fhae** and **disable-fhae** added for 3gpp2 FAs. To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent foreign-agent {default | {fa-address mask}} access-type {wimax | 3gpp2} [enable-fhae | disable-fhae]`	Configures the FHEA extension received in an RRQ or revocation messages from a Wimax or 3gpp2 FA.

Here are some configuration details:

- Whenever the command options are modified for the same address and mask values of FAs from option-less/enable-fhae to disable-fhae, then the HA will clear already stored FA-HA keys for those FAs.
- When the Access-type option is modified for the configured address and mask values, then the HA deletes the already stored FA-HA keys.

RRQ Processing on HA

The following scenarios are indicate how the HA processes the RRQ in these scenarios

SCENARIO -1

FA access-type is not configured with **enable-fhae** or **disable-fhae** indicated in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

Configure FA-HA key values for 3gpp2 FAs locally on the HA using the following commands:

ip mobile secure foreign-agent *start-ip end-ip* spi …..

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is configured locally
RRP is sent successfully with FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ does not have FHAE.

a. FA-HA key is configured locally
RRP is sent with error code 132 with FHAE.

b. FA-HA key is not configured locally
RRP is sent successfully without FHAE.

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is already derived from HA-RK (or) HA-RK is already present.
Access-Request is not sent for HA-RK, but may be sent for other purpose.
RRP is sent successfully with FHAE.

b. FA-HA key is not present and HA-RK is not present. Access-Request is sent.
- HA-RK is downloaded.
- RRP is sent successfully with FHAE.

c. HA-RK is not downloaded.

- RRQ is dropped and RRP is not sent.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is already derived from HA-RK. or earlier RRQ from this FA has FHAE.
RRP is sent with error code 132 with FHAE.

b. FA-HA key is not present. None of the RRQs from this FA have FHAE.
RRP is sent successfully without FHAE.

SCENARIO -2

FA access-type is configured with **enable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

To configure the FA-HA keys for 3gpp2 FAs locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys for 3gpp2 locally on the HA.

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is configured locally
RRP is sent successfully with FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ does not have FHAE.

a. FA-HA key is configured locally
RRP is sent with error code 132 by appending FHAE.

b. FA-HA key is not configured locally
RRP is sent with error code - 132 without FHAE.

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is already derived from HA-RK (or) HA-RK is already present.
Access-Request is not sent for HA-RK, but may be sent for other purpose.
RRP is sent with FHAE.

b. FA-HA key is not present and HA-RK is not present.
Access-Request is sent.

a. HA-RK is downloaded.
RRP is sent with FHAE.

b. HA-RK is not downloaded.
RRQ is dropped and RRP is not sent.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is already derived from HA-RK. The earlier RRQ from this FA has FHAE. (This result is the same even if the FA-HA key is deleted because of the HA-RK lifetime expiry. Using FHAE once for this FA is enough for this condition).
RRP is sent without FHAE - (FA Failed Authentication error code).

b. FA-HA key is not present.
Irrespective of whether HA-RK is downloaded or not. RRP is sent with error code 132 without FHAE.

SCENARIO -3

The FA access-type is configured with **disable-fhae** using the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

To configure the FA-HA key values locally on HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys locally on the HA.

Case 1:

3GPP2 FA, RRQ has FHAE.

a. FA-HA key is not configured locally
Access-Request is not sent (for obtaining FA-HA key).
RRP is sent with error code 132 (without FHAE).

3GPP2 FA, RRQ doesn't have FHAE.

a. FA-HA key is not configured locally
RRP is sent successfully (without FHAE).

Case 2:

Wimax FA, RRQ has FHAE.

a. FA-HA key is not present and HA-RK is not present.
Access-Request is sent.
a.HA-RK is downloaded.
b.RRP is sent without FHAE.

b. HA-RK is not downloaded.
RRP is sent without FHAE.

Wimax FA, RRQ does not have FHAE.

a. FA-HA key is not present.
RRP is sent without FHAE.

Processing and Initiating Revocation Messages

SCENARIO -1

The FA access-type is not configured with **enable-fhae** or **disable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

To configure the FA-HA key values for 3gpp2 FAs locally on HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	Configures the FA-HA keys for 3gpp2 locally on the HA.

- For 3ggp2 FAs, the HA sends a Registration Revocation Message to the FA by authenticating the message with/without FHAE-based FA-HA key configuration
- For Wimax FAs, the HA does not send a Registration Revocation Message to the FA if the HA-RK key timer expires, or if the HA-RK key or FA-HA key are unavailable.

- The HA drops the received Registration Revocation Message from the FA if the Registration Revocation Message has FHAE and the HA does not have a FA-HA key locally for the corresponding FA. This is true for both 3gpp2 and Wimax FAs.
- The HA drops the received Registration Revocation Message from the FA if the received message does not have FHAE, but is configured with the FA-HA key locally on the HA for 3gpp2, or if the key is already derived for Wimax.
- For other cases, the HA processes or initiates the Registration Revocation Messages +vely.

SCENARIO -2

The FA access-type has an option with **enable-fhae** in the following commands:

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

To configure the FA-HA keys for 3gpp2 FAs locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent` *start-ip end-ip* `spi`	Configures the FA-HA keys for 3gpp2 locally on the HA.

- For 3ggp2 FAs, the HA does not send a Registration Revocation Message to the FA if the FA-HA key is not available locally.
- For Wimax FAs, the HA does not send a Registration Revocation Message to the FA if the HA-RK key timer expires, or if the HA-RK key or FA-HA key is unavailable.
- The HA drops the received Registration Revocation Message from the FA if the received message does not have FHAE, but is configured with FA-HA key locally on the HA for 3gpp2, or the key is already derived for Wimax.
- For other cases, the HA initiates the Registration Revocation Messages +vely.

SCENARIO -3

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

To configure FA-HA key values locally on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile secure foreign-agent` *start-ip end-ip* `spi`	Configures the FA-HA key values locally on the HA.

- The HA drops the received Registration Revocation Message from the FA if the Registration Revocation Message has FHAE. This is true for both 3gpp2 and Wimax FAs.
- For other cases, the HA initiates the Registration Revocation Messages +vely.

Absolute Timeout Per NAI

In case of data-path idle timer, the user gets deleted whenever it remains idle (no traffic) for the configured interval. But, when started, the absolute timer removes the user, even though the user is active.

This feature sets the absolute timeout for a session either locally, or through a Radius Access Accept, to disconnect the user's session when the timer expires regardless if the user sends traffic, or not. Currently, the HA supports the AAA attribute session-timeout [27] in case of hotline users. The same attribute is extended for the absolute-timer.

The absolute-timer should be initiated during Registration only and should never get modified until the binding is deleted. If the absolute-timer is not received during registration, but it is received during re-registration, then the absolute timer is not started. The absolute-timer has meaning only for initial registration.

The absolute-timer runs independent of the hotline timer. Once configured, the absolute timer clock continues and will delete the binding when it expires.

Redundancy is supported, and the absolute timeout value needs to be synched to the standby.

Configuring the Absolute Timeout Feature

To enable the HA to set the absolute timeout for a session, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm realm absolute-time interval-in seconds`	Configures the **absolute-time** locally on HA. When Session- Timeout [27] gets downloaded from the AAA, it takes a higher precedence and will overwrite the locally configured **absolute-time** value.

Verifying the Configuration

Here are some examples to help you verify and troubleshoot the configuration:

For 3GPP2 binding, the output will be as follows:

```
# show ip mobile binding

Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:52
    Flags sBdmg-T-, Identification CD735149.00000005
    Tunnel0 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Tunnel0 Output ACL: p1_test - ACL is empty or not configured
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:52
    Traffic Plane Id:6
```

For WiMAX binding, the output will be as follows:

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
sony6@cisco.com (Bindings 1):
```

```
    Home Addr 65.0.0.3
    Care-of Addr 50.1.1.90, Src Addr 50.1.1.90
    Lifetime granted 02:00:00 (7200), remaining 01:59:07
    Flags sBdmg-T-, Identification CD7352EA.00000006
    Tunnel0 src 14.0.0.2 dest 50.1.1.90 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: WiMAX(802.16e)
    Acct-Session-Id: 0x00000004
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:02:00 (120), remaining 00:01:07
    Traffic Plane Id:5
```

Incase of both hotline timer and absolute timer are present for the binding, the output will be:

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:49
    Flags sBdmg-T-, Identification CD7358E6.00000005
    Tunnel1 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000009
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Hotline session granted 00:01:00 (60), remaining 00:00:49
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:49
    Traffic Plane Id:6
```

The following new debug statements will appear when this feature is configured.

```
MobileIP: Absolute timer expired for MN derath5@cisco.com
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000009
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel1 src 14.0.0.2 dest 50.1.1.92
MobileIP: Delete database info. for MN 65.0.0.2
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel0 src 14.0.0.2 dest 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000007
MobileIP: Delete database info. for MN 65.0.0.2
```

Restrictions and Limitations

- The HA should not delete the binding on the standby CP. Otherwise, the binding deletion from the active will fail and appear in the error statistics.

  The following special case/race conditions are handled separately (for example, one race condition):

  - A binding is created on the active/standby.
  - The timer expires on the active and standby.

- The binding is deleted from active, but not from the standby because the timer expired.
- A switchover occurs before the binding deletion event is sent from the active to the standby.
- The standby becomes the active and has a binding for which the absolute timer expired.

To handle the above case, the absolute-timer is stopped and re-started on the standby for the interval with which it initially started. After this interval expires, the binding is deleted.

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.

Configuring Mobile IP Tunnel Template Feature

To enable the Mobile IP Tunnel Template feature, perform these tasks:

	Command	Purpose
Step 1	`Router(config)# interface tunnel 10` `ip access-group 150`	Configures an interface type and enters interface configuration mode. **tunnel** interface; a virtual interface. The number is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
Step 2	`Router(config)# access-list 150 deny any 10.10.0.0 0.255.255.255` `access-list permit any any`	Configures the access list mechanism for filtering frames by protocol type or vendor code
Step 3	`Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1`	Configures the Home Agent to use the template tunnel.

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

```
interface tunnel 10
ip access-group 150 in -------> apply access-list 150
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
ip mobile home-agent template tunnel 10 address 10.0.0.1
```

Note If you enable the Mobile IP Tunnel Template feature and remove the tunnel interface from the configuration, you should also manually remove the corresponding **mobileip tunnel template** command. If necessary, you can reconfigure the **mobileip tunnel template** command after you configure a new tunnel interface.

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:

Step 1 The HA receives an RRQ from the PDSN/FA

Step 2 The HA sends an Access Request to AAA. The HA adds the MHAE SPI of the RRQ to the Access Request as MN-HA-SPI(26/57) attribute.

Step 3 The AAA server matches the MN-HA-SPI (26/57) against the corresponding MN-HA-SHARED-KEY (26/58).

Step 4 The AAA server includes that MN-HA-SHARED-KEY (26/58) in the access reply.

Step 5 The HA authenticates the MHAE of RRQ using the downloaded shared key MN-HA-SHARED-KEY (26/58).

Note If the MN-HA key and SPI are downloaded from AAA using 3gpp2 attributes [57/58], then the HA authenticates MHAE using MD5 algorithm only.

User Profiles

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

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

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

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

The Home Agent supports the local configuration of a maximum of 200000 user profiles; on the SAMI, the HA supports 6 x 200000 user profiles. The User profile, identified by the NAI, can be configured locally, or retrieved from a AAA server.

Mobility Binding Association

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

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

The binding association contains the following information:

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

MS Traffic Redirection in Upstream Path

This feature allows any traffic received from a mobile node to be redirected to the next-hop address in the upstream path. Even mobile node to mobile node traffic is sent outside of the Home Agent, and gets routed back from the external device. The feature can be configured on a per realm basis, which allows that each realm can have a different next hop IP address. This means that only NAI-based hosts are supported; IP address-based hosts are not supported in the redirection. Redundancy is also supported for this feature.

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.

Selective Mobile Blocking

You might want to block access to a specific mobile for reasons such as prepaid quota is over, service is disabled due to non-payment of bills, or other reasons. You can accomplish this by adding the “mobileip:prohibited” cisco-avpair attribute to the user profile on AAA server. When the “mobileip:prohibited” attribute is returned to Home Agent in access accept, the behavior is as follows:

- If the AAA server returns “mobileip:prohibited=1” in an access accept, and if the MN-HA Security Association for the mobile is configured on the AAA server and also returned to Home Agent in an access accept, the Home Agent sends a registration request (failure) with error code 129 (Administratively Prohibited) to the MN.
- If the AAA server returns “mobileip:prohibited=0” in an access accept, or if the attribute is not returned to the HA in an access accept, the HA performs normal processing of the registration request.

Note The “mobileip:prohibited” attribute should not be set to any value other than 0 and 1.

Support for Mobile Equipment Identifier (MEID)

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. It is a globally unique 56-bit identification number for a physical piece of mobile station equipment. In the interim period though, both the attributes need to be supported on the Home Agent.

The MEID NVSE will be appended by the PDSN node to the Mobile IP RRQ. When the MEID NVSE is received on the HA, and the **ip mobile cdma ha-chap send attribute A3** command is configured, the MEID value is included in the HA-CHAP access request.

Support for Call Admission Control (CAC)

Currently, the number of bindings and amount of memory usage are considered for calculating load balancing in HA-SLB. The existing dynamic feedback protocol (DFP) weight calculation equation can be modified by considering the frequency of calls per second (CPS) and throughput parameters on each real server (HA).

The CPS on the HA can be calculated every minute, and is called Usage CPS. Additionally, it can be configured to some maximum value (Available CPS) that can be handled by HA. If the Usage CPS equals the Available CPS, then the HA real server will return less weight to SLB.

As it is difficult to calculate throughput on router and it can be solved by usage of interrupt CPU for packet handling.

From the above two parameters, the equation looks like this:

```
dfp_weight = (Maxbindings - NumberofBindings)*(cpu+mem)*
(Available cps - Usage cps) *dftp_max_weight / (Maxbindings*32*Available cps)
```

Configuring CAC on the HA

To configure the maximum number of bindings that are allowed on the HA, perform the following task:

	Command	Purpose
Step 1	`Router(config)#` **`ip mobile home-agent max-binding`** *`max-binding-value`*	Limits the number of bindings that can be opened on the HA. The default value of max-binding-value is 235,000.

Congestion Control Feature

In Cisco Mobile Wireless Home Agent Release 5.0, the congestion control feature requires that the call admission control algorithm implemented by the Home Agent is modified to take action when it is determined that the congestion state is reached.

You can configure the DFP weight to determine when congestion occurs. Typically, the DFP value corresponds to 70% congestion state. The DFP weight, by default, is in the range **0-24**. You can configure the max weight to have a required range of the values. **0** corresponds to maximum resources used, and the max scale value indicates that resources are 100% available.

The DFP value used is calculated solely for the control processor in the Single IP model. It is not expected that Traffic Plane processor resource usage will contribute to congestion.

When the congestion state is reached, four possible actions can occur:

- Reject: Reject any new call attempts. The rejection is indicated by sending a MIP Registration Reply with error code 130 (insufficient resources).
- Abort: Reject any new call attempts and abort any “in progress” calls. In-progress means any MIP registration where the Registration Request has been received and the Registration Reply has not yet been sent. The rejection is indicated by sending a MIP Registration Reply with error code 130 (insufficient resources).

- Redirect: Reject any new call attempts and abort any "in progress" calls. In-progress means any MIP registration where the Registration Request has been received and the Registration Reply has not yet been sent. The rejection is indicated by sending a MIP Registration Reply with error code 136 (unknown Home Agent address). The Home Agent address field will contain the address of the Home Agent that the call attempt should be redirected to. The to-be-redirected-to-address is configured globally on the Home Agent.
- Drop: Drop existing calls based on Data Path Idle Timer evaluation. Any bindings with the data path idle time that surpassed a configured value are released. This event sends a Resource Revocation message, if configured. If Resource Revocation is not configured, the binding is silently removed as if a local binding clear was requested.

Note Only one action is configurable at one time. If you try to configure a second action, that will overwrite the first one.

Configuring the Congestion Control Feature

Perform the following tasks to define the call admission control actions when the congestion trigger occurs:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent congestion` *dfp_weight* **action | reject | abort | redirect** *HA-address* **| drop data-path-idle** *minutes*	Defines the call admission control actions when the congestion trigger occurs.
Step 2	`Router# show ip mobile home-agent congestion`	Displays the following information: • Congestion state—congested or not congested. • Configured value of congestion-threshold = dfp_weight from configured CLI. • Current dfp-value. The current-dfp-value is the average DFP value over the last five minutes.

Additionally, the CISCO-SLB-CLIENT-MIB contains the following information:

- DFP congestion onset threshold above which a Congestion On Trap is generated.
- DFP congestion abatement threshold, which when crossed following congestion generates a Congestion Off trap.
- Current DFP value

Here is sample output for the Congestion Control feature:

```
router#show ip mobile home-agent congestion
Home Agent congestion information :
Current congestion level:  Congested
Configured Action : Reject
Configured threshold : 10
Current DFP value = 7
```

Framed-Pool Standard

Framed-Pool is an AAA attribute that contains the name of the assigned address pool used to assign an address for the user on the HA. In HA3.1, this functionality is supported by a Cisco VSA.

The HAAA sends these attributes in an Access-Accept message to the HA for dynamic/static address allocation. If the HA receives both attributes in an Access-Accept, it can accept one among them as pre-configured on HA.

Perform the following task to configure the framed-pool standard feature:

Step 1	`router# ip mobile home-agent aaa attribute framed-Pool`	Enables the HA to use the Framed-Pool attribute, and contains the Local Pool name returned as part Access-Accept from the RADIUS server.

Here is an example:

```
ip mobile home-agent aaa attribute Framed-Pool
ip local pool haPool 70.1.1.1 70.1.1.254
ip mobile home-agent
ip mobile virtual-network 70.1.1.0 255.255.255.0
ip mobile host nai @cisco.com interface FastEthernet1/0 aaa load-sa
```

Priority-Metric for Local Pool

In order to assign IP addresses to mobile clients, the HA uses local pools configured with a range of IP addresses. Whenever a registration request arrives, the HA authenticates the MN and gets the pool name to assign an IP address. The HA gets the pool name either from its own configuration, or from the Radius Server thru a Cisco-VSA or Framed-Pool attributes.

While configuring for IP local pool, you can have multiple groups, each group can have multiple pools, and each pool can have a multiple range of IP addresses. In a single group you cannot have an overlapping range of IP Addresses. All the addresses under a group are unique.

By default, the request for an IP address contains the pool name (mandatory), static IP address (optional), and an associated username (optional). Initially all the IP addresses are put in a free pool and from there each IP address is assigned. Whenever you are assigning IP address, you should associate an IP address with the given username.

You can also add priority to the addresses to select a desired range of IP addresses from the pool for the new requests. Once all of the subscribers move to the new addressing scheme, the old addressing (low priority range) can be removed from the system.

Generally, if an IP address is reserved, it will be associated with that user (by userid). If the user disconnects and connects again, the same IP address will be given to that user if it is not used by anyone. This user IP address association is controller by cache-limit along with the pool configuration. So if you change the priority of the addressing scheme, or if a high priority addressing scheme is available with a free address, then the HA assigns a new IP address from the new addressing scheme rather than giving the old reserved IP address. If there is no change in the priority, HA will try to assign the previous IP address.

You can also set and get the priority value through the SNMP MIBS by accessing the same from Network Manager. The new MIB object for priority is added to the “cIpLocalPoolConfigEntry” table to access the priority value. With the new MIB object, you can change the priority of an existing local pool.

Configuring Priority Metric for Local Pool

To configure the Priority Metric for local pool feature perform the following tasks:

Step 1	`router# Router(config)#` **`ip local pool {default |`** *`poolname`***`} [`***`low-ip-address`*** **`[`***`high-ip-address`***`]] [group`** *`group-name`***`] [cache-size`** *`size`***`] [priority`** *`1-255`***`] [theshold`** *`low-threshold high-threshold`***`]**	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, to generate traps when pool utilization reaches a high or low threshold in percentage. The new option **priority** *1-255* is allows you to assign a priority to a newly created pool, and this priority is used to assign IP addresses.
Step 2	`Router(config)#` **`no ip local pool`** `vsa-pool 1.0.0.201 priority 180`	Unconfigures the pool.

Here is an example:

The HA creates a local pool with default priority as 1 (lowest priority)

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255
```

The HA creates a local pool with priority 100

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255 priority 100
```

Verifying the Configuration

Perform the following task to verify the configuration:

Step 1	`Router#` **`show running-config | include pool`**	Displays the local pool configuration along with its priority only if the priority is not equal to 1 (default and lowest value).

Here is an example:

```
Router# show running-config | include pool
ip local pool frmd-pool 1.0.0.191 priority 20
ip local pool vsa-pool 1.0.0.201 priority 180
ip local pool vsa-pool 1.0.0.211 1.0.0.219
ip local pool vsa-pool 1.0.0.202 1.0.0.209 priority 100


router# show ip local pool

 Pool          Begin         End           Free  In use  Priority
 frmd-pool     1.0.0.191     1.0.0.191        1       0        20
 vsa-pool      1.0.0.201     1.0.0.201        1       0       180
               1.0.0.211     1.0.0.219        9       0         1
               1.0.0.202     1.0.0.209        8       0       100
```

Mobile IPv4 Host Configuration Extensions RFC4332

This section describes the Mobile IP host configuration extensions as implemented in IOS.

An IP device requires basic host configuration to be able to communicate. For example, it typically requires an IP address and the address of a DNS server. This information is configured statically or obtained dynamically using Dynamic Host Configuration Protocol (DHCP), or Point-to-Point Protocol/IP Control Protocol (PPP/IPCP). However, both DHCP and PPP/IPCP provide host configuration based on the access network. In Mobile IPv4, the registration process boots up a Mobile Node at an access network, also known as a foreign network. The information to configure the host needs to be based on the home network. The Mobile Node at a foreign network needs to get the IP address, home subnet prefix, default gateway, home network's DNS servers in the boot up of the network interface.

When the Mobile Node needs to obtain its host configuration, the Host Configuration Request VSE is appended to the Registration Request. This VSE indicates to the Home Agent that either all, or selected host configuration VSEs need to be appended to the Registration Reply. If the Home Agent retrieves the information from a DHCP server in Proxy DHCP mode, then the DHCP Client ID and DHCP Server extensions are appended in the Registration Reply. These DHCP-related extensions are populated with values that had been used in the DHCP messages exchanged between the Home Agent and the DHCP server. The VSEs are authenticated as part of the registration message using any of the authentication mechanism defined for Mobile IP.

The following Cisco vendor-specific extensions provide the host configuration for a Mobile node. The "Host Configuration Request" extension is allowed only in the Registration Request.

The rest of the extensions are appended in the Registration Reply.

- Host Configuration Request: request for host configuration information from the Mobile Node to the Home Agent.
- Home Network Prefix Length: the length of the subnet prefix on the home network.
- Default Gateway: the default gateway's IP address on the home network.
- DNS Server: the DNS server's IP address in the home network.
- DNS Suffix: the DNS suffix for hostname resolution in the home network.
- DHCP Client ID: the DHCP Client ID used to obtain the IP address. When the Mobile Node returns home and is responsible for managing its own address, this information maps to the Client identifier option.
- DHCP Server: the DHCP server's IP address in the home network.
- Configuration URL: the URL for the Mobile Node to download configuration parameters from a server.

Note The DNS suffix is not appended in RRP when it is downloaded from the DHCP Server.

WiMAX AAA Attributes

Cisco Home Agent Release 4.0 and above adds support for AAA Authorization and Accounting attributes. The following sections describe the attributes, and provide information on specific attribute support.

HA-AAA Authorization Attributes Support for WiMAX

Following HA-AAA attributes will be added in order to extend support for WiMAX.

- Framed IP Address: When the **ip mobile home-agent send-mn-address** command is configured, the home address received in the MobileIP RRQ is sent as the value of the Framed-IP-Address attribute in Access-Request messages.

Note In the Home Agent Release 4.0 software, the Framed-IP-Address attribute is missing in the access request when opening a MIP flow (Wimax).

- WiMAX Capability: This attribute identifies the WiMax capabilities of the HA, and is sent in all Access-Request messages. It can also be sent by the HAAA in Access-Accept messages. If this attribute is present in an Access-Accept message, it can contain only the Accounting Capabilities sub-TLV, which indicates the accounting capabilities selected by the server for the sessions. It is expected that the accounting capabilities returned by the HAAA in the Access-Accept match the value specified by the HA sent in the Access-Request. Currently, the HA does not process the WiMAX Capability VSA received in an Access-Accept, and performs no verification if the accounting capabilities match.
- HA-IP-MIP4: This attribute identifies the IP address of the HA making the request. This attribut is included in all Access-Request messages from the HA. For existing bindings (Access-Requests corresponding to re-registration and deletion), it's value is set to the home agent address of the binding. For new bindings, the value of this attribute is set to the HA IP address (not Home Address) that is assigned for the binding from the HA configuration that is also sent as the Home Agent IP address in RRP. Refer to the Configuring Home Agent IP Address for the Bindings section.
- RRQ-HA-IP: the HA includes this attribute in an Access-Request message if the IP address in the Home Agent field of the MobileIP RRQ is different from the IP address of the HA. If present, its value is set to the Home Agent IP address in the Mobile IP RRQ.
- MN-HA-MIP4-KEY: This attribute identifies the MN-HA key used for MIP4 procedures. This attribute is included in an Access-accept message, and it is similar to MN-HA-SHARED-KEY. The HA computes the MN-HA Authentication Extension based on the MN-HA MIP4 key for WiMAX subscribers.
- MN-HA-MIP4-SPI: This attribute identifies the MN-HA SPI used for MIP4 procedures. This attribute is included in an Access-Request message, and it is similar to MN-HA-SPI.

Table 16-1 identifies the WiMAX AAA Authorization attributes for the Home Agent.

Table 16-1 WiMAX AAA Authorization Attributes

Attribute Name	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject	Supported in HA 4.0 and above
Message-Authenticator	80	Message Authenticator to integrity protect the AAA message	1	0	1	0	Yes
WiMAX Capability	26/1	Identifies the WiMAX Capabilities supported by the HA. Indicates capabilities selected by the RADIUS server.	1	0	0-1	0	Yes
CUI (Chargeable User Identity)	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1	0	0-1	0	Yes
AAA-Session-ID	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	0-1	0	1	0	Yes
HA-IP-MIP4	26/6	The IP address of the HA making this request	0-1	0	0	0	Yes
RRQ-HA-IP	26/18	The HA-IP address contained in the Registration Request or Binding Update.	0-1	0	0	0	Yes
MN-HA-MIP4-KEY	26/10	The MN-HA key used for MIP4 procedures.	0	0	1	0	Yes
MN-HA-MIP4-SPI	26/11	The SPI associated with the MN-HA-MIP4-KEY.	1	0	1	0	Yes
RRQ-MN-HA-KEY	26/19	The MN-HA-KEY that is bound to the HA-IP address as reported by RRQ-HA-IP attribute.	0	0	0-1		Yes
HA-RK-Key-Requested	26/58	Indicates that the HA-RK-KEY attribute should be included in the Access-Accept.	1	0	0	0	Yes
HA-RK-KEY	26/15	HA-RK key used to generate FA-HA keys.	0	0	0-1	0	Yes
HA-RK-SPI	26/16	The SPI associated with the HA-RK.	0-1	0	0-1	0	Yes
HA-RK-Lifetime	26/17	HA-RK key used to generate FA-HA keys for MIP4 operations.	0	0	0-1	0	Yes
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1	0	Yes

AAA Attributes for “ip mobile host/realm”

The following attributes will be supported as part of this feature.

- Attribute “data-path-idle”—This is to set the data-path idle timer per Mobile basis as a AAA attribute. It would be downloadable as a Cisco AV pair. If the value is downloaded from AAA and also configured locally, then AAA downloaded value takes precedence. In the RSIM subscriber profile, the config would look like this.

  vsa cisco generic 1 string “mobileip:data-path-idle=300”

  Notes:

  – If the binding were already created with AAA attribute “data-path-idle” and if the **ip mobile realm** *realm* **data-path-idle** is configured/modified later, then only the bindings that were created without the AAA attribute will be updated. This is to make sure that AAA precedence is still intact.

  – Re-registrations can update the data-path-idle timer.

- Attribute “Nexthop”—This is to set the nexthop IP per Mobile basis as a AAA attribute. This would be downloadable as a cisco AV pair. If this value is downloaded from AAA and also configured locally, then AAA downloaded value takes precedence. In the RSIM subscriber profile, the config would look like this.

  vsa cisco generic 1 string "mobileip:nexthop=1.1.1.1"

  Notes:

  – If the bindings were already created with nexthop downloaded from AAA, and if the **ip mobile realm** *realm* **any-traffic nexthop** *ip* command is configured, the CLI will not be accepted.

  – When **nexthop ip** is configured through CLI with bindings already created, then only the confirmation of the deletion of bindings, the value can be updated.

  – Re-registrations cannot update the downloaded nexthop attribute.

MN and Foreign Agent Authentication

The HA includes the SPI received in the MHAE as the value of the MN-HA-MIP4-SPI attribute in the Access-Request along with HA-IP-MIP4. The value of the MN-HA-MIP4-KEY attribute downloaded from the AAA corresponding to HA-IP-MIP4 and SPI value in the MN-HA-MIP4-SPI attribute is used to verify the MHAE in the Mobile IP RRQ and to generate MHAE for Mobile IP RRP.

The following information is extracted from the Registration Request:

- MN-HA SPI in the MN-HA Authentication Extension.
- HA IP address in Home Agent field.
- Recipient IP address in the Destination IP address field.
- FA-HA SPI in the FA-HA Authentication Extension if this extension is in the message.

The HA includes the MN-HA-MIP4-SPI and HA-IP-MIP4 attributes (which contain the MN-HA SPI and HA IP address, respectively) in the Access-Request that is sent to the AAA server. The Access-Accept from the AAA server includes the MN-HA-MIP4-KEY attribute which corresponds to the two attributes in the Access-Request. The HA sets up the MN-HA security association with the downloaded key. The security association is used to authenticate the MN-HA Authentication Extension in the Registration Request, and for generating this extension in the Registration Reply.

The Registration Request may contain the Home Agent field with IP address set to all ones or zeros to indicate dynamic HA assignment. In this case, the HA includes an additional RRQ-HA-IP attribute, which is set to the Home Agent field value, in the Access-Request. The MN-HA-MIP4-SPI attribute is the same as described before. However, the HA-IP-MIP4 attribute is set to the Recipient IP address instead. The AAA server includes the additional RRQ-MN-HA-KEY attribute (which corresponds to the

RRQ-HA-IP attribute) in the Access-Accept. The HA uses this key to authenticate the MN-HA Authentication in the Registration Request. Upon successful authentication, the HA sets up the MN-HA security association with the MN-HA-MIP4-KEY to send the Registration Reply. Subsequent registration authentication uses this security assocation.

In case of CMIP, if the RRQ contains HA IP as ALL-ZERO-ONE-ADDR, then along with MN-HA-MIP4-SPI and HA-IP-MIP4, RRQ-HA-IP is also sent in Access-Request with the value equal to HA IP of RRQ. HA downloads RRQ-MN-HA-KEY for RRQ-HA-IP and MN-HA-MIP4-KEY for HA-IP-MIP4 corresponding to MN-HA-MIP4-SPI. The HA verifies MHAE of Mobile IP RRQ using RRQ-MN-HA-KEY and generates MHAE for Mobile IP RRP using MN-HA-MIP4-KEY.

If a RRQ received from a FA contains FHAE, then Foreign-agent authentication happens for that FA. Also all sub sequent RRQs received from that FA should contain FHAE. For authenticating FA at HA, HA-RK needs to be present at HA. If HA-RK is not present at HA , HA downloads HA-RK from AAA.

The HAAA creates a random 160 bit HA-RK key for each HA-IP. The HA-RK is not based on the MIP-RK generated as a result of a specific EAP authentication. Thus, it is not bound to a individual user or authentication sessions, but to Authenticator-HAAA pairs.

If the HA needs to download HA-RK from AAA, then the HA includes an HA-RK-Key-Request VSA with the value set to 1 in Access-Request to indicate that it expects to receive the HA-RK-KEY attribute in the Access-Accept. The HA-RK-SPI attribute is also included in the Access-Request, and its value is set to the SPI received in the FHAE. The HAAA will return the HA-RK-KEY, HA-RK-SPI and HA-RK-Lifetime attributes in Access-Accept associated with the HA-IP-MIP4 attribute sent in the Access-Request. If one of these attributes is present, then all must be present. If not then HA discards the Access-Accept. This attribute is not included in any of the Accounting (Start/Stop/Interim) messages.

HA-RK Key(26/15), HA-RK SPI(26/16), HA-RK lifetime(26/17) will be synched to standby or redundant HA.

Both the HA and the FA (which is most likely co-located with the Authenticator) compute the FA-HA key from the HA-RK as follows:

FA-HA = H(HA-RK, “FA-HA” | HA-IPv4 | FA-CoAv4 | SPI)

Where

H = HMAC-SHA1, specified in RFC 2104, HMAC: Keyed-Hashing for Message Authentication

HA-IPv4 = HA-IP-MIP4 attribute sent in Access-Request. (i.e. Binding Home Agent IP).

FA-CoAv4 = Address of the FA expressed as a 32-bit value as seen by the HA

If the MobileIP RRQ received from the FA contains the FHAE extension, then the FA-HA key generated using the above algorithm along with the SPI is used to validate this extension.

You can display the downloaded HA-RK key, SPI, and lifetime using the following **show ip mobile secure home-agent ha-rk** *ha-ip* command.

Here is an example:

```
router#show ip mobile secure home-agent
HomeAgent HA-RK List:
15.1.1.80:
    SPI 102, Lifetime 00:10:30 (630), Remaining 00:10:24
    Key 31323334353637383930313233343536373839 30
```

You can display the generated FA-HA-Keys using the **show ip mobile secure foreign-agent** *fa-ip* command.

Here is an example:

```
router#show ip mobile secure foreign-agent
Security Associations (algorithm,mode,replay protection,key):
14.1.1.28:
    SPI 102,  HMAC-MD5, Timestamp +/- 7, HA-IP 15.1.1.80
    Key b932c46406dcfe411f8bd147103ac53ca0c7fe65
```

The above downloaded HA-RK and generated FA-HA-keys are deleted if the HA-RK lifetime expires. If a new HA-RK key is downloaded before the lifetime expires, both the keys will continue to co-exist and authentication will be successful using any one of the keys. The same keys can be deleted using the **clear ip mobile secure all** command. This command clears all the keys MN, FA and HA-RK, generated and downloaded from AAA.

For WiMAX, it is not possible to configure locally the SPI and the key for MHAE or FHAE verification.

Configuring Home Agent IP Address for the Bindings

There are vairous ways to configure the Home Agent to assign the Home Agent IP address to the bindings. Perform the following tasks to enable this feature:

Step 1	**ip mobile realm @cisco.com vrf** *vrf-name* **ha-addr** ***vrf-ha-address***	Enables inbound user sessions to be disconnected when specific session attributes are presented for a specific realm
Step 2	**ip mobile home-agent dynamic-address** *dynamic-ha-address*	Sets the Home Agent Address field in a Registration Response packet.
Step 3	**ip mobile virtual-network** *virtual-net-start mask* **address** *virtual-net-ha-address*	Defines a virtual network.
Step 4	**ip mobile home-agent address** *global-ha-address*	Enables the IP address for virtual networks.
Step 5	**HA HSRP redundancy virtual IP address** *hsrp-ha-ip-address*	Specifies the HSRP IP address.

The Home Agent IP address for the bindings is selected using the preceding configuration details. The same Home Agent IP address is sent as HA-IP-MIP4 in an Access-Request and the Home Agent IP in RRP. The following logic does not apply to the RRQs for previously existing bindings. For an existing binding, the current Home Agent IP address for the binding is used.

- RRQ HA IP and RRQ destination IP are same.

  HA-IP-MIP4 = RRP HA IP address =

  - *vrf-ha-address* if configured.
  - RRQ destination IP address.

- RRQ HA IP is not equal to RRQ Destination IP (holds true for dynamic HA, RRQ HA IP = 0.0.0.0 or 255.255.255.255).

  HA-IP-MIP4 = RRP HA IP address =

  - *vrf-ha-address* if configured.
  - RRQ HA IP if **ip mobile home-agent address** *global-ha-address* **unknown-ha accept reply** is configured. (not for dynamic HA).
  - *dynamic-ha-address* if configured
  - RRQ destination IP address.
- RRQ HA IP or RRQ Destination IP is a subnet-directed broadcast address (RRQ HA IP is not equal to 255.255.255.255). HA discovery!

  HA-IP-MIP4 = RRP HA IP address =

  - MN is on physical interface (above IP corresponds to a physical interface)

    hsrp-ha-ip-address if configured.

    physical interface ip address.
  - MN is on virtual network (above IP corresponds to virtual network). This assumes one of *virtual-net-ha-address* or *global-ha-address* is configured.

    virtual-net-ha-address if configured.

    global-ha-address.

HA-AAA Accounting Attributes Support for WiMAX

The functionality for AAA Accounting Attributes is as follows:

- The HA sends an Accounting Start record when the first binding for a mobile is created.
- The HA sends and Accounting Stop record when the last binding for a mobile is deleted.
- The HA sends Accounting Update when Handoff occurs.

Table 16-2 identifies the WiMAX AAA Accounting Attributes for the Cisco HA:

Table 16-2 WiMAX AAA Accounting Attributes

Name	Type	Description	Start	Int	Stop
Acct-Multi-Session-Id	50	This identifier is set to the value of AAA-Session-Id which is generated by AAA after successful authentication and delivered to the NAS in an Access-Accept message. It is unique per CSN and is used to match all accounting records within a session.	1	1	1
Framed-IP-Address	8	The IPv4 address assigned to the MS. This identifies the IP-Session.	0-1	0-1	0-1
CUI (Chargeable User Identity)	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1	0-1	0-1
HA-IP-MIP4	26/6	The IP address of the Home Agent.	1	1	1

Table 16-2 WiMAX AAA Accounting Attributes

Event-Timestamp	55	The time the event occurred.	1	1	1
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS or HA.	0-1	0-1	0-1

Configuring WiMAX Support

By default the HA assumes that all of the bindings are of 3gpp2 access type. For WiMAX, the **per foreign-agent access type** command must be configured (Refer to the Per Foreign-Agent Access-Type Support section). In addition, perform the following tasks to enable WiMAX AAA support:

Step 1	`Router# radius-server vsa send authentication wimax`	Configures the WiMAX VSAs included in RADIUS messages. When this command is enabled, the following following RADIUS attributes will be included in Access-Request messages generated by the HA. • Acct-Interim-Interval (85) • Message-Authenticator(80) • Chargeable-User-Identity(89) • WiMAX Capability (26/1) • HA-IP-MIP4 (26/6) • RRQ-HA-IP (26/18) • MN-HA-MIP4-SPI (26/11)
Step 2	`Router# radius-server vsa send accounting wimax`	Configures the WiMAX VSAs included in RADIUS messages. When this command is enabled, the following following RADIUS attributes will be included in accounting messages generated by the HA. • Acct-Terminate-Cause (49) • Acct-Multi-Session-Id (50) • Acct-Session-Time (46) • Chargeable-User-Identity(89) • Acct-Input-Gigawords (52) • Acct-Output-Gigawords (53) • HA-IP-MIP4 (26/6) • GMT-Time-Zone-Offset (26/3)
Step 3	`Router# ip mobile home-agent send-mn-address`	Configures the standard IETF attributes included in RADIUS messages. When configured, the home address received in the MobileIP RRQ is sent as the value of the Framed-IP-Address attribute in Access-Request messages.

Step 4	`Router#` **`radius-server attribute 55 access-request include`**	Includes the Event-Timestamp (55) attribute in Access-Requests.
Step 5	`Router#` **`radius-server attribute 55 include-in-acct-req`**	Includes the Event-Timestamp (55) attribute in accounting messages.

Verifying the Configuration

Perform the following task to verify that WiMAX support is enabled:

Step 6	`Router#` **`show ip mob bind`**	Indicates when WiMAX capabilities are negotiated during authentication of a subscriber.

Here is an example:

```
Router# show ip mob bind
Mobility Binding List:
Total 15000
MIP-USER12573@ispxyz.com (Bindings 1):
    Home Addr 193.1.1.28
    Care-of Addr 7.0.0.85, Src Addr 7.0.0.85
    Lifetime granted INFINITE
    Flags sbdmg-T-, Identification C9ED9187.10000
    Tunnel3 src 73.0.0.42 dest 7.0.0.85 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Acct-Session-Id: 1677265
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

Support for Acct-Terminate-Cause

In Home Agent Release 4.0, the Acct-Terminate-Cause RADIUS attribute (as defined in RFC 2866 Radius Accounting) was supported, however a value of 0 was always inserted.

In Home Agent Release 5.0, the list of values that follows are supported.

The Value field is four octets, containing an integer specifying the cause of session termination.The termination causes are as follows:

- User Request (1) : User requested termination of service, for example with LCP Terminate or by logging out. - On normal MIP session termination.
- Lost Service (3) : Service can no longer be provided; for example, user's connection to a host was interrupted. - When Resource Revocation is received.
- Idle Timeout (4) : Idle timer expired. - When MIP session is terminated on Idle Timer expiry
- Session Timeout (5) : Maximum session length timer expired. - When MIP session registration timer expires.
- Admin Reset (6) : Administrator reset the port or session. - When binding is cleared by the operator.
- NAS Error (9) : NAS detected some error (other than on the port) which required ending the session. - When RRQ for reregistration is in error or FA-HA AE cannot be verified.

- NAS Request (10) : NAS ended session for a non-error reason not otherwise listed here. - When binding is removed for reason not defined for other values of Terminate-Cause.
- Port Preempted (13) : NAS ended session in order to allocate the port to a higher priority use. - When a session is terminated due to congestion.
- User Error (17) : Input from user is in error, causing termination of session. - When the MN-HA AE cannot be verified on re-registration and the binding is removed.

Note Basic Accounting feature needs to be enabled on the HA in order for this Acct-Term-Cause attribute to be included in Accounting-Stop messages.

Per Foreign-Agent Access-Type Support

This feature enables the HA to know which access-type is supported by a foreign-agent based on the IP address of the foreign-agent. The access-type of a foreign-agent can be either **3gpp2** or **WiMAX**, but not both. Depending on the access-type specified, all authentication and accounting records sent from the HA to the AAA server for all the mobiles under that foreign-agent contain either 3gpp2 or WiMAX attributes, but not both. On reception of Access-accept, the HA processes the attributes based on the access-type specified. If the access-type is not specified for a specific foreign agent address, then the default access-type **3gpp2** is used for all the mobile nodes under that foreign-agent. The default access-type can be changed from **3gpp2** to **WiMAX**.

Configuring Foreign-Agent Access-Type Support

Perform the following tasks to configure support for the Forign-Agent Access type:

	Command	Purpose
Step 1	`Router# ip mobile home-agent foreign-agent { default |{ip-address mask} } access-type {3gpp2 | wimax}`	Selects either **3gpp2** or **wimax** access-type for a subscriber based on the IP address of the foreign agent through which the request came.

This configuration will not be considered if the respective access-type is not configured under RADIUS (**radius vsa send authentication 3gpp2/wimax** for authentication, and **radius vsa send accounting 3gpp2/wimax** for accounting).

Configuration on AAA Server

This section describes the configuration of AAA authentication and accounting attributes on the AAA server. Please note this is a general configuration.

Table 16-3 AAA Authentication and Accounting Attributes on the AAA Server

Attribute	Description
attribute 4 *vsa string*	A unique identifier in the home realm for this Session as set by the HAAA
attribute 6 *ip address as string*	The IPv4 address of the HA for MIP4. This is IP address of the HA making the request.

Table 16-3 AAA Authentication and Accounting Attributes on the AAA Server (continued)

attribute 10 *ascii or hex corresponding string*	The MN-HA-KEY sent by the RADIUS Server to the ASN (for PMIP) or HA use for MIP4 (MIP or PMIP). It is used by the ASN during PMIP4 to calculate the MN-HAAE. It is sent to the HA to validate the MN-HA-AE (MIP4) and to compute the MN-HAAE for of the MIP4 Registration Response or the AUTH for MIP6 Binding Answer based on the MIP version(MIP4 or MIP6) and the SPI.
attribute 11 *spi hex value* range of hex value- 100-FFFFFFFF	The SPI associated with the MN-HA-MIP4-KEY
attribute 15 *ascii or hex corresponding string*	The HA-RK-KEY determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate FA-HA keys.
attribute16 *spi hex value* range of hex value- 100-FFFFFFFF	The SPI used for the HA-RK.
attribute 17 *vsa value*	The lifetime of the HA-RK and derived keys.
attribute 19 *ascii or hex corresponding string*	The MN_HA key sent by the HAAA to the HA to be used to validate the MN-HA-AE of the Mobile IP Registration Request.

Foreign Agent Classification

The Home Agent supports the inclusion of the Proxy Mobile IPv4 Access Technology Type Extension received in a Mobile IP Registration Request. Tech-type values of **3** indicate 802.16e (WiMax) and **7** indicates that 1xRTT/HRPD are supported. If no extension is received the per-Foreign Agent configuration applies. If there is no Per-FA configuration, the global value applies. This defaults to 3GPP2, and can be configured instead to WiMax.

Other values are not supported and the extension is ignored in this case. A single counter is present that indicates the number of times the extension is received with non-supported values. The extension contents are displayed in a debug command that displays mobile messaging contents.

Receipt of tech-type value **3** indicates that the mobile IP registration is for WiMax access. In this case, the actions taken are identical to those for the case when a Foreign Agent is locally configured to support WiMax access.

Receipt of tech-type value **7** indicates that the mobile IP registration is for 1xRTT/HRPD access. In this case, the actions taken are identical to those for the case when a Foreign Agent is locally configured as supporting 3GPP2 access.

The actions taken based on tech-type value take precedence over any locally-configured per-Foreign Agent Access Type configuration. For example, if the locally configured value indicates 3GPP2 and the tech-type value indicates WiMax, then the actions for WiMax are taken.

Note The Access-type of a binding remains the same even if the Home Agent receives different Access Technology Type in Re-registration

MS Traffic Redirection in Upstream

This feature allow any IP traffic received from a mobile node to be redirected to a next-hop IP address in the upstream path. The next-hop IP address is configured on a per realm basis, and is only supported for NAI-based mobile nodes. The same configuration needs to be present both on the active and standby Home Agents for redundancy support.

Configuring MS Traffic Redirection in Upstream Traffic

In addition to the previous configuration details, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *realm* `any-traffic next-hop` *next-hop-ipadress*	Sets the next-hop address for the realm. **any-traffic** indicates that any or all traffic in the upstream from the mobile is redirected. **next-hop** indicates the next-hop feature. *next-hop-ip-address* is the IP address of the next-hop, where the packets needs to be redirected to.

Verifying the Configuration

Perform the following task to verify that MS traffic is redirected:

	Command	Purpose
Step 1	`Router# show ip mobile binding`	Displays that the binding is modified, and displays the next-hop address configured for the mobile.

Here is an example:

```
Router#sh ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
xyz1@xyz.com (Bindings 1):
    Home Addr 11.110.1.1
    Care-of Addr 13.1.1.112, Src Addr 13.1.1.112
    Lifetime granted 00:30:00 (1800), remaining 00:29:52
    Flags sbdmg-T-, Identification CAF62BE1.1
    Tunnel0 src 13.1.254.254 dest 13.1.1.112 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled
    Next-hop set for any-traffic to 14.1.1.201
```

MAC Address as Show/Clear Binding Key

In Cisco Mobile Wireless Home Agent Release 5.0, sessions now contain the MAC address of the terminal. This identifier is learned through Mobile IP signaling. The initial registration request includes the MAC address, and re-registration and de-registration may also include the MAC address. This feature allows a network administrator to search for a session, delete a session, and enable debugging for a host based on the MAC. The debugging and syslog messages are contained the MAC address of the terminal whenever applicable.

The MAC address should also be added to the Cisco-Mobile-IP-MIB.

Note The MAC address is unique for an access network technology, and can be learned from the Proxy Mobile IPv4 Access Network Technology Extension. The default value for access network technology is none.

The following commands are changed to include this new field:

Show Commands :

show ip mobile binding mac address: displays the binding information for a host with the specified MAC address. The output includes the MAC address.

Debug Commands :

debug ip mobile host mac address: displays debugging events for a host with the specified MAC address. The messages include the MAC address when applicable.

Clear Commands :

clear ip mobile binding mac address: deletes the mobility binding entry for the host with the specified MAC address.

Data Path Idle Timer

In Cisco Mobile Wireless Home Agent Release 5.0, when there is no data traffic to and from a terminal for a specified period of time (idle time), the session is terminated. This idle time is configurable either on a per-domain basis, or globally. The per-domain configuration takes higher precedence. Revocation messaging triggered by the binding deletion event may occur.

Re-registrations do not reset the idle timer since RRQs are not received on the data path.

For split Control/Data Plane consideration, only the Traffic Processor is aware of the data traffic for a session. It needs to inform the Control Processor if the idle time has been reached.

The data path idle timer information is synchronized between the Home Agents using the Accounting Interim Sync feature.

Perform the following tasks to enable this feature:

	Command	Purpose
Step 1	`Router(config)# ip mobile realm` *realm* `data-path-idle` *minutes*	Deletes the mobility binding entry in the domain when there is no traffic for a configured period of time (idle time) for a mobility host with NAI that matches the specified realm. The range is 1 - 65535.
	`Router(config)# ip mobile home-agent data-path-idle` *minutes*	Deletes the mobility binding entry when there is no traffic for a configured period of time (idle time). The range is 1 - 65535.

Here is example show output for the Data Path Idle Timer feature:

```
cisco-1@cisco.com (Bindings 1):
    MAC Addr 0000.0001.0000
    Home Addr 5.1.0.1
    Care-of Addr 2.2.2.200, Src Addr 2.2.2.200
    Lifetime granted 10:00:00 (36000), remaining 09:52:39
    IdleTime granted 00:10:00 (10 min), remaining 00:09:24
    Flags sBdmg-T-, Identification CCA7F408.1
    Tunnel0 src 81.81.81.81 dest 2.2.2.200 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit not set
```

OM Metrics for 3GPP2 / WiMAX Bindings

This feature returns peak value for MaxActiveBindings, MaxActive3GPP2Bindings and MaxActiveWimaxBindings when queried for OIDs for the previous interval.

Cisco HA Release 5.1 introduces two timers to handle the OM Metric feature. One of the timers supports the interval starting at the top/bottom according to NTP time. The second timer calculates the OM metrics. The first timer starts when the router boots up, or when the command is modified. The second timer starts when the first timer expires, and this timer expires based on a configured value.

By default this feature is enabled with a default interval of 30 minutes. The default configuration is not displayed in the running-configuration.

Note Redundancy is not supported for the OM-metrics feature.

Configuring OM Metrics

To configure the interval for this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# om-metric-interval {15 | 30 | 60 }`	This is a sub-command that is available under sub-menu of the **ip mobile options** command.

Here is sample output to help verify the configuration:

Metric counters such as number of 3gpp2 bindings, number of Wimax bindings, etc., are displayed under **show ip mobile binding summary**.

```
router#sh ip mob binding summary
Mobility Binding List:
Total 1
3gpp2 Bindings 1
Wimax Bindings 0
```

The new metric values are displayed under a new command.

```
router#show ip mobile options ommetrics
OM Metric Statistics:

 Peak Active bindings in the elapsed (previous) interval 0
 Peak Active 3GPP2 binding in the elapsed (previous) interval 0
 Peak Active Wimax binding in the elapsed (previous) interval 0
 Elapsed configured interval size is 15 minutes
```

Additionally, the following new debug statements are printed when **debug ip mobile** is enabled:

```
%IPMOBILE-6-OMMETRICS_TIMER_INFO: OM Metric Interval Timer will be started after 1170577
milliseconds.
MobileIP:  OM Metric Sleep Timer is Started
MobileIP:  OM Metric Sleep Timer is Stoped
MobileIP:  OM Metrics Interval Timer is Started for 900005 milliseconds
MobileIP:  OM Metrics Interval Timer is Expired
MobileIP:  OM Metrics Interval Timer is Stoped
MobileIP:  System clock has been updated,
                    So Om Metric Timers will restart
%IPMOBILE-4-OMMETRICS_TIMER_WARNING: Clock skew is more, So Om metric timers will restarts
 metrics interval time is 900000.
 deltaOffset is 39599997.
 currentSystemClock is 3599997.
 nextSystemClock is 50400000.
```

Single IDB for MIP/UDP Tunnels

MIP/UDP RFC 3519 requirements dictate that each MIP/UDP CCoA binding to the MN requires a separate MIP/UDP tunnel. In HA Release 5.0, the HA utilized a hardware/software Interface Descriptor Block (IDB) for each tunnel. Since the system can support a maximum of 16K hardware IDBs, the maximum number of MIP/UDP CCoA bindings is limited to 16K.

Cisco HA Release 5.1 can support hundreds of thousands of MIP/UDP CCoA bindings. In order to support this requirement, we utilize a Single IDB for all types of tunnels.

The Single IDB, or tunnel scalability feature, supports MIP/UDP tunnels only. However, the functionality of other types of tunnels (such as IP/IP and GRE/IP) is not affected.

As part of this feature support:

- Tunnel APIs are modified as required so that other types of tunnels such as IP/IP, GRE/IP, etc., are not affected and remain functional.
- The supported CPS rate for MIP/UDP tunnels (either CoA or CCoA) remains the same as HA 5.0.
- The supported data throughput rates for MIP/UDP tunnels (either CoA or CCoA) remains the same as HA Release 5.0
- The maximum number of supported MIP/UDP tunnels on a 1GB SAMI card will be 80,000. To achieve this number I/O Memory has to be increased from 64MB to 128MB.

Configuring the SAMI for Single IDB

Note To configure the I/O Memory from 64MB to 128MB, issue the **memory-size iomem 128** command, and reboot the card after changing I/O Memory.

Verifying the Configuration

There are no new configuration tasks to implement this feature. The following commands are modified to verify that the Single IDB feature is functional.

show ip mobile tunnel summary command output is modified as follows:

```
#show ip mob tunnel sum
Mobile IP tunnels summary:
```

```
   One IDB used per tunnel for IP/IP, GRE/IP tunnels
   Single IDB used for MIP/UDP tunnels

   Total mobile ip tunnels 2
```

show ip mobile tunnel command output is slightly modified for MIP/UDP tunnels only. The two changes that are applicable to MIP/UDP tunnels are:

- The tunnel number for all MIP/UDP tunnels will be same because all MIP/UDP tunnels are utilizing the single IDB feature.
- Tunnel stats are stored in IDB data structure. Since we have a single IDB for all MIP/UDP tunnels, individual tunnel counters are be displayed for MIP/UDP tunnels. However, aggregate-statistics for all tunnels is displayed using a new show command, **show ip mobile tunnel mip-udp aggregate-statistics**.

The output of the IP/IP and GRE/IP tunnels will remain same.

```
router#show ip mob tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1244
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1245
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
```

The **show ip mobile tunnel mip-udp aggregate-statistics** output will display as follows:

```
router#show ip mob tunnel mip-udp aggregate-statistics
Tunnel0 Aggregate Counters:
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    300 packets input, 45600 bytes, 0 drops
    300 packets output, 39600 bytes
```

In the **show ip mobile traffic** output, the number of keepalives received and sent on all tunnels is displayed under this existing show command. New lines are highlighted below:

```
router#show ip mob traffic
IP Mobility traffic:
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 22961, denied 0, ignored 0, dropped 0, replied 22961
    Register requests accepted 22961, No simultaneous bindings 0
```

```
    . . .
    . . .
    . . .
  MIP/UDP Tunnel:
      Number of Keepalives received (on all tunnels) 13809
      Number of Keepalives sent (on all tunnels) 13809
```

Support for RFC 4917

RFC 4917 specifies the Message String Extension appended to Registration Replies or Registration Revocation messages that are sent to the terminal to provide users with a displayable notification from the network. The text in the extension can be obtained from the AAA server through the RADIUS Reply-Message attribute that is carried in Access-Accept, Access-Reject, or Disconnect (RFC 3576) messages. The RADIUS Change of Authorization does not cause Registration Reply or Registration Revocation messages to be sent. Thus, this message is not supported for the Mobile IP extension.

Debug output that displays mobile registration messages includes registration reply and revocation messages.

To enable this feature, perform the following task:

	Command	Purpose
Step 1	`Router(config)# ip mobile home-agent message-string`	Enables or disables the delivery of the text from the AAA server to the user.

Here is a sample configuration for the Message String extension:

HA Config

```
ip mobile home-agent template Tunnel10 address 10.10.10.188
ip mobile home-agent template Tunnel10 address 10.10.10.203
ip mobile home-agent template Tunnel10 address 10.10.10.179
ip mobile home-agent binding-overwrite
ip mobile home-agent message-string
ip mobile home-agent accounting ha-acct
ip mobile virtual-network 2.0.0.0 255.0.0.0
ip mobile host nai @aricent.com address pool local mip-pool-1 virtual
network 2.0.0.0 255.0.0.0 aaa load-sa lifetime 3600
ip mobile secure mn-aaa spi 101 algorithm md5 mode ppp-chap-style
```

RADIUS Config

```
simulator radius subscriber 123
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  attribute 18 string “Welcome TO Cisco”

simulator radius subscriber 124
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  reply-message RFC4917 “HA-CHAP Failed”
```

CHAPTER 17

Network Management, MIBs, and SNMP on the Home Agent

This chapter contains information pertaining to various aspects of Network Management on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

Operating and Maintaining the Cisco Mobile Wireless Home Agent

This section describes configuration details, statistics, and MIBs supported by the Home Agent. A definitive description of each Mobile IP command can be found at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfmobip.htm

The Home Agent can be managed using either the Cisco IOS CLI or using Cisco Works for Mobile Wireless.

Cisco's Mobile Wireless Home Agent has the following configurable parameters:

- Managing user profiles (local users)
- Configuring IP pools locally
- Configuring security associations with communicating nodes
- Configuring ingress/egress filtering
- Configuring mobile binding updates
- Configuring routing information

Statistics

The Mobile Wireless Home Agent maintains statistics on a global basis for the following parameters:

- Advertisements, received and sent
- Registrations, requests and replies
- Registrations, accepted and denied
- Bindings
- Binding Updates
- Gratuitous and Proxy ARPs
- Route Optimization Binding Updates

The Mobile Wireless Home Agent maintains statistics on a per FA-HA tunnel basis for the following parameters:

- Source and Destination IP address of the tunnel
- Tunnel Type, IPinIP or GRE
- Reverse Tunneling allowed
- Number of Users using that tunnel
- Traffic sent on the tunnel, packets and bytes
- Traffic received on the tunnel, packets and bytes

The Mobile Wireless Home Agent maintains statistics per Host, identified by NAI or Home IP Address, for the following parameters:

- Lifetime
- Session duration
- Traffic transmitted to the host, packets and bytes
- Traffic received from the host on the reverse tunnel, packets and bytes

Note The statistics can be cleared from the CLI. The MIB counters are not cleared.

Tunnel Stats via SNMP

In HA Release 5.1, a new command option is introduced under the **show ip mobile tunnel** command to display entries of the form HA-FA IP pair, along with the number of session users, and packets/bytes statistics.

The command looks like this: **show ip mobile tunnel brief**

Additionally, a new MIB table “cmiHaRegTunnelStatsTable” is added to the CISCO-MOBILE-IP-MIB, and each entry in the stats table contains information shown in the new command option that is introduced.

This feature is applicable only to IP/IP and GRE/IP tunnels.

SNMP, MIBs and Network Management

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The Home Agent supports the MIB defined in The Definitions of Managed Objects for IP Mobility Support UsingSMIv2, RFC 2006, October 1995. An additional Cisco MIB, CISCO- MOBILE-IP-MIB provides enhanced management capabilities. The RADIUS MIB, as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999. A full list of MIBs that are supported on the Cisco 7600 series platform can be found at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Session counters maintained in the MIB cannot be reset using SNMP or the Cisco IOS CLI. Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

Release 3.0 adds a Home Agent Version MIB Object.

SNMPv3 is supported.

HA Release 5.0 MIB Enhancements

In HA Release 5.0, the CISCO-MOBILE-IP-MIB has the MAC address added as a per binding variable. The RADIUS-CLIENT-AUTHENTICATION-MIB contains entries for timeout on AAA access. The trap is added in the CISCO-RADIUS-MIB. The new CISCO-SLB-DFP-MIB is added.

For more information about MIBs, please refer to the following URL:

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

CLI for IP-LOCAL-POOL-MIB

Cisco Mobile Wireless Home Agent Release 3.0 enhanced the CISCO-IP-LOCAL-POOL-MIB to generate traps when pool utilization reached a low threshold or high threshold in percentage. Objects “cIpLocalPoolPercentAddrThldLo” and “cIpLocalPoolPercentAddrThldHi” are defined for the high and low threshold watermark, respectively.

When the percentage of used addresses in an IP local pool equals or exceeds the high threshold, a “cilpPercentAddrUsedHiNotif” notification is generated. Once the notification is generated, it is disarmed and will not be generated again until the number of used addresses falls below the value indicated by “cIpLocalPoolPercentAddrThldLo”.

When the percentage of used addresses in an IP local pool falls below the low threshold, a “cilpPercentAddrUsedLoNotif” notification will be generated. Once the notification is generated, it is disarmed and will not be generated again until the number of used addresses equals or exceeds the value indicated by “cIpLocalPoolPercentAddrThldHi”.

The Cisco IOS 12.3(11)YX5 release implements new variables to the **ip local pool** command to configure the low and high threshold.

The command syntax is as follows:

ip local pool {**default** | ***poolname***} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** *low-threshold high-threshold*]

The *low-threshold* argument is the low threshold to generate pool utilization traps, and *high threshold* argument is the high threshold to generate pool utilization traps.

Additionally, two additional varbinds will be seen in cilpPercentAddrUsedHiNotif notification:

- cIpLocalPoolChildIndex : IP Pool Name
- cIpLocalPoolPercentAddrThldHi: High IP Local Pool threshold percentage value

And two additional varbinds will be seen in cilpPercentAddrUsedLoNotif notification:

- cIpLocalPoolChildIndex : IP Pool Name
- cIpLocalPoolPercentAddrThldLo: : Low IP Local Pool threshold percentage value

Note The CISCO-IP-LOCAL-MIB file has not been changed as per the SNMP SMIv2 standard.

Restrictions

The following restrictions apply to the IP Local Pool Threshold Trap:

- The IP Local Pool name can be up to 240 ASCII characters long (depending on the parameters used).
- SNMP Trap names are limited to a maximum of 48 characters in length because the SNMP MIB only supports names that are up to 48 characters long.
- No Trap is generated if the Pool Name is longer than 48 characters.

How to Configure IP Overlapping Address Pools

This section contains the following procedure:

- Configuring and Verifying a Local Pool Group

Configuring and Verifying a Local Pool Group

This section contains the steps necessary to configure a local pool group and verify that it exists.

SUMMARY STEPS

1. enable
2. configure terminal
3. **ip local pool** {**default** | ***poolname***} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** *low-threshold high-threshold*]
4. **show ip local pool** [*poolname* | [**group** *group-name*]]

Detailed Steps

	Command or Action	Purpose
Step 1	**enable** Example: `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** Example: `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** *low-threshold high-threshold*] Example: `Router(config)# ip local pool XYZPool  100.1.1.1 100.1.1.10 group MWG cache-size 50 threshold 50 90`	Configures a group of local IP address pools, gives this group a name, and specifies a cache size. *low-threshold* is the low threshold configured to generate pool utilization traps. The value of this variable should never be greater than the value the *high threshold.* *high threshold* is the high threshold configured to generate pool utilization traps. The value of this variable should never be less than the value the *lowthreshold.*
Step 4	**show ip local pool** [*poolname* | [**group** *group-name*]] Example: `Router(config)# show ip local pool group testgroup testpool`	Displays statistics for any defined IP address pools.

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.

From the CLI, it is possible to trace activity of all or a particular user identified by NAI. Monitoring the activity of a particular user, called conditional debugging, will display the user activity related to Mobile IP messages and the RADIUS messages.

Starting in Release 3.0, an option is provided to display the condition (username/IMSI), along with each debug statement. This helps to match a debug statement to its condition. To enable this feature, use the following command:

ip mobile home-agent debug include username

The following MobileIP debugs are supported for conditional debugging:

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

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**

Monitoring and Maintaining the HA

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

Command	Purpose
`Router# clear ip mobile binding`	Removes mobility bindings.
`Router# clear ip mobile host-counters`	Clears the mobility counters specific to each mobile station.
`Router#clear ip mobile secure`	Clears and retrieves remote security associations.
`Router#clear ip mobile traffic`	Clears IP mobile traffic counters.
`Router# debug ip mobile advertise`	Displays advertisement information.
`Router# debug aaa pod`	Displays debug information for Radius Disconnect message processing at AAA subsystem level
`Router# debug ip mobile ?` `advertise` Mobility Agent advertisements `dfp` DFP Agent `host` Mobile host activities `ipc` Distributed HA Mobile activities `local-area` Local area mobility `mib` Mobile MIB Events `redundancy` MobileIP redundancy debugging `router` Mobile router activities `udp-tunneling` UDP Tunneling `vpdn-tunnel` VPDN tunnel	Displays IP mobility activities. The following list identifies all of the various options for the debug ip mobile command: • **advertise**-Mobility Agent advertisements • **dfp**-DFP Agent • **host**-Mobile host activities • **ipc**-Distributed HA Mobile activities • **local-area**-Local area mobility • **mib**-Mobile MIB Events • **redundancy**-MobileIP redundancy debugging • **router**-Mobile router activities • **udp-tunneling**-UDP Tunneling • **vpdn-tunnel**-VPDN tunnel
`Router# debug ip mobile host mac`	Displays mobility event information. In HA Release 5.0 a new option is introduced. The **mac** keyword displays the MN identified by the MAC address.
`Router# debug ip mobile redundancy`	Displays display IP mobility events.
`Router# debug radius`	Displays information associated with RADIUS.

Command	Purpose
Router#**debug tacacs**	Displays information associated with TACACS.
Router# **show ip mobile binding**	Displays the mobility binding table.
Router# **show ip mobile binding vrf**	Displays all the bindings on the HA that are VRF-enabled.
Router#**show ip mobile binding vrf realm**	Displays all bindings for the realm that are VRF-enabled.
Router#**show ip mobile globals**	Displays global information for Mobile Agents.
Router# **show ip mobile host**	Displays mobile station counters and information.
Router# **show ip mobile proxy**	Displays information about a proxy Mobile IP host.
Router#**show ip mobile secure**	Displays mobility security associations for Mobile IP.
Router#**show ip mobile traffic**	Displays Home Agent protocol counters. For Single IP, this command shows all redundancy binding counters as 0. For these counters there is a new command introduced **show ip mobile redundancy statistics.**
Router#**show ip mobile redundancy statistics**	Displays the redundancy status of the HA.
Router#**show ip mobile tunnel**	Displays information about the mobile IP tunnel.
Router#**show ip mobile violation**	Displays information about security violations.
Router#**show ip route vrf**	Displays the routing table information corresponding to a VRF.

CHAPTER A

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

MEID—Mobile Equipment Identifier

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