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/docs/wireless/service_application_module/sami/user/guide/samiv1.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*.

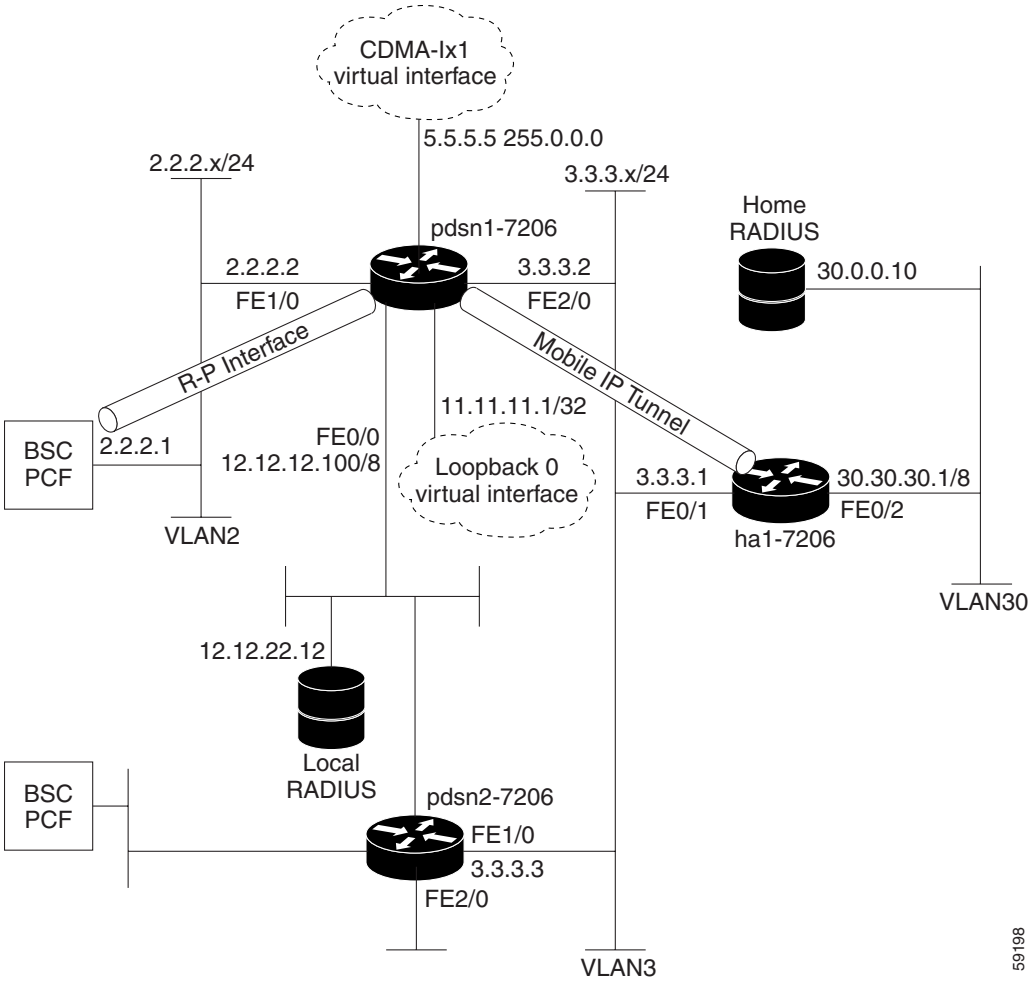
To configure RADIUS in the HA environment, use the following commands in global configuration mode:

	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.