



Release Notes for the Cisco Mobile Wireless Home Agent Feature in Cisco IOS Release 12.4(15)XM

7 February 2008

Cisco IOS Release 12.4(15)XM is a special release that is based on Cisco IOS Release 12.4, with the addition of enhancements to the Cisco Mobile Wireless Home Agent (HA) feature. The Cisco IOS Release 12.4(15)XM is a release optimized for the Cisco Mobile Wireless Home Agent feature on the Cisco 7600 Internet Router platform.

Contents

These release notes include important information and caveats for the Cisco Home Agent software feature provided in Cisco IOS 12.4(15)XM for the Cisco 7600 Internet Router platform.

Caveats for Cisco IOS Release 12.4 can be found on Cisco.com at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/tsd_products_support_series_home.html

Release notes for the Cisco 7600 Router can be found on Cisco.com at:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_release_notes_list.html

This release note includes the following topics:

- [Contents, page 1](#)
- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading the SAMI Software, page 4](#)
- [User Migration, page 5](#)
- [Feature Compatibility and Seamless Migration, page 6](#)
- [Required Base Configuration, page 12](#)
- [Cisco IOS Feature Sets, page 13](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- [MIBs, page 13](#)
- [Cisco Mobile Wireless Home Agent Software Features in Release 12.4\(15\)XM, page 14](#)
- [Caveats, page 15](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 21](#)

Introduction

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.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(15)XM:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Software Compatibility, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading the SAMI Software, page 4](#)
- [User Migration, page 5](#)

Memory Requirements

[Table 1](#) shows the memory requirements for the Home Agent Software Feature Set that supports the SAMI blade on the Cisco 7600 Internet router platform.

Table 1 *Memory Requirements for the SAMI on the Cisco 7600 Router Platform*

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7600 Internet Router	HA Software Feature Set	Sup720-3BXL – Sup IOS 12.2(33)SRC HA Image 12.4(15)XM	256MB	1GB	RAM

Hardware Supported

The Cisco Mobile Wireless Home Agent runs on the Cisco Service Application Module for IP (SAMI) module on the Cisco 7600 Series router. 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.

Software Compatibility

Cisco IOS Release 12.4(15)XM is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(15)XM supports the same features that are in Cisco IOS Release 12.4, with the addition of the Cisco Mobile Wireless HA feature.

Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version EXEC** command:

```
Router#show version

Cisco IOS Software, SAMI Software (SAMI-H1IS-M), Version 12.4(15)XM, RELEASE SOFTWARE
(fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 04-Feb-08 16:35 by prod_rel_team

ROM: System Bootstrap, Version 12.3(20070912:070840) [ramantha-bouncer_091207 101],
DEVELOPMENT SOFTWARE

HA43 uptime is 5 hours, 18 minutes
System returned to ROM by power-on
System restarted at 01:29:25 UTC Tue Feb 5 2008
System image file is "c7svcsami-hlis-mz.124-15.XM.fc4"

Cisco Systems, Inc. SAMI (MPC8500) processor (revision 2.2) with 983040K/65536K bytes of
memory.
Processor board ID SAD114203JW
FS8548H CPU at 1250MHz, Rev 2.0, 512KB L2 Cache
1 Gigabit Ethernet interface
65536K bytes of processor board system flash (AMD S29GL256N)

Configuration register is 0x2102
```

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.

For 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-hlis-ms
Loading c7svcsami-hlis-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 on the SAMI platform.

Here are several Migration scenarios that are possible:

Table 2 Migration Scenarios

	HA R3.0 or Older	HA R3.1 or Older	HA R4.0
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 maintenance 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 3 offers several migration paths:

Table 3 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 configuration change for both hardware and software.

Table 3 Migration Scenarios for the Cisco Mobile Wireless Home Agent on the Cisco SAMI Blade (continued)

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 SRC	Minimal configuration change for hardware and software. Changing from SXF to SRC release for SUP requires chassis reset.
6	7600/redundant SUP720 HA-SLB enabled redundant MWAM (Dual chassis) SUP IOS SXF	7600/redundant SUP720 HA-SLB enabled redundant SAMI (Dual chassis) SUP IOS SRC	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 R4.0, 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 4 offers various steps you need to take in order to migrate to the SAMI platform. Each of the possible migration scenarios is considered.

Table 4 Migration Steps that Correspond to Migration Scenarios from Table 3

Scenario	Migration Steps
1	<ul style="list-style-type: none"> • 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 maintenance window, and service is disrupted).
2	<ul style="list-style-type: none"> • 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 SRC 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	<ul style="list-style-type: none"> • 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. <p>Note SAMI HA R4.0 may not be backward compatible in term of redundancy</p> <ul style="list-style-type: none"> – 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. Syncing bindings from R4.0 to 3.0 and prior works. So far the binding information is only information synced 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. <ul style="list-style-type: none"> • This is the ideal case, and does not have to be done in a maintenance window.
4	<ul style="list-style-type: none"> • 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 maintenance window, and user service will be disrupted. • You must verify HA-SLB.

Table 4 *Migration Steps that Correspond to Migration Scenarios from Table 3 (continued)*

5	<ul style="list-style-type: none"> • For a single chassis, changing from SUP720 SXF to SUP720 SRC resets the whole chassis, so all service modules (such as MWAM and SAMI) are reset, too. • You must perform this migration during a maintenance window. • After this, both SUP720 in the same chassis run SRC release. • Configure the SUP720 to support SAMI: <ol style="list-style-type: none"> 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. <p>If HA redundancy does not work across the releases, perform the following tasks (with more configuration on SAMI HSRP).</p> <ul style="list-style-type: none"> • 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 4 Migration Steps that Correspond to Migration Scenarios from [Table 3](#) (continued)

6	<ul style="list-style-type: none"> • Upgrade chassis #1 from SUP720 SXF to SUP720 SRC. • Configure chassis #1 to support the SAMI blade. <ul style="list-style-type: none"> – 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. <p>If HA redundancy does not work across the releases, perform the following tasks (SAMI HSRP configuration needs to be changed):</p> <ul style="list-style-type: none"> • 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.
---	--

Additional Migration Instructions

The following instructions outline the steps needed to install a new SAMI and configure it so that an application image is booting on the PPCs. These instructions assume that this is a brand new SAMI, not a board being transferred from another chassis.

Upgrade Supervisor Image

You might need a new SUP image in order to recognize the SAMI. The URL to the SUP image that can recognize SAMI will be provided when it is available.

Please note that currently, this process is under review, and will be updated when details are finalized.

Insert the Board into the Chassis

After reloading the SUP, insert the SAMI into the chassis. Make sure to select a slot that has an empty slot above it so the cables can be easily connected.

Set up and connect a console port for the Itasca/LCP console. Also, set up and connect console ports to the PPC1 console. Even if only one will be used initially, there is a front panel port for each daughter card that will be enabled shortly. It will allow multiplexed access to all 3 processors.

Boot SAMI from the SUP

- Copy the latest LCP image to your tftp server.
- Copy the image to the sup.
- Add the following to the sup configuration:


```
boot device module {slot} disk0:sb-csg2-image.bin
```
- Boot the board (LCP Console):


```
boot eobc:
```
- After it boots, log in using admin as both the username and password.

Upgrade the LCP ROMMON

Follow below steps to upgrade the LCP ROMMON:

- Copy the latest stable LCP ROMMON image.
- Copy the latest LCP ROMMON image to the Itasca compact flash.
- Upgrade the ROMMON:


```
reprogram bootflash fur-image image:rommon-image
```
- Reload the blade (LCP Console):


```
reload
```

```
boot eobc: (from the rommon prompt)
```

Boot SAMI from Itasca CF

Below steps illustrate this:

- Copy the latest LCP image to the Itasca compact flash. Example (from LCP console).
- Add the boot command to the Itasca configuration:


```
boot system image:sb-csg2-mzg.bin
```



Note Remove any existing boot system commands first.

- Change the config register to auto boot the Itasca.


```
config-register 1
```
- Reload the board.

Reprogram ROMMON on PPCs

Below steps illustrate this:

- Copy the latest LCP ROMMON image.
- Copy the image to the Itasca.
- Burn the new rommon image on all PPC's. Example (from LCP console):

```
testdc upgrade-rommon BOUNCER_RM.bin
```
- Set the ppc rommon to autoboot. Example (from the PPC console):

```
confreg 0x2102 (This is no longer needed, see note 1)
```

Load and Run PPC Image

- Copy the latest stable ppc application image.
- Copy the image to the Itasca. Example:

```
copy tftp://64.102.16.25/{username}/svcsami-ipbase-mz.sami  
image:svcsami-ipbase-mz.sami_060626
```
- Restart a PPC. Example (from LCP console):

```
testdc restart svcsami-ipbase-mz.sami_060626 proc 1
```

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 to SAMI 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, page 12](#)

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 submenu.
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.

MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 5](#).

Table 5 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be decided
OLD-CISCO-DECNET-MIB	To be decided
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be decided
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be decided
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be decided

Cisco IOS Feature Sets

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.4(15)XM supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XM includes the Cisco Mobile Wireless Home Agent feature. The HA feature is optimized for the Cisco SAMI blade on the 7600 Internet router.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Cisco Mobile Wireless Home Agent Software Features in Release 12.4(15)XM

The Cisco IOS Release 12.4(15)XM supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XM includes the HA feature. The Cisco HA feature is optimized for the Cisco SAMI blade on the 7600 Internet router, and includes the following features:

- Support for Service and Application Module for IP (SAMI)
- Cisco HA 4.0 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.
- The number of SAMI cards that can be supported in a single Cisco 7600 Series Router chassis varies depending on the chassis.



Note

The Cisco Mobile Wireless Home Agent 4.0 release is not supported on the Cisco 7200 or Cisco 6500 Series Router platforms.

- Enhancements to Hot-lining
- Enhancements to Home Agent Quality of Service
- Framed-Pool Standard
- WiMAX AAA Attributes
- MS Traffic Redirection in Upstream Path
- Per Foreign-Agent Access-Type Support
- Support for Max Bindings
- Support for Call Admission Control (CAC)
- MIP/LAC (PPP Regeneration) Support
- Priority-Metric for Local Pool
- Mobile IPv4 Host Configuration Extensions RFC4332
- Mobile Equipment Identifier (MEID) Support
- 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
- 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 SNMP, MIBs and Network Management
- Mobile IPv4 Registration Revocation
- Home Agent Accounting
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE)
- VRF Support on HA
- Radius Disconnect
- Home Address Assignment
- Home Agent Redundancy
- Virtual Networks
- On-Demand Address Pool (ODAP)
- Mobile IP IPSec
- Support for ACLs on Tunnel Interface
- Support for AAA Attributes MN-HA-SPI and MN-HA SHARED KEY
- 3 DES Encryption
- User Profiles
- Mobility Binding Association
- User Authentication and Authorization
- HA Binding Update
- Per User Packet Filtering
- Security

All other software features in Cisco IOS Release 12.4 are described in the documentation for Cisco IOS Release 12.4, which can be found at:

http://www.cisco.com/en/US/products/ps6350/tsd_products_support_series_home.html

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Caveats for Cisco IOS Releases 12.4 can be found on CCO at http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html

The “[Open Caveats](#)” section lists open caveats that apply to the current release and might also apply to previous releases.

The “[Resolved Caveats](#)” section lists caveats resolved in a particular release, which may have been open in previous releases.



Note

If you have an account with CCO, you can use the Bug Toolkit to find caveats of any severity for any release. You can reach the Bug Toolkit at <http://tools.cisco.com/Support/BugToolkit/action.do?hdnAction=searchBugs>

Open Caveats

The following caveats are unresolved in Cisco IOS Release 12.4(15)XM:

- CSCsj60511—Purpose of **clear ip mobile binding all coa** CLI is Not Served
 On a Cisco router running Release 4.0 HA software, the **clear ip mobile binding all coa** option is not working as expected.
Workaround: none.
- CSCsk47814—HA Should Not Send RRQ-HA-IP Attribute for a Successful VRF Call
 On a Cisco router running Release 4.0 HA software, after a successful VRF call, the Home Agent IP address for that realm is *vrf home agent ip address*. Here there is no mismatch between the Home Agent address configured on the HA and the IP address specified in Home Agent field of RRQ. This scenario RRQ-HA-IP should not be included in access request.
Workaround: none.
- CSCsl45076—Memory Leak Found After Unconfig the Service-Policy, at qos stat fo.
 On a Cisco Home Agent (HA) 4.0, with the per-user Quality of Service feature enabled, configuring service-policy for both input and output directions, sending traffic, and then unconfiguring the service-policy causes a memory leak.
 The issue is only seen if the QoS feature is enabled, in cases where policing is configured for both input and output directions, and you unconfigure the service-policy after sending traffic through the bindings.
Workaround: none.
- CSCsl50039—Upgrade Takes Long Time in some New SAMI Modules
 In some Cisco Service and Application Module for IP (SAMI) modules for Cisco7600 routers, the **upgrade** command may take a long time (approximately 11-12 minutes) to finish execution and many timeouts may be observed.
 This problem may happen with some specific types of Compact Flash in the SAMI Linecard Control Processor (LCP).
Workaround: none; although the update process takes longer, the image upgrade completes and the module operates normally.
- CSCsl72185—SAMI Module Status Shows Shutdown Even When it Boots Up
 When a user upgrades the SAMI image from the SUP using the **upgrade** command, the functionality executes correctly, but the show information at the moment of process appears incorrectly. While the SAMI card is in the process of coming up, the **show module** should show the module status as “Other”, but now it shows “shutdown”. When the SAMI card finally comes on-line, the **show module** status is displayed correctly as “OK”.
 This condition occurs during during the upgrade process.
Workaround: none.

- CSCsm02215—CPU Goes Beyond 90% While Running GetMany Command for CISCOMobileIpMIB

On Cisco Home Agent (HA) 4.0, with more than 15K bindings, querying the ciscoMobileIpMIB for all the bindings, with 5k handoff, 10K flap, and downstream traffic being sent causes the CPU to go beyond 90%.

The CPU goes beyond 90%, when the ciscoMobileIpMIB is queried for more than 15k bindings when 5k bindings are handed off, 10k are flapped, and downstream traffic is sent.

Workaround: none.
- CSCsm04576—HA R4.0: Memory Leak Found @ Process Name: MobileIP Standby

On a Cisco router running the HA 4.0 release software, a memory leak occurs in newly coming up standby HA.

This condition occurs only when per user ACL is used, and during sync update occurs before the bulk update occurs.

Workaround: none.
- CSCsm04725—HA R4.0: Unexpected debug msg with memory ref seen with VPDN failure

An extra debug line shows up when debugging is not enabled.

This condition occurs when VPDN fails for MIPLAC.

Workaround: none.
- CSCsm05763—HA R4.0: RedBind Update Being Sent for Hotlining COAs for MIPLAC Binding

On a Cisco router running the HA 4.0 release software, redundancy updates are sent to the standby Ha for MIP-LAC sessions when hotlining COA message is received even though redundancy is not supported for MIP-LAC sessions.

This condition occurs if hotlining is enabled for MIP-LAC sessions, when a COA message comes for the same redundancy update is sent to standby even though redundancy is not supported for MIP-LAC sessions.

Workaround: none.
- CSCsm07799—Chunk Leaks and Low IOMem Hit Even With 25k Bindings - Scalability Limit

A memory leak is identified when IOMem is low and the CPU is hit.

The low IOMEM is hit only when the HA is purged with a high rate of CoAs.

Workaround: none.
- CSCsm12641—HA Reloaded While Configuring no router mobile

On a Cisco router running Release 4.0 HA SAMI software, configuring **no router mobile** reloads the HA.

This condition occurs only when you configure **no router mobile**.

Workaround: none.

- CSCsm14422—MIP Binding Open Fails With 3GPP2 Attributes for RRQ without GENAE
MIP binding open fails for RRQ without GENAE.
This condition occurs when a MIP binding for a 3GPP2 user is authenticated with 3GPP2 attributes 57 and 58 (MN-HA shared key and MN-HA SPI) for MHAE.
Workaround: configure the following Cisco vsa for MHAE instead of 3GPP2 attributes:
vsa cisco generic 1 string "mobileip:spi#0=spi 11111 key ascii yyyy replay timestamp within 200"
- CSCsm14831—HA R4.0: Debug Message to Identify the Missing Config Access-Type
On a Cisco router running HA R4.0, the debug message "SA Not Retrieved" does not indicate the access-type of FA.
This condition occurs if the access-type of FA is missing.
Workaround: none.
- CSCsm17186—User Being Hotlined Although Reverse Tunnel is Disabled
On a Cisco router running the HA 4.0 release software, a non-reverse tunnel user is being hotlined
This issue occurs under the following conditions:
 - a. Open a normal MIP binding without enabling reverse tunneling.
 - b. Send a COA with ip-redirect rule.
 After step b. the CoA should get NACKed as reverse-tunnel is not enabled for the user and cannot be made hotlined. But now the Coa is NACKed, an accounting stop/start pair is initiated, the user is hotlined and the rule is applied
Workaround: enable reverse tunnel for a hotlined user.
- CSCsm17204—Access-reject Not Being Sent For a Non-reverse Tunneled User
Ideally, the Home Agent will reject the RRQ if Reverse-Tunnel is not requested by the user and hotlining policy is downloaded for the user.
The current behavior is that when there is an access-accept and the hotlining policy is downloaded, the debug displays that the user is made hotline active, but the binding is not hotlined.
Workaround: reverse tunneling should be enabled for a hotlined user.
- CSCsm34309— Issue with Conditional Debugging for Hotlined User
When a hotlined user is brought back to normal , and conditional debugging is on for RADIUS debugs of the accounting stop/start pair, we only see a RADIUS accounting stop message. The "Accounting Start" message is not displayed.
Workaround: none.
- CSCsm38451—HA R4.0: Tracebacks found on HA for every upstream packet
For every upstream packet through the MIP/LAC tunnel, a traceback occurs.
This happens only when the packet is switched through process path (most likely, when both CEF and fast switching are disabled through CLI).
Workaround: do not disable fast and CEF switching.

- CSCsm38957— **clear ip mob bin all sync** Initiates del sync Request to the Standby for MIPLAC

A delete sync request message occurs from active to standby for MIPLAC bindings. This is seen on the counters of the **show ip mobile traffic** command. There is no impact.

When a MIPLAC session is cleared with **clear ip mobile binding all sync**, it initiates delete sync request to standby.

Workaround: none.
- CSCsm41386—Memory Leak Found During the long run of MIP-LAC test

Memory leak and memory leak chunks are noticed after 8 hours of MIP-LAC testing involving registration / re-registration of 8K MIP-LAC sessions.

This happens after 8 hours of MIP-LAC testing (opening 8K MIP-LAC sessions and leave them open for 8 hours).

Workaround: none.
- CSCsm45543—Framed IP Address Attribute is Missing in Access-Request

On a Cisco router running Release 4.0 HA software, the framed IP address attribute is missing in an access request when opening a MIP flow of Wimax.

This occurs when opening a MIP flow of WiMAX type only.

Workaround: none.
- CSCsm45978-RRQ-MN-HA-SPI Attribute 19 and 20 Bindings Do Not Come Up (WIMAX)

Bindings are coming up when using WIMAX attributes 19 and 20 MN-RRQ-HA-IP .

This condition occurs when you configure attribute 19 and 20 in the AAA server. The bindings are not seen.

Workaround: none.
- CSCsm46468—Mem Leak Found During QoS Testing in Both Active and Standby HA

On a Cisco router running the HA 4.0 release software, memory leaks are seen in both active and standby HA when a switchover is triggered during a QoS stress test.

Workaround: none
- CSCsm51252—Multiple ACL in Subscriber Profile Leads to - 130 Insufficient Resource

On a Cisco router running the HA 4.0 release software, bindings fail to get created when more than one in and out ACL are configured in the AAA server subscriber profile.

Workaround: configure only one IN and OUT ACL.
- CSCsm51925—Alignment Errors and Reload @ ipmobile_GetSPI in MIP-LAC

On a Cisco router running Release 4.0 HA MWAM software, the HA reloaded when mip-lac user authenticates locally on the HA.

Workaround: none.

- CSCsm55178—Reload @ ip_forward during MIPLAC+QoS testing
The HA reloads during load test of around 5 hours where MIPLAC bindings are flapped(open/close).
This condition occurs when you enable QoS policing on the MIPLAC sessions that are open/closed.
Workaround: none.
- CSCsm55222-HA Reloads with Traceback SYS-2-BADBUFFER @ ip_feature_fastswitch
On a Cisco router running the HA 4.0 release software, the HA reloads during stress testing on MIPLAC functionality with IMIX upstream traffic.
This condition occurs when bindings are flapped at a slow rate.
Workaround: none.

Resolved Caveats

There are no resolved in Cisco IOS Release 12.4(15)XM.

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 20](#)
- [Platform-Specific Documents, page 20](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4T:

- *Cisco Mobile Wireless Home Agent Feature for Cisco IOS Release 12.4(15)XM* at the following url:
http://www.cisco.com/en/US/products/ps6706/products_feature_guides_list.html

Platform-Specific Documents

Documentation specific to the Cisco 7600 Router is located at the following location:

- On Cisco.com at:
http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2008, Cisco Systems, Inc.
All rights reserved.

