Release Notes for the Cisco Mobile Wireless Home Agent Feature in Cisco IOS Release 12.4(15)XM3

31 July 2009

Cisco IOS Release 12.4(15)XM3 is a special release that is based on Cisco IOS Release12.4, with the addition of enhancements to the Cisco Mobile Wireless Home Agent (HA) feature. The Cisco IOS Release 12.4(15)XM3 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)XM3 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:

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

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)XM3:

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)XM3	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.

Cisco MW HA Release 12.4(15)XM3 is supported on the following platforms:

- Cisco 7600 Internet Router platform—Please refer to the following URL for installation and configuration information:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/pref.html

Software Compatibility

Cisco IOS Release 12.4(15)XM3 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(15)XM3 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) [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-h1is-mz.124-15.XM3"

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-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 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 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 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 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.

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

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 SUP72 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	• 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).

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

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 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	• 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. Synching bindings from R4.0 to 3.0 and prior works. 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 4 Migration Steps that Correspond to Migration Scenarios from Table 3 (continued)

5	• 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 maintanence window. • After this, both SUP720 in the same chassis run SRC 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 4 Migration Steps that Correspond to Migration Scenarios from Table 3 (continued)

6	• Upgrade chassis #1 from SUP720 SXF to SUP720 SRC. • 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.

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

Perform the following tasks to boot the SAMI card from the SUP:

Step 1 Copy the latest LCP image to your TFTP server.

Step 2 Copy the image to the SUP.

Step 3 Add the following to the SUP configuration:

```
boot device module {slot} disk0:sb-csg2-image.bin
```

Step 4 Boot the board (LCP Console):

```
boot eobc:
```

Step 5 After the SAMI card boots, log in using “admin” as both the username and password.

Upgrade the LCP ROMMON

The following steps illustrate how to upgrade the LCP ROMMON:

Step 1 Copy the latest stable LCP ROMMON image.

Step 2 Copy the latest LCP ROMMON image to the Itasca compact flash.

Step 3 Upgrade the ROMMON:

```
reprogram bootflash fur-image image:rommon-image
```

Step 4 Reload the blade (LCP Console):

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

Boot SAMI from Itasca CF

The following steps illustrate how to boot the SAMI from the Itasca compact flash:

Step 1 Copy the latest LCP image to the Itasca compact flash. Example (from LCP console).

Step 2 Add the boot command to the Itasca configuration:

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

Note Remove any existing boot system commands first.

Step 3 Change the config register to auto boot the Itasca.

```
config-register 1
```

Step 4 Reload the board.

Reprogram ROMMON on PPCs

To reprogram the ROMMON on the PPCs, perform the following tasks:

Step 1 Copy the latest LCP ROMMON image.

Step 2 Copy the image to the Itasca.

Step 3 Burn the new rommon image on all PPC's. Example (from LCP console):

```
testdc upgrade-rommon BOUNCER_RM.bin
```

Step 4 Set the ppc rommon to autoboot. Example (from the PPC console):

```
confreg 0x2102
```

Load and Run PPC Image

Perform the following tasks to load and run the PPC image:

Step 1 Copy the latest stable ppc application image.

Step 2 Copy the image to the Itasca. Example:

```
copy tftp://64.102.16.25/{username}/svcsami-ipbase-mz.sami
image:svcsami-ipbase-mz.sami_060626
```

Step 3 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 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.

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.

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)XM3 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XM3 includes the Cisco Mobile Wireless Home Agent feature. The HA 4.0 feature set 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)XM3

The Cisco IOS Release 12.4(15)XM3 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XM3 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

There are no new unresolved caveats in Cisco IOS Release 12.4(15)XM3:

- CSCta85459—HA Fails to Send Revocation Message When Having Multiple Bindings

  With multiple sessions of same nai and different address on HA, HA fails to send revocation message when having multiple bindings .

  This issue is seen only for NAI-based users. For non-NAI based users, it works fine.

  Here are the steps to recreate this issue.

  - Enable MIP registration Revocation on PDSN and HA by configuring **ip mobile foreign-service revocation** and **ip mobile home-agent revocation**.
  - Configure FA-HA authentication parameters on the PDSN and HA.
  - Open two MIP flows on the PDSN/HA for the same user.
  - Clear the first MIP flow on the HA by issuing the **clear ip mobile binding** command.
  - HA will fail to send revocation message.
  - Clear all MIP flows on the HA using the **clear ip mobile binding all** command.
  - HA suceeds.

  Workaround: For non-NAI based it works fine.

Unresolved Caveats Prior to 12.4(15)XM3

The following caveats are open in IOS Release 12.4(15)XM2:

- CSCek65827—Avoid Trying to Write to Standby Supervisor When Not Present

  Error message “Failed to upload config to standby” is seen when there is an attempt to write on a card when standby SUP is not present.

  Workaround: none.

- CSCsr19808—Traffic Fails Through MIPLAC Session wth NAT Enabled

  On a Cisco router running HA(c7svcsami-h1is-mz_080721) software, traffic failed through MIPLAC session.

  This happens when bindings are created with NAT enabled between HA/LAC and FASIM.

  Workaround: none.

- CSCsr62914—Framed IP address Not Sent in Access Request

  When you configure the **radius-server attribute 8 include-in-access-req** command, the RADIUS Attribute 8 (Framed-IP-Address) is not contained in the Access-Request.

  Workaround: none.

- CSCsr62995—**show ip mobile secure host** Does Not Display Key Properly

  The HMAC MD5 key does not sync completely to the standby in a redundant setup. Only 16 bytes of the 20 bytes key syncs up.

  This condition occurs when the key length is greater than or equal to 20 bytes.

  Workaround: none.

- CSCsr67110—Revocation Not Supported After Switchover With HA-RK

Revocation will fail with HA-RK.

Workaround: none.

- CSCsr67141—CUI Sent With Wrong Value in Acess-Request

  A CUI (Chargeable User identity) is sent with value other than NULL in access-request.

  This condition occurs when HA sends access-request to AAA for re-registration.

  Workaround: none.

- CSCsr70803—Stale FHAE Keys Seen on Home Agent

  Failing RRQ with FHAE authentcation failure.

  This condition occurs when you configure Security Associations with Binding in the system

  Workaround: unconfigure previously configured local FA-HA SPI and key. Additionally, do not configure Security Association with bindings in the system.

- CSCsr72927—**resync-sa** Functionality Broken

  Re-registration fails when security associations are re-synched

  Re-registration fails when a new SPI and key comes, and when load-sa is configured along with resync-sa,

  Workaround: none.

- CSCsr73005—Additional Configuration Seen When **resync-sa** is Configured

  When you configure the **ip mobile home-agent resync-sa** command, the **ip mobile home-agent reject-static-addr** command also is configured.

  Workaround: manually unconfigue the **ip mobile home-agent reject-static-addr** command.

- CSCsr76554—Failed to send VPDN request to LNS over AAA

  On a Cisco router running HA Release 4.0 software, the HAfailed to initiate a MIPLAC session over AAA.

  Workaround: none.

- CSCsr82781—HA is Not Accepting Piggybacked HA-RK SPI, Keys and Lifetime

  For every new HA-RK key generated, re-registration is sent to RADIUS.

  This condition occurs when HA-RK key, SPI and lifetime are piggybacked; they are not accepted by the HA.

  Workaround: none.

- CSCsr93284—Not Able to Create Bindings Without FHAE

  Unable to create a binding.

  Topology

  ```
        | -------------------------FA-A(w/FHAE)---------------------------|
  MN-A                                                                HA
        |-------------------------FA-B(wo/FHAE)------------------------- |
  ```

  This condition occurs during the following scenario:

  - MN-A connect HA via FA-A
  - MN-A handoff to FA-B
  - MN-A handoff to FA-A—HA-RK lifetime expires on HA
  - MN-A handoff to FA-B : Problem Occurs on this connection try.

  Workaround: none.

- CSCsu01576—Per domain Authentication Using Different Server-groups Not Supported

  Per domain authentication using different servers groups is not being supported on the HA. Even in cases where VRF is used, all domains use the same server group. This is not the desired behavior.

  Workaround: none.

- CSCsu07999—HA Drops Fragmented Packet Less Than 5 Bytes of Data

  The HA drops incoming packets from the MN.

  This condition occurs when the packets that are coming in are fragmented, and the size of the second packet is is less than 64 bytes. When this happens, the ethernet layer pads them. Only when they are padded is the packet dropped.

  Workaround: none.

- CSCsu20447—Deregistration Failed When VRF is Downloaded from AAA with OSPF

  Deregistration failed after a switchover when VRF is downloaded from AAA with OSPF configured.

  Workaround: none.

- CSCsu24283—Tracebacks and Spurious Memory Access Detected in Home Agent

  On a Cisco Home Agent running the 12.4(15)XM2 image, tracebacks and spurious memory were detected while opening and closing bindings with tunnel template configured.

  Workaround: none.

Unresolved Caveats Prior to IOS Release 12.4(15)XM2

The following caveats are unresolved in Cisco IOS Release 12.4(15)XM1:

- CSCso45075—HA crashed while sending CoA from RSIM

  The HA crashed while sending CoA requests.

  This problem occurs when you send the coa request for the profile with the following attributes configured:

  vsa vendor-id 5535 code 139 binary 00000011

  vsa vendor-id 5535 code 130 binary 62345600

  vsa vendor-id 3729 code 11 binary 0010

  Workaround: none.

- CSCso77952—Failed to Parse avp 31 During the ICCN Phase in SIP-VPDN Call

  On a Cisco router running HA(c7svcsami-h1is-mz_080330) software, the HA failed to parse avp 31 during the ICCN phase in a SIP-VPDN call with "avp-hidden" attribute from AAA.

  Workaround: none.

- CSCso78391—Traceback Seen While Redistributing Mobile Virtual Networks to ospf -vrf

  On a Cisco router running HA(c7svcsami-h1is-mz_080330) software, a traceback was seen while redistributing mobile virtual networks to ospf -vrf.

  Workaround: none.

- CSCsq06343—High CPU Observed for 5K Bindings 50 Mbps Traffic

  High CPU is observed and bindings start getting deleted.

  This condition occurs when around 5K bindings are present, all the bindings created have QoS enabled on them, and there is a 5MBps traffic flowing in both directions continuously for around 5 hours.

  Workaround: none.

- CSCsq16441—AAA WiMAX Attribue 28 and 29 not Supported

  Wimax binding fails to come up when AAA is configured with WiMAX attributes 28 and 29, and are sent in Access-Accept.

  Workaround: Access-Accept should not contain WiMAX attributes 28 and 29 (26/28, 26/29).

- CSCsq38262—Sup32: PPCs Fail To Download Configuration Unless Boot String is Configured in Sup

  SAMI processors fail to download configuration from supervisor. EOBC traffic does not work. Session from supervisor to processors 1-8 does not work.

  One or more of the following conditions can cause the problem:

  - Sup32 is used in the chassis without executing boot eobc method of upgrade once.
  - LCP rommon version 121 was used now or prior on the SAMI.
  - Sup32 is used following Sup720/RSP720 or vice versa, with the same SAMI.
  - Booting through eobc is used with different version of supervisor.

  Workaround:

  Perform the following tasks once after SAMI is moved from a Sup720/RSP720 chassis to Sup32 chassis, or vice versa:

Step 1 Configure the boot string on the supervisor:

```
Sup(config)#boot device module sami-slot disk0:sami image
```

Step 2 Reset the SAMI card to boot normally—general case, where SAMI has a usable image on its compact flash.

```
Sup#hw-module module sami-slot reset
```

OR

Boot the SAMI card through EOBC from supervisor:

```
Sup(config)#boot device module sami-slot disk0:sami image
Sup#hw-module module sami-slot boot eobc
Sup#hw-module module sami-slot reset
```

After SAMI comes up, use the **upgrade** command to make sure the image is stored on the SAMI and comes back up automatically on reboot:

```
Sup#upgrade hw-module slot sami-slot software disk0:sami image
```

Step 3 SAMI boot string can be un-configured on the supervisor. Leaving it there will not cause a problem .

```
Sup(config)#no boot device module sami-slot disk0:sami image
```

- CSCsq46332—Traceback While Binding When PMIP is Configured on FASIM

  Bindings do not come up with memory allocation failure and traceback.

  This condition occurs when the HA receives a RRQ with nvse and cvse extensions of vendor-id type 9 (cisco) and proxy type.

  Workaround: ensure that the RRQ does not contain nvse and cvse of vendor-id type 9.

- CSCsq64929—HA Processor Hanged While Unconfiguring VRF Configs

  The HA processor hangs while unconfiguring vrf sub interface.

  This condition occurred after configuring 500 VRFS, keeping it for 4-5 hours, then unconfiguring one sub interface.

  Workaround: do not unconfigure the sub interface.

- CSCsq65155—HA Rejects RRQ with an Extension 147

  Access-Request to AAA does not contain SPI attribute, so registration of MN fails.

  This condition occurs when the HA receives RRQ with 147 extension (PMIP skippable extension).

  Workaround: RRQ should be sent without the 147 extension..

Unresolved Caveats Prior to Cisco IOS Release 12.4(15)XM1

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 Idenitfy 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.

  CSCsm36593—Data Path Fail to Proc 1 (NP1)

  When the HA is under a load of 40K flaps with less traffic @40 MBPS.

  HA restarts due to data path fail to proc 1.

  Workaround: switch off **fast switching no ip route-cache** on interface

- 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 initates 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 RSIM. 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 Rasim 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

The following caveats are resolved in Cisco IOS Release 12.4(15)XM3:

- CSCsm57705—RCP Debug Messages Should be Printed Based on IFS Verbose Flag

  When the "write memory" is done from SAMI in config-on-sup mode, if the standby SUP is not present, RCP messages are printed on the console. Standby SUP not being present is a valid scenario and no error messages have to be printed on the screen. The RCP debug messages are printed without any debug flag. The debug messages should be printed based on whether the verbose flag sent to the ifs API's.

  This condition occurs when the standby SUP is not present and "write memory" is done from SAMI processor in config-on-sup mode.

  Workaround: none.
- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.
- CSCsq31776

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.
- CSCsq68357—*invalid_group_handle* on Removing and Configuring Servergroup

  Error message "Invalid group handle" is seen when trying to bring up a session.

  This condition occurs when configuring client and NAS for a PPPoe session, and then when triggering a session from the client, the following message is seen:

Error Message `%AAA-3-BADSERVERTYPEERROR: Cannot process authentication server type *invalid_group_handle*`

While removing the server-group and configuring the same server-group.

Workaround: none.

- CSCsr38182—Dynamic ACL Info is not Getting Updated on TP for a Specific Host Address

  The issue is observed when rule-based Rules are downloaded with values src-ip/mask and dst-ip/mask value. The Rules are not created correctly on the Home Agent.

  This condition occurs when rule-based hotlining is enabled on HA and Rules are downloaded from AAA during Access-Accept or CoA.

  Workaround: none.
- CSCsr62914—Framed IP Address not Sent in Access Request

  When you configure the **radius-server attribute 8 include-in-access-req** command, RADIUS Attribute 8 (Framed-IP-Address) is not contained in Access-Request.

  Workaround: none.
- CSCsr62995—**Show ip mobile secure host** Does Not Display Key Properly

  The HMAC MD5 key does not sync completely to the standby in a redundant setup. Only 16 bytes of the 20 bytes key syncs up.

  The key length is >=20 bytes

  Workaround: none.
- CSCsr72927—"resync-sa" Functionality Broken

  Re-registration failure occurs with re-synch SA.

  This condition occurs when a new SPI and key comes, when Load-sa is configured along with resync-sa, re-registration fails

  Workaround: none.
- CSCsr73005—Additional Configs Seen, When We Configure "resync-sa"

  Additional CLI **ip mobile home-agent reject-static-addr** is seen

  When you configure the **ip mobile home-agent resync-sa** command, the **ip mobile home-agent reject-static-addr** command automatically gets configured as well.

  Workaround: manually unconfigure the **ip mobile home-agent reject-static-addr** command.
- CSCsu01846—Authentication Per Realm with VRF fails on HA4.0

  Authentication Server Groups Per Realm with VRF feature does not work in HA4.0.

  Authentication Server Groups Per Realm with VRF feature is explained in Configuration Guide of 12.4(15)XM1.

  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.

  According to this document, it should be configure multiple RADIUS server for each realm with VRF in HA4.0.

  Workaround: none.

- CSCsu07999—HA Drops Fragmented Packet Less Than 5 Bytes of Data

  The HA drops incoming packets from the MN.

  This condition occurs when the packets that are coming in are fragmented, and the size of the second packet is small, and is less than 64 bytes in itself because of which ethernet layer pads them. Only when they are padded is the packet dropped.

  Workaround: none.

- CSCsu18124—Revocation Request Fails on Multi-VRF Environment

  If each session has the same home address under the multiple VRF environment, the **clear ip mobile clear binding all sync** command deletes the session from the HA. However only one revocation request is sent to the BWG. Other sessions remain on the BWG.

  The issue is found at the HA4.0 Wimax environment, and the HA is configured multiple VRF that has the same prefix. If this issue occurs, accounting information is corrupted.

  Workaround: none.

- CSCsu20447—Deregistration Failed When VRF is Downloaded from AAA with OSPF

  Deregistration failed after switchover. This condition occurs when VRF is downloaded from AAA with OSPF configured.

  Workaround: none.

- CSCsu24283—Tracebacks and spurious memory access detected in Home Agent

  On Cisco Home Agent running 12.4(15)XM2 image tracebacks and spurious memory were detected while opening and closing bindings with tunnel template configured.

  Workaround: none.

- CSCsu64794—HA Stops Sending RadiusTestPacket After Server is Marked Dead

  RADIUS test packet is not sent after the server is marked DEAD. This issue is seen with following radius server configuration:

  ```
  radius-server deadtime 1
  radius-server host 10.2.2.2  test username cisco1@cisco.com idle-time 1
  radius-server host 10.3.3.3  test username cisco1@cisco.com idle-time 1
  radius-server host 10.4.4.4  test username cisco1@cisco.com idle-time 1
  ```

  Once the HA stops sending Radius test packet, server keeps status of DEAD, it never come to active.

  Workaround: none.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsv06584—“Overall Service Time” Shows Incorrect Value (7w0d) After Handing Off FA

  “Overall service time” in **show ip mobile host** command shows incorrect value (7w0d) after handing off from one FA to another, then the value comes back to correct value when the HA returns to the original FA.

  This condition occurs under the following conditions:

  - HA with Wimax attributes.
  - After Handing off from one FA to another.

  Workaround: none.

- CSCsv18275—Standby HA Cannot Create Binding with 246 length Acct-Multi-Session-ID

  Standby HA fails to create Mobile IP binding when the active HA received a Radius Access Accept included 246 bytes length of the AAA-Session-ID.

  Even though the standby HA fails to create the bindings with 246 length AAA-Session-ID/Acct-Multi-Session-ID, this binding is created on the active HA without any problem.

  Workaround: none.

- CSCsv25763—**clear ip mobile binding nai** NAI Clears Wrong Users.

  When using VRF, and when there is overlapping MN’s IP address among MNVO(VRF), **clear ip mobile binding nai** NAI clears wrong users.

  Example:

  ```
  NAI(IP Address)
  001@mvno1.test(10.200.0.1)
  001@mvno2.test(10.200.0.1)
  001@mvno3.test(10.200.0.1)

  clear ip mobile binding nai 001@mvno2.test synch

  001@mvno1.test(10.200.0.1) -> Clear
  001@mvno2.test(10.200.0.1) -> Not Clear
  001@mvno3.test(10.200.0.1) -> Clear
  ```

  This condition occurs on a Cisco7609 running Cisco IOS Release 12.4(15)XM2 on a SAMI card.

  Workaround: none.

- CSCsv41454—“Dynamic IP Pool allowing Static Access' Does Not Work Properly

  RRQ is rejected unexpectedly when using “Dynamic IP Pool allowing Static Access”.

  Here is the scenario.

  - RRQ (HoA=a.b.c.d, NAI=test@wimax):From FA
  - RRP Code:0 :To FA
  - RRQ (HoA=0.0.0.0, NAI=test@wimax):From FA
  - RRP Code:0x82 :To FA

  The expected result in the above 4 should be to update the session. When HoA is set as 0.0.0.0 in the above 1, the session is updated by 2nd RRQ correctly.

  This issue occurs under the following conditions:

  - HA with Wimax attributes.
  - HA Address management is configured as “Dynamic IP Pool allowing Static Access”.

  Workaround: none.

- CSCsv57656—**show ip mobile binding** with NAI and HoA Display Unexpected in VRF Environment

  show ip mobile binding with **nai** and *ip address* option is showing all binding information that has the same HoA in multiple VRF environment as below.

```
MobileHomeAgent#show ip mobile binding nai 001@test1.cisco.com 10.0.0.1
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is NTP, 09:28:28.804 JST Fri Oct 31 2008

Mobility Binding List:
001@test3.cisco.com:
    Home Addr 10.0.0.1
    Care-of Addr 192.168.1.100, Src Addr 192.168.1.100
    Lifetime granted 01:23:20 (5000), remaining 01:22:27
    Flags sbdmg-T-, Identification CCB4CF78.14662000
    Tunnel2 src 192.168.2.3 dest 192.168.1.100 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Revocation negotiated - I-bit not set
    VRF test3
    Acct-Session-Id: 0x00000089
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Next-hop set for any-traffic to 172.16.3.100
001@test2.cisco.com:
    Home Addr 10.0.0.1
   Care-of Addr 192.168.1.100, Src Addr 192.168.1.100
    Lifetime granted 01:23:20 (5000), remaining 01:22:26
    Flags sbdmg-T-, Identification CCB4CF77.14572000
    Tunnel1 src 192.168.2.2 dest 192.168.1.100 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Revocation negotiated - I-bit not set
    VRF test2
    Acct-Session-Id: 0x00000088
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Next-hop set for any-traffic to 172.16.2.100
001@test1.cisco.com:
    Home Addr 10.0.0.1
   Care-of Addr 192.168.1.100, Src Addr 192.168.1.100
    Lifetime granted 01:23:20 (5000), remaining 01:22:25
    Flags sbdmg-T-, Identification CCB4CF76.1681E000
    Tunnel0 src 192.168.2.1 dest 192.168.1.100 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Revocation negotiated - I-bit not set
    VRF test1
    Acct-Session-Id: 0x00000087
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Next-hop set for any-traffic to 172.16.1.100
MobileHomeAgent#
```

It should display only “001@test1.cisco.com” binding entry.

This condition is confirmed 12.4(15)XM2

Workaround: none.

- CSCsv58240—**clear ip mobile binding ip-address synch** Deletes Binding Unexpectedly

  The **clear ip mobile binding** *ip address* **synch** command deletes bindings unexpectedly like those below.

  If there are NAI-based bindings on the HA with VRF environment and you execute the **clear ip mobile binding 10.0.0.1 synch** command, the following result is observed.

  ```
  001@test3.cisco.com -> deleted
  001@test3.cisco.com -> not deleted
  001@test3.cisco.com -> deleted
  ```

  It should not delete NAI-based bindings, so this command should be available for the user identified by IP address.

  This condition is confirmed in Cisco IOS Release 12.4(15)XM2.

  Workaround: none.

- CSCsw21999—Memleak on Standby HA with Per User IN/OUT ACLs

  Memory leak is observed on the standby-HA during bindupates received with per-user in/out ACLs when the active-HA receives RRQ for re-registration. The leak is observed on the standby HA when the active HA downloads the RADIUS filter-id [11] attribute for locally configured in/out ACLs.

  The leak is observed on the standby HA when the active HA downloads filter-id[11] attribute or cisco-av-pair mobileip in/out acl attributes during authentication with AAA server.

  Workaround: do not download either the filter-id or cisco-av-pair in/out acl attributes if those values are not configured locally on the HA.

- CSCsw27536—HA-RK context is created from attributes of two different Access-Accept

  HA-RK context is created with the HA_RK attributes Even though binding creation is not successful.

  If two Access-Accepts are received containing the HA-RK attributes such as:

  The first one with

  – HA-RK key

  – HA-RK lifetime

  and the second Access-Accept with

  – HA-RK SPI

  Workaround: configure all the attributes related to HA-RK for the initial RRQ.

- CSCsw43148—High CPU is noticed when using 1500+ MIP/UDP CCoA tunnels on Home Agent

  In customer deployment, when having 1500 MIP/UDP CCoA tunnels on Home Agent/HA (which is running HA 4.0 release image), traffic flowing through these 1500 tunnels is causing high CPU.

  This high CPU issue is hit only when MIP/UDP tunneling is being used by the customer. Upstream traffic (i.e., traffic entering tunnels on HA) is 20 Mbps. Downstream traffic (i.e., traffic leaving tunnels on HA) is 50 Mbps.

  Workaround: the high CPU only occurs in case of MIP/UDP tunnel.

- CSCsx28401—Incorrect Processing of Keepalive Packets Received on HA

  Incorrect processing of NAT keepalive messages received in the HA.

  Workaround: none.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsx68809—SAMI PPC Reboot Stops After Multiple Iterations (Non-Single-IP)

  When the PowerPC processors are reloaded, they hang, unable to boot. Session does not work, and the **show sami processors** command run on the LCP (processor 0) yields the status of the Processor as “ROMMON INITIALIZING (0x00000800)”, they are unable to go beyond this state in the bootup process.

  The PowerPC processors must have been rebooted around 250 times for this to happen, without reloading the complete SAMI card in the process. (If all the 6 are rebooted, then it can happen in 42 times, 42X6=252).

  Workaround: Reboot the SAMI card.

  To confirm that you are facing this issue, session to the LCP (processor 0) of the SAMI from the SUP. And then execute:

  ```
  debug sami ppc_download errors
  ```

  And then reload any one processor.

  ```
  reload sami processor 3
  ```

  You should see an error stating “Failed to open file”. Execute **show sami processors**, which should show that the processor you just reloaded remains in the “ROMMON INITIALIZING (0x00000800)” state. If both of these conditions are satisfied, then this confirms that this bug is causing this behavior.

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- CSCsy15227

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsz04598 - Home Agent not requesting default gw in DHCP Discover message

  Cisco Home Agent running release 12.4(22)YD software and acting as proxy DHCP client is not requesting default GW in DHCP Discover message when it receives MN Host Config subtype 0 and 5.

  Workaround: none.

- CSCsz16702—Host Configuration Extensions Received in DHCP Offer are lost After MN re-reg

  Host configuration parameters obtained from DHCP server are not send back in RRP by the HA after initial registration.

  This condition occurs after first-timer registration message. Any re-reg will not get host configuration parameters sent by the DHCP server.

  This issue occurs only when the HA assigns an IP address from the DHCP srever dynamically by acting as DHCP proxy client.

  Workaround: set the binding lifetime to a very large number (if possible).

- CSCsz38104

  The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

- CSCta02726—Incorrect TCP checksum in HTTP 302 Redirect Message

  HA is sending 302 Redirect Message with wrong TCP checksum after intercepting the HTTP GET Request packet.

  This condition occurs when the HA intercepts the HTTP GET Request packet.

  Workaround: none.

- CSCta73159—[XM3] Bulk Sync Failure on Home Agent.

  Bulk sync fails on the Home Agent.

  When you open a session with class attribute “R30-HA-ACCT” of 13 bytes length, the bulk-sync fails.

  - Setup a redundancy setup and create a binding.
  - Make sure bindings get synced to the standby HA.
  - Reload current active HA.
  - Once the card comes up, check for bindings on the current standby HA.
  - Notice that the bindings were not synched to the current standby HA.

  Workaround: if you do not use the class attribute “R30-HA-ACCT” with a length of 13 bytes, this issue does not occur.

- CSCta95521—[XM3] Memory Leaks @IPMOBILE DHCP CLIENT & @MobileIP AAA Response

  Seeing memory leaks on the HA while processing DHCP host configuration request extension over Wimax session.

  Workaround: none.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XM3

The following caveats are resolved in Cisco IOS Release 12.4(15)XM2:

- CSCsm27390—Writing to Slavebootflash: Takes a Long Time

  Writing to slavebootflash: takes a long time.

  This condition occurs when a “write memory” is executed .

  Workaround: none.

- CSCso77952—Failed to Parse AVP 31 During the ICCN Phase in SIP-VPDN Call

  On Cisco router running HA(c7svcsami-h1is-mz_080330) software, the HAfailed to parse AVP 31 during the ICCN phase in a SIP-VPDN call with avp-hidden attribute from AAA.: none

  Workaround: none.

- CSCsq46332—Traceback While a Binding When PMIP Configured on FASIM

  Binding do not come up with memory allocation failure and traceback.

  This occurs when the HA receives RRQ with NVSE and CVSE extensions of vendor-id type 9 (cisco) and proxy type.

  Workaround: RRQ should not contain NVSE and CVSE of vendor-id type 9.

- CSCsq65155—HA Rejects RRQ with an Extension 147

  Access-Request to AAA does not contain SPI attribute, therefore registration of MN fails.

  This condition occurs when the HA receives RRQ with 147 extension (PMIP skippable extension).

  Workaround: RRQ should be sent without 147 extension.

- CSCsq89116—HA Reloads While Displaying Security Associations and Deleting the Binding

  HA reloads while displaying security associations and deleting the binding.

  This condition occurs when displaying the SPI, delete the SPI from MN.

  Workaround: none.

- CSCsq99663—Not Able to Open Bindings When Length of NAI is 160 Bytes

  Binding fails to be created whe the NAI length is > 160 bytes.

  Workaround: none.

- CSCsr24323—SAMI : The Length of GMT-Time-Zone-Offset is Incorrect

  The length of GMT-Time-Zone-Offset(26/3) of WIMAX RADIUS VSAs that SAMI sends is 5 although the length is required by NWG-Stage3 to be 4.

  This condition occurs on the Cisco7609 and SAMI using the 12.4(15)XM1 image.

  Workaround: none.

- CSCsr62059—MN-HA-MIP-Key is Different in Active and Standby

  In HA redundancy environment, binding information is inherited to standby HA. Switchover fails due to different value of MN-HAMIP4-Key confirmed by "show ip mobile secure host" command as seen below.

  ```
  HA01(Active HA)  MN-HA-MIP-Key:0000000000000000000000000000000000000001
  HA02(Standby HA) MN-HA-MIP-Key:00000000000000000000000000000000
  ```

  This condition occurs in a redundant environment.

  Workaround: none.

- CSCsr76576—Unable to Create a Binding Due to HA-CHAP Failure

  No bindings are created while opening a basic mip flow.

  Workaround: none.

- CSCsr65146—“Overall service time” is Incremented Incorrectly Every MN Connection

  “Overall service time”, which is displayed by the **show ip mobile host** command is incremented incorrectly.18 hours are incremented at every connection of the mobile node. Even though they have tried to connect the MN to the HA 3 times within 3 minutes, the overall service time incremented 18h as below.

  First Connect:Overall service time 18:12:15

  Second Connect:Overall service time 1d12h

  Third Connect:Overall service time 2d06h

  This conditions occurs using HA redundancy with WiMAX attributes.

  Workaround: none.

- CSCsr67393—Re-registration Fails After Switchover

  Binding is deleted during Re-registration.

  This condition occurs in a redundant setup after binding gets established; there should be a switchover.

  Workaround: none.
- CSCsr79637—Unable to Close Binding

  Binding does not get closed.

  This problem occurs under all conditions.

  Workaround: none.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XM2

The following caveats are resolved in Cisco IOS Release 12.4(15)XM1:

- 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.
- 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.
- 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.

- 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 Idenitfy 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 initates 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 RSIM. 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 Rasim 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.
- CSCso81854

  Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

  To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml.

  This security advisory is being published simultaneously with announcements from other affected organizations.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XM1

There were no resolved caveats prior to Cisco IOS Release 12.4(15)XM1.

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 39
- Platform-Specific Documents, page 39

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