Release Notes for the Cisco Mobile Wireless Home Agent Feature in Cisco IOS Release 12.4(22)YD3

Published: May 20, 2010, OL-21462-02

Cisco IOS Release 12.4(22)YD3 is a special release that is based on Cisco IOS Release12.4, with the addition of enhancements to the Cisco Mobile Wireless Home Agent feature. The Cisco IOS Release 12.4(22)YD3 is a release optimized for the Cisco Mobile Wireless Home Agent feature on the Cisco Service Application Module for IP (SAMI) for the Cisco 7600 Series. The physical interfaces supported on the Cisco 7600 Series platforms are mainly Fast Ethernet and Gigabit Ethernet, FlexWAN (ATM, Frame Relay), and the new line of Shared Port Adaptor (SPA) and SPA Interface Processor (SIP) line cards, and are independent of physical media.

Contents

These release notes include important information and caveats for the Cisco Home Agent software feature provided in Cisco IOS 12.4(22)YD3 for the SAMI card on 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/ps6441/prod_release_notes_list.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 works in conjunction with a Foreign Agent and mobile node to provide an efficient Mobile IP solution.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(22)YD3:

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	Mobile Wireless Home Agent Software Feature Set	SUP32, SUP720 and RSP720 Home Agent Image 12.4(22)YD3	256MB	2GB 1GB DRAM	RAM

Hardware Supported

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

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

Before you install the Cisco Mobile Wireless Home Agent, keep the following considerations in mind:

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

A Cisco SAMI module is required to run Home Agent functionality.

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

Cisco Mobile Wireless Home Agent Release 12.4(22)YD3 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(22)YD3 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(22)YD3 supports the same features that are in Cisco IOS Release 12.4, with the addition of the Cisco Mobile Wireless Home Agent 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-H2IK9S-M), Version 12.4(22)YD3, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Fri 14-May-10 11:12 by prod_rel_team

ROM: System Bootstrap, Version 12.4(20080703:222712) [plin2-sami-bouncer 104], DEVELOPMENT
SOFTWARE

Router uptime is 1 hour, 14 minutes
System returned to ROM by reload at 12:58:25 UTC Tue May 18 2010
System restarted at 13:03:19 UTC Tue May 18 2010
System image file is "c7svcsami-h2ik9s-mz.124-22.YD3.bin"
Last reload reason: Reload command by admin
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco Systems, Inc. SAMI (MPC8500) processor (revision 2.2) with 1835008K/262144K 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 pre-loaded 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.

	Command	Purpose
Step 4	`Sup# show upgrade software progress`	Displays status of the upgrades that are occurring.
Step 5	`Sup# show module` *`slot_num`*	Ensures that the SAMI card comes up properly after the reset. The status of the SAMI should be "OK".

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

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

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

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

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

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-h2ik9s
Loading c7svcsami-h2ik9s 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#
```

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

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 Restart a PPC. 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-h2ik9s.sami
image:svcsami-h2ik9s.sami_060626
```

Step 3 Restart a PPC. Example (from LCP console):

```
testdc restart svcsami-h2ik9s.sami_060626 proc 1
```

Required Base Configuration

A typical Mobile Wireless Home Agent configuration requires that you define interfaces in three directions: PDSN/Foreign Agent, home network, and AAA server. If Mobile Wireless Home Agent redundancy is required, then you must configure another interface for HSRP binding updates between Home Agents. If you are running the Home Agent on the SAMI, the Home Agent 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 sub-interfaces provided for each necessary network access.

VLANs can be defined corresponding to each interface: PDSN/FA, home network, AAA. In the case of multiple Home Agent instances in the same 7600 chassis, the same VLAN can be used for all of them.

The following section illustrates the required base configuration for the Cisco Mobile Wireless Home Agent:

Basic IOS Configuration on Supervisor for SAMI Module

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

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

	Command	Purpose
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

Home Agent Release 5.0 introduces two new MIBs:

- CISCO-SLB-DFP-MIB
- CISCO-RADIUS-MIB

And the following MIBs are updated:

- CISCO-MOBILE-IP-MIB
- RADIUS-CLIENT-AUTHENTICATION-MIB

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 2.

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

Deprecated MIB	Replacement
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(22)YD3 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(22)YD3 includes the Cisco Mobile Wireless Home Agent feature. The Cisco Mobile Wireless Home Agent 5.0 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 Cisco IOS Release 12.4(22)YD3

The Cisco IOS Release 12.4(22)YD3 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(22)YD3 includes the Home Agent feature. The Cisco Mobile Wireless Home Agent feature is optimized for the Cisco SAMI blade on the 7600 Internet router.

The following features were introduced prior to Cisco IOS Release 12.4(22)YD3:

- Support for Alternative Mobile Node Identifier
- Exclude NAI in Revocation Messages
- Reject Framed-IP if Already in Use
- GRE Key CVSE in Non-VRF Environment
- Conserve Unique IP ID for FA-HA IP-in-IP Tunnel
- Setting Fragmentation Size of First Packet With Offset=0
- CoA for WiMAX Hotlining
- DNS Redirection with Monitoring
- NAI Authentication with Local Mobile Node-Home Agent SPI and Key
- IP Redirect for Non-Hotlined Users
- In/Out Access List Per NAI/Realm
- Home Agent - Realm Case-Insensitive Option

- Foreign Agent- Home Agent Auth Extension Mandatory
- Absolute Timeout Per NAI
- AAA Attributes for “ip mobile host/realm”
- VSE Support for China Telecom Attributes
- OM Metrics for 3GPP2 / WiMAX Bindings
- Single IDB for MIP/UDP Tunnels
- Redundancy Support for Hotlining
- No Authorization for Re-Reg / De-Reg
- Tunnel Stats via SNMP
- 3GPP2 RRQ Without MHAE
- Single IP Infrastructure
- Home Agent Session Redundancy Infrastructure
- Automatic Intra-Chassis Configuration Synchronization
- Bounded Limit For Maximum Bindings
- Congestion Control Feature
- Foreign Agent Classification
- MAC Address as Show/Clear Binding Key
- Data Path Idle Timer
- Support for RFC 4917
- Address Assignment Feature
- Accounting Interim Sync
- RADIUS Accounting Support in Single IP Home Agent infrastructure
- Global Per Domain Accounting
- Support for Acct-Terminate-Cause
- Authentication Configuration Extension
- Support for Service and Application Module for IP (SAMI)—Up to 9 SAMI cards can be supported in a single Cisco 7600 Series Router chassis.
- 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
- Priority-Metric for Local Pool
- Mobile IPv4 Host Configuration Extensions RFC4332
- Support for Mobile Equipment Identifier (MEID)
- Home Agent Accounting Enhancements
  - Home Agent Accounting in a Redundant Setup

  - Packet count and Byte count in Accounting Records
  - Additional Attributes in the Accounting Records
  - Additional Accounting Methods—Interim Accounting is Supported.
- VRF Mapping on the RADIUS Server
- Conditional Debugging Enhancement
- Home Agent Redundancy Enhancements
  - Redundancy with Radius Downloaded Pool Names
- CLI for IP-LOCAL-POOL-MIB
- Mobile-User ACLs in Packet Filtering
- IP Reachability
- DNS Server Address Assignment
- Mobile IP MIB Enhancements in Network Management, MIBs, and SNMP on the Home Agent
- Mobile IPv4 Registration Revocation
- Home Agent Server Load Balancing
- Home Agent Accounting
- Skip Home Agent-CHAP with Mobile Node-Foreign Agent Challenge Extension (MFCE)
- VRF Support on Home Agent
- Radius Disconnect
- Conditional Debugging
- Home Address Assignment
- Home Agent Redundancy
- Virtual Networks
- Mobile IP IPSec
- Support for ACLs on Tunnel Interface
- Support for AAA Attributes Mobile Node-Home Agent-SPI and Mobile Node-Home Agent SHARED KEY
- 3 DES Encryption
- User Profiles
- Mobility Binding Association
- User Authentication and Authorization
- Home Agent Binding Update
- Per User Packet Filtering
- Security

Feature Support

In addition to supporting Cisco IOS networking features, a Cisco 7600 series router configured as a Home Agent, supports the following Home Agent-specific features:

- Support for both intra-chassis and inter-chassis Home Agent redundancy
- Support for static IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Support for dynamic IP addresses assignment
  - Public IP addresses
  - Private IP addresses
- Multiple flows for different Network Access Identifiers (NAIs) using static or dynamic addresses
- Multiple flows for the same NAI using different static addresses
- Foreign Agent Challenge extensions in RFC 3012 - bis 03
  - Mobile IP Agent Advertisement Challenge Extension
  - Mobile Node-Foreign Agent Challenge Extension
  - Generalized Mobile IP Authentication Extension, which specifies the format for the Mobile Node-AAA Authentication Extension
- Mobile IP Extensions specified in RFC 2002
  - Mobile Node-Home Agent Authentication Extension
  - Foreign Agent-Home Agent Authentication Extension
- Reverse Tunneling, RFC 2344
- Mobile NAI Extension, RFC 2794
- Multiple tunneling modes between Foreign Agent and Home Agent
  - IP-in-IP Encapsulation, RFC 2003
  - Generic Route Encapsulation, RFC 2784
  - MIP-UDP tunneling
- Binding Update message for managing stale bindings
- Home Agent redundancy support
- Mobile IP Extensions specified in RFC 3220
  - Authentication requiring the use of SPI. section 3.2
- Support for Packet Filtering
  - Input access lists
  - Output access lists
- Support for proxy and gratuitous ARP
- Mobile IP registration replay protection using time stamps. Nonce-based replay protection is not supported.

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(22)YD3:

- CSCtg65827—Handoff support between 3G and 4G networks when an access tech-type extension is received in Registration Request (RRQ).

  This issue is observed with Home Agent running 12.4(22)YD2 when the client roams between WiMAX (4G) and CDMA (3G) networks with tech type extension enabled.

  Ideally, the initial RRQ from ASN-GW must contain the PMIP tech type extension. After the handover to CDMA, the RRQ from the client mobile IP should not contain tech type extension. Similarly, the initial RRQ from CDMA should not contain tech type extension and after the handover to ASN-GW, the RRQ from the Proxy mobile IP must contain the tech type extension.

  Workaround: The initial RRQ from ASN-GW must not contain the PMIP tech type extension. After the handover to CDMA, the RRQ from the client mobile IP must not contain any tech-type extension.

- CSCtc89986—DHCP RELEASE message is sent from an active Home Agent during forced reload.

  This issue is observed with a Home Agent running 12.4(22)YD in a redundant setup.

  When the active Home Agent is forcefully reloaded using the **reload** command, the active Home Agent sends “DHCP RELEASE” messages to the DHCP server for all leased IP address. This leads to the resources on the DHCP Server being cleared.

  Ideally “DHCP RELEASE” should not be sent for proxy clients in a redundant setup because the sessions will get synchronized to the standby Home Agent.

  Workaround: There is no workaround.

Unresolved Caveats Prior to Cisco IOS Release 12.4(22)YD3

The following caveats are unresolved in Cisco IOS Release 12.4(22)YD1:

- CSCtb39102—Session Not Synced to Standby When MTU Size is 1600

  The session does not get synched to the standby unit from the active unit if MTU is configured as 1600 bytes in the Gigabit0/0 interface of the SAMI. The router could possibly RF induced self-reload.

  This problem could happen on a redundant system with MTU size configured as 1600 bytes.

  Workaround: Configure the default MTU size of 1500 bytes.

- CSCtb41029—DHCP Redundancy Issues in Home Agent 5.0 and Home Agent 5.1

  The improper behavior of DHCP redundancy contexts between active and standby Home Agent with or without switchover are observed when the Home Agent is acting as a DHCP Proxy Client. And, the issue is seen on Home Agent 5.0 and Home Agent 5.1.

  This condition occurs when the Home Agent is acting as DHCP Proxy Client to lease the IP addresses from the DHCP Server for MIP sessions by configuring **ip mobile host nai** *word* **address pool dhcp-proxy-client dhcp-server** *dhcp-server-ip* **interface Loopback60 aaa**.

  Workaround: There is not workaround.

- CSCtb46311—Conditional Debugging For Radius Debugs Not Working

  RADIUS logs are not displayed.

  This condition occurs when RADIUS debugs are enabled along with conditional debugging.

  Workaround: There is not workaround.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(22)YD3:

- CSCtf24293—Per binding policing did not work if the policy map was created with pdp burst and pdp peak-burst, and applied to a realm.
- CSCte97458—Lease time did not get renewed after the standby became active.

  This occurred when a smaller value was configured for the lease time, for example, 5 minutes, after which a switchover from active to standby occurred.
- CSCtg49772—While performing a forced reload on an active Home Agent, the Home Agent that was initially active did not send a DHCP release message. However, the newly active Home Agent sends the DHCP release message to the DHCP server after completing the renewal request for rebinding.
- CSCte16762—Home Agent crashed after reconnecting PMIP sessions after clearing the old bindings. This affected the coexistence of PMIP and CMIP on Home Agent.
- CSCtd42574—HoA was not assigned by the Framed IP Attribute provided by Access-Accept packet from AAA for PMIP calls.
- CSCte80849—On Home Agent running 12.4(22)YD1 software, spurious memory access was recorded while using MIP-UDP tunnels.
- CSCsv43658—The Gateway GPRS Support Node (GGSN) crashed when a service policy that was already being used by the PDPs of an APN was applied to another APN. This issue occurred when the same service policy was applied to multiple APNs.

- CSCso89298—Policing on PDP stopped after the service policy attached to an APN was reconfigured.
- CSCtc35449—Suppression of syslog messages, which are generated on identifying the security violation, cannot be disabled.

  A new command is introduced in Home Agent 5.3 to configure the security violation-interval.
- CSCtd49501—`3gpp2` was spelled wrongly in the **show mobile ip binding summary** command output. The spelling is corrected.
- CSCte13718—When Home Agent was used as the DHCP server for allocating IP addresses, multiple bindings were created for a single session. This left a stale session on the Home Agent after the mobile node was deregistered.
- CSCsy48122—While creating PDP, spurious memory access error messages and tracebacks related to the UMTS service policy were generated.

  This issue occurred when PDPs with police and CAC policy were created and deleted, after which the police policy was unconfigured. Traceback was seen when PDP was re-created.

Caveats Resolved Prior to Cisco IOS Release 12.4(22)YD3

The following caveats were resolved in Cisco IOS Release 12.4(22)YD2:

- CSCtb25158—Bulk Sync Not Happening For All DHCP-Returned Attributes
  - Configure DHCP pool with DNS Server Address, Default-Gateway etc. options.
  - Send Host-Config request from FASIM.
  - Check in the debugs that all DHCP returned attributes are not syncing to standby card (DNS Server Address, Default-Gateway)

  Because of this, after switchover, the new active card sends the Default-Gateway incorrectly on reregistration. As a result, a few attributes are not synching to the standby card.
- CSCtb39102—Session Not Synced to the Standby When MTU Size is 1600

  The session does not get synched to the standby unit from the active unit if MTU is configured as 1600 bytes in the Gigabit0/0 interface of the SAMI.

  This problem could happen on a redundant system with MTU size configured as 1600 bytes.

  Workaround: configure the default MTU size of 1500 byes.
- CSCtb41029—DHCP Redundancy issues in Home Agent 5.0 and Home Agent 5.1

  Improper behavior of DHCP redundancy contexts between active and standby Home Agent with or without switchover was observed when the Home Agent acted as a DHCP Proxy Client.

  This condition occurs when the Home Agent acted as a DHCP proxy client to lease the IP addresses from the DHCP Server for MIP sessions by configuring **ip mobile host nai** *word* **address pool dhcp-proxy-client dhcp-server** *dhcp-server-ip* **interface Loopback60 aaa**.
- CSCtb46311—Conditional Debugging For Radius Debugs Not Working

  RADIUS logs are not displayed.

  This condition occurs when RADIUS debugs are enabled along with conditional debugging.

- CSCtb48982—Acct-Interim-Interv: Local Value Gets Overwritten by Access-Accept Value

  The Home Agent overrides the locally configured periodic value for sending Accounting Interim to the value received in the Access-Accept message.

  This condition occurred when the Home Agent receives a Acct-Interim-Interval attribute in Access-Accept message from the Radius Server, and also has **aaa accounting update periodic** *x* configured locally.

- CSCtb64346—The IP Redirect Feature With Non-Hotline Profile Does Not Work When Destination is Not on the Routing Table

  The IP Redirect feature with the non-hotline profile does not work when the route information for the redirected destination is not on the routing table.

  This condition occurs when

  - Non-Hotline profile is configured with IP redirect.
  - There is no route information for the redirected destination.
  - Next-hop any-traffic is configured (because the destination is not on the routing table).

  Workaround: Add a route information for the destination to the routing table.

- CSCtb83004—Input Queue Drops Increment Every 7-10 Seconds on G0/0 With Minimal Traffic

  The **show interface GigabitEthernet 0/0** input queue drops increments with minimal traffic.

  This happens when unknown L2 packets reach the Home Agent. This does not impact any data traffic from the mobile nodes.

The following caveats were resolved in Cisco IOS Release 12.4(22)YD1:

- CSCsw47076

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsv48603

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsx07114

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- 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.

- 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

- CSCsy26261—Key Value Displayed Wrongly in Standby Home Agent
  - Configure load-sa for a realm.
  - Use hmac-md5 algorithm with ascii key value for Mobile Node-Home Agent authentication
  - Use AAA to send Mobile Node-Home Agent authenticator
  - Display the cached spi/key value in standby.
  - It will show the ascii value in hex.

  This is just a display problem and does not affect functionality

  Workaround: none.

- CSCsy54122

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- 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.

- CSCsz91894—Session Timeout Should Be Able to Display More Than 2^32 Value

  Currently there is no direct API to display such a large value [136 year] for the timers that get started based on AAA downloaded session timeout.

  To reproduce this condition, configure “session timeout 4294967295” or “attribute 27 numeric 4294967295”.

  Any timer starts for this value, is not able to display it.

- CSCta00770— Previous DNS Servers Info Persists in Bindings for Full NAI

  Mobile IP bindings incorrectly retain the previous configured DNS value.

  This is seen only for full an NAI Mobile Node user.

- CSCta00810—After local SA Removed for Full-NAI, locals for Realm Not Being Used

  The locally configured Mobile Node-Home Agent security association (SA) is not used in some scenarios.

  The following conditions exist:

  - Configure Mobile Node-Home Agent security association (SA) for both full NAI and the corresponding realm.
  - Now, unconfigure SA for full-NAI.
  - When the same full-NAI user tries registering, the local SA configured for the corresponding realm is not used. Because of this the authentication may fail.

  Workaround: If a separate SA for full-NAI is not needed, do not configure. Configure SA for realm only.

- CSCta41989—**clear ip mob sec empty load** is Causing Tracebacks

  Spurious memory access tracebacks are seen in Home Agent.

  This is seen while issuing the **clear ip mob sec empty load** command.

- CSCta55764—IPC Config Synch Error

  The following error appears on the Home Agent when **ip mobile home-agent data-path-idle 2** is configured.

Error Message `%IPC-4-CFG_SYNC_ERROR: Configuration Sync error: IPC Communication failure in sending cmd to TP`

  This condition occurs when there is a large number of mobile IP session active (500k), all this sessions get updated with data path idle time.

  Workaround: configure **ip mobile home-agent data-path-idle** when there is no active sessions or a few number of sessions.

- CSCta58990—Home Agent Reloads When Secure Host is Configured With Full NAI for Overlap IP VRF

  The Home Agent reloads when same overlapping IP address is used across two bindings under two different vrfs.

  The following conditions exist:

  a. **ip mobile secure host** has to be configured for full NAI Mobile Node.
  b. Static HoA assignment (RRQ HoA is non-zero).
  c. Open/Close and Open should happen.

- CSCta62685—VRF is Not Applied For Mobile Node When Configured Before VRF Configuration

  The VRF is not applied for the Mobile Node when configured before the VRF configuration.Conditions:</B>

  The following conditions exist:

  - Configure **ip mobile host** CLI for domain
  - Configure **ip mobile secure host nai** for full NAI Mobile Node.
  - Configure VRF for the domain

  Workaround: after configuring VRF, unconfigure **secure host** and configure again.

- CSCta65964—Dynamic User Not Cleared in **show ip mobile host** Output

  SA and Dynamic users details of the opened binding are still present even though the binding is cleared.

  This conditions occurs when you enable the revocation and clear the binding on Home Agent using the **clear ip mobile binding all** command.

  Workaround: Delete the new recovery compared mn node after deleted registration revocation entry ASK for Mobile Node.

- CSCta74909—Home Agent Crashed While Displaying lot of Bindings

  Home Agent crashed while displaying lot of bindings.

  The condition occurs when a binding gets deleted, while executing **show ip mobile binding**.

  While displaying binding information, if the Mobile Node structure gets freed due to deletion of the binding, it results into crash.

  Workaround: Terminal length should not be set to 1 or 0.

- CSCta75127— Memory Leak Found on TPs After Sending For Long Times With Acls

  When packets from downstream are dropped by per user/realm ACL, memory leak of 180K (for 2.2Gbps for 2 hours) is observed.

  This condition occurs when you configure a per user/realm ACL which denies the packet in the downstream and send downstream packets.

- CSCta98702—“attribute 44 include-in-access-req” Configured But Not Going in Access-Req

  The Accounting Session-ID is not included in Access-Request.

  This issue occurs under the following conditions:

  - “radius-server attribute 44 include-in-access-req" is configured on the Home Agent.
  - Accounting is enabled on the Home Agent.

- CSCsy60479—Configuration Sync Error for Tunnel Template

  A configuration sync error was observed during MIP session creation or deletion using the Tunnel Template feature.

  This condition occurs when a Tunnel Template is applied to an Home Agent IP address.

- CSCsy78653—Unable to Configure **ip mob sec host** After Modifying Named ACLs

  This problem occurs when operator configures or modifies or updates a named extended ACL, and then tries to configure a security association for Mobile Node-Home Agent authentication for a realm/NAI.

  In this scenario, local configuration of the security association is not possible due to a bug in the ACL component (refer to CSCsy69542)

  This DDTS fixes the problem in the IP-mobile component, and acts as a temporary solution until the actual problem is fixed by the ACL team.

  Workaround: Modify or update the local security association for Mobile Node-Home Agent authentication before modifying a named extended ACL.

- CSCsy89105—When ACL Denies a Packet From the Mobile Node, Packet Counter Decrements in Some Cases

  A data packet from the Mobile Node is received by the Home Agent through IP/IP, GRE/IP or MIP/UDP binding. If the ACL is configured for this particular user, and the packet gets denied, the ACL counters get incremented twice.

  This happens only when the packet gets denied with ACLs.

- CSCsy98146—Traceback Seen on Home Agent During Bulk Synchronization.

  A traceback appears on the standby Home Agent during bulk synchronization of Mobile IP sessions.

  This condition occurs in a redundancy setup with the Home Agent 5.0 release. When the standby comes up and a bulk synchronization occurs, a traceback appears on the router console.

- CSCsz23375—Bindings Not Getting Synced to Standby With NAI Configured for DHCP

  Binding does not sync from the active device to the standby device

  This condition occurs when the NAI is configured with DHCP proxy option, then only, the binding (which brought up with that NAI) does not sync from the active to the standby.

- CSCsz30815—Tracebacks in Home Agent with High HA-RK Lifetime

  Tracebacks are observed on the Home Agent while starting Home Agent-RK lifetime timer.

  This condition occurs when you download an HA-RK lifetime value is greater than 2147483 seconds.

  Workaround: Use an HA-RK lifetime value of less than 2147483 seconds.

The following caveats were resolved in Cisco Home Agent Release 12.4(22)YD:

- CSCsu11522

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

  Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

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 23
- Platform-Specific Documents, page 23

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4(22)YD3:

- *Cisco Mobile Wireless Home Agent Feature for Cisco IOS Release 12.4(22)YD3* at the following url:

  http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22yd3/feature_guide/ha_5_3_fg.html
- *Cisco Mobile Wireless Home Agent Command Reference for Cisco IOS Release 12.4(22)YD3* at the following url:

  http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22yd3/command_ref/ha53_cr.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