



Release Notes for the Cisco Home Agent 2.1 Feature in Cisco IOS Release 12.3(11)YF

December 2004

Cisco IOS Release 12.3(11)YF is a special release that is based on Cisco IOS Release 12.3, with the addition of enhancements to the Cisco Mobile Wireless Home Agent feature. Cisco IOS Release 12.3(11)YF is optimized for the Cisco Mobile Wireless Home Agent Release 2.1 feature on the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco Multi-Processor WAN Application Module on the Cisco 6500 Catalyst switch platform, and the 7600 Internet router platform.

Contents

These release notes include important information and caveats for the Cisco Mobile Wireless Home Agent software feature provided in Cisco IOS 12.3(11)YF for the Cisco 7206 Series Internet Router, Cisco 7301 Series Internet Router, and the MWAM card on the 6500 Catalyst Switch and Cisco 7600 Series Router platforms.

Caveats for Cisco IOS Releases 12.3 can be found on CCO at:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/index.htm>

Release notes for Cisco 7000 Family for Release 12.3T can be found on CCO at:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/7000/index.htm>

Release notes for the Cisco 6000 and 7600 Family for 12.3T can be found on CCO at:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm>

This release note includes the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Cisco Mobile Wireless Software Features in Release 12.3\(11\)YF, page 5](#)
- [Related Documentation, page 40](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation, page 42](#)
- [Obtaining Technical Assistance, page 43](#)

Introduction

The Cisco Mobile Wireless Home Agent (HA) maintains mobile user registrations and tunnels packets destined for the mobile to the PDSN/FA. It supports reverse tunneling, and can securely tunnel packets to the PDSN using IPSec. Broadcast packets are not tunneled. Additionally, the HA performs both static and dynamic home address assignment for the mobile. Home address assignment can be from address pools configured locally, through either DHCP, ODSF, or AAA server access.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(11)YF:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Software Compatibility, page 3](#)
- [Determining the Software Version, page 4](#)
- [Upgrading to a New Software Release, page 4](#)
- [MIBs, page 4](#)

Memory Requirements

[Table 1](#) shows the memory requirements for the Cisco Mobile Wireless Home Agent Software Feature Set that supports the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco Multi-Processor WAN Application Module on the Cisco 6500 Catalyst switch platform, and the 7600 Internet router platform. The table also lists the memory requirements for the IP Standard Feature Set (for the Cisco Mobile Wireless Home Agent [HA]).

Table 1 Memory Requirements for the Cisco 7206 Router, 7301 Router, and the MWAM on the 6500 Catalyst Switch and 7600 Router

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7206VXR Router NPE-400	Home Agent Software Feature Set	c7200-h1is-mz.123-11.YF c7200-h1ik9s-mz.123-11.YF	20MB	512MB	RAM
Cisco 7206VXR NPE-G1	Home Agent Software Feature Set	c7200-h1is-mz.123-11.YF c7200-h1ik9s-mz.123-11.YF	20MB	1 Gigabyte	RAM
Cisco 6500 Catalyst Switch	Home Agent Software Feature Set	svcmwam-h1is-mz.123-11.YF c6svc-5mwam-h1is-b21_11.123-11.YF.bin (This is a bundled image)	40MB	512MB	RAM
Cisco 7600 Internet Router	Home Agent Software Feature	svcmwam-h1is-mz.123-11.YF c6svc-5mwam-h1is-b21_11.123-11.YF.bin (This is a bundled image)	40MB	512MB	RAM

Hardware Supported

The Cisco IOS Release 12.3(11)YF is a release optimized for the Cisco Home Agent Release 2.1 feature on the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco Multi-Processor WAN Application Module on the Cisco 6500 Catalyst switch platform, and the 7600 Internet router platform.

For recommended hardware configuration, and for a complete list of supported interfaces on the 7200 platform, refer to the 12.3(11)YF Product Bulletin. If you require a different configuration you should consult with your Cisco representative before you order.

The recommended hardware configuration for Home Agent Release 2.1 is based on a Catalyst 6500 or 7600 chassis with a SUP2/MSFC2, and 512 MB of DRAM.

A Cisco IPSec Services Module (VPNSM) is required for hardware support of IPSec. VAMII is used for 7200 and the Cisco IPSec VPN Services Module is used for 6500/7600.

For a complete list of interfaces supported on 6500 and 7600 platforms, please refer to the on-line product information at Cisco.com home page. For hardware details on the 6500 and 7600 platforms, please refer to the Catalyst 6500 product specifications at <http://www.cisco.com/en/US/products/hw/switches/ps708/index.html>.

Software Compatibility

Cisco IOS Release 12.3(11)YF is a special release that is developed on Cisco IOS Release 12.3.

Cisco IOS Release 12.3(11)YF supports the same features that are in Cisco IOS Release 12.3, with the addition of the Cisco Home Agent Release 2.1 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 Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-H1IS-M), Version 12.3(8)XW3, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1) Synched to technology version 12.3(8)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

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 2](#).

Table 2 *Deprecated and Replacement MIBs*

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

Cisco IOS Feature Sets

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

Cisco IOS Release 12.3(11)YF supports the same feature sets as Cisco Release 12.2, with the exceptions that Cisco Release 12.3(11)YF includes the Cisco Home Agent Release 2.1 feature. The Home Agent Release 2.0 feature is optimized for the Cisco 7206 router, the Cisco 6500 Catalyst Switch, and 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 Software Features in Release 12.3(11)YF

- Mobile IPv4 Registration Revocation
- HA Server Load Balancing
- HA Accounting
- Skip HA-CHAP with MN-FA Challenge Extension (MFCE)
- VRF Support on HA
- Hot-lining
- Radius Disconnect
- Conditional Debugging
- Dynamic Home Agent Assignment
- Home Agent Redundancy
- Virtual Networks
- Home Address Assignment
- 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
- Packet Filtering
- Security

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 12.2 can be found on CCO at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cavs/122mcavs.htm>

The “[Open Caveats](#)” section on page 6 lists open caveats that apply to the current release and might also apply to previous releases.

The “[Resolved Caveats](#)” section on page 30 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 Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II**, or at <http://www.cisco.com/support/bugtools>.

Open Caveats

The following caveats are unresolved in Cisco IOS Release 12.3(11)YF

- CSCed50040—Memory Leak While Opening 8000 MOIP Tunnels
On a Cisco 7200/7600 router running Home Agent R2.0 Software, a memory leak is observed on both active and standby HA while opening 8000 MOIP tunnels.
Workaround: none.
- CSCee19678—Tracebacks on MWAM HA When Interface is Shut While Running Load Test
On a Cisco MWAM based module acting as Home agent and handling calls and traffic to simulate background load conditions, when a processor acting as active is forcibly made standby by shutting down the interface NULLIDB tracebacks appear of the processor on which the transition is made.
This condition occurs when the interface is shut, or the PI link flaps.
Workaround: none. There is no functional breakdown of Home Agent. This traceback does not have any effect on Home Agent functionality.

- CSCee26364—MN SA Deleted on **clear ip mobile binding** CLI on HA
Security-Association for the NAI is deleted when one of the flows are closed on the HA.
This symptom has been observed on a router that is running Cisco IOS release 12.3T under the following conditions:
 - Configure the **load-sa** config on the HA and open multiple flows for same NAI.
 - Close one of the flows and subsequently, the Security Association for the NAI is deleted, even though the other MIP flow is active.
 - If any other new flow is opened, a new security association is again invoked from AAA.
 *The above symptom is seen for NAI-based users when multiple MIP flows are opened with same NAI but different home-addresses.
Workaround: none.
- CSCee34368—Standby HA Reloads in this Scenario
A Cisco router running Home Agent R2.0 software and configured as Standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA.
This condition exists when the bindings on the standby HA are cleared after reloading the active HA.
This problem is very rare and was seen only once during testing.
Workaround: none.
- CSCee37327—HA Reloaded Upon Clearing Bindings in this Scenario
On a Cisco 7200/7600 router running Home Agent R2.0 software, alignment and spurious memory errors occur and HA may reload when bindings are cleared after a stress test.
The errors are seen only when NAI related CLI (**ip mobile host nai**) is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the radius server.
Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.
- CSCee52886—Proxy DHCP: Active HA Releases the DHCP Address on Standby Interface
The active HA releases the DHCP address for the binding when the HSRP interface of the standby HA goes down, when proxy DHCP allocation is configured.
This condition is observed when the standby HA's HSRP interface is shut down while the active and standby has active Mobileip bindings with dynamic allocation using proxy DHCP.
Workaround: none.
- CSCee56692—Spurious Memory Access Observed While Opening Bindings With DHCP
On a Cisco 7200/7600 router running Home Agent R2.0 Software, spurious memory access is observed on the standby HA while opening and closing of bindings using DHCP.
This condition exists when opening and closing Mobile IP bindings using DHCP, and the HA is configured with redundancy.
Workaround: none.

- CSCef57953—Security Violation Counters Are Not Incrementing in HA

Security violation counters are not incrementing in a Cisco router running 12.3T R2.0 Release HA software.

This condition occurs when MNHA authentication failed for an invalid SPI value .

Workaround: none.
- CSCef86760—Standby HA Reloads on Bindupdate from Active HA When Pre-emption is Configured

The standby Home Agent reloads on receiving a bind update from the active when pre-emption is configured

The reload is observed only after repeating the switchover more than once .

Workaround: none.
- CSCef95682—PMIP Flow Does Not Open With HA-SLB (Directed Mode)

On Cisco router running Release 2.0 PDSN software, when Proxy MIP flow is opened in a setup with HA-SLB(Directed Mode), the flow does not come up as the destination address set in the RRP seems to be incorrect.

This symptom occurs when Proxy MIP flow is opened with HA-SLB operating on Directed Mode. This issue is not seen when HA SLB used in Dispatched mode for PMIP flow.

Workaround: none.
- CSCeg00126—Security Violation on HA Without User Config Not Properly Recorded

Error condition for Registration request in the debug message is not reflecting the actual failure scenario.

Workaround: none.
- CSCeg03745—Spurious Memory Access When Downloading SAa With Command **aaa-download**

Spurious memory access is observed on the Home Agent when Security associations are cleared and downloaded using the **ip mob sec aaa-download rate 10** command.

The traceback is seen only when using the **aaa-download rate** command.

Workaround: none.
- CSCeg16482—Standby HA Does Not Get All SAs When the Interface in Shut/No Shut

The SA is not getting downloaded in standby HA.

This problem occurs under the following conditions:

 - when the HSRP interface on standby is shut
 - clearing the binding in standby HA
 - making the HSRP interface in standby up.

Workaround: do not shut the HSRP interface in the standby HA.
- CSCeg22858—HA:Rejects MN Binding When MN is Unconfigured and Configured Again

When the MN NAI is unconfigured and configured again, the HA rejects the binding for that NAI. This only occurs when the NAI is unconfigured and configured, and tries to register with HA. This happens in local pool, static and DHCP address allocation schemes.

Workaround: do not unconfigure the NAI in HA for which the registration has to be made.

- CSCin79571—HA Cannot Install SA for RRQ With Unknown Extension

The HA drops RRQ under following conditions:

- RRQ has an unknown extension.
- HA downloads MHAE Shared Key for the user from radius server in 3gpp2-mn-ha-shared-key format.

Workaround: ensure that the MN and FA do not send an unknown extension in RRQ.

- CSCin79585—**show run** Displays Invalid Commands

When **ip mobile home-agent nat traversal keepalive 10** is configured, the following configurations appear:

```
ip mobile home-agent revocation traversal keepalive 10
ip mobile home-agent nat traversal keepalive 10
```

This has no effect on revocation or NAT traversal feature behavior, but, when the HA is reloaded, revocation may get disabled.

Workaround: remove **ip mobile home-agent revocation traversal keepalive 10** from the startup configuration, or reconfigure revocation manually on reload.

- CSCin84300—HA Sends Weight Updates Only When **home-agent dynamic-address** is Configured

Cisco router running release 2.0 HA software and configured with DFP does not send weight updates when the **ip mobile home-agent dynamic-address ip-addr** command is not configured.

Workaround: configure the **ip mobile home-agent dynamic-address ip-addr** command.

- CSCin84856—Binding Does Not Sync to SBY on Changing Config From Group to User

Binding does not sync to the standby HA when the configuration is changed from group to a single user.

This condition occurs when the **ip mobile host nai** command is initially configured for a group of users, and then unconfigured and changed to a single user.

Workaround: do not change the configuration from group to per-user.

- CSCsa44092—ODAP Standby Client Become Active When Active Client is in Active state

The standby ODAP client changes its state to active without any changes in the configuration either in active or standby ODAP clients.

The active client is in the active state when the stanby client changes its state.

This condition is very rare. After a few open/close and reopening of bindings for MIP flow, this behaviour was observed.

Workaround: none.

- CSCsa44815—Stanbdy HA Reloaded on Getting Info From DHCP Server After Shut/No Shut

The standby HA reloaded when the DHCP server interface connected to the standby HA (DHCP client) is shut and no shut.

This condition only occurs when the DHCP server interface is shut/no shut.

Workaround: do not shutdown the DHCP server interface.

- CSCsa44954—MWAM Reloaded After Configuring DHCP Pool in ODAP Client
On a Cisco router running release 2.1 PDSN software and acting as an ODAP client, when the DHCP pool is configured and a subnet is being leased from the ODAP server, the client reloads.
This condition occurs when the DHCP pool is configured and is expecting a subnet from the ODAP server.
Workaround: none.
- CSCsa44959—Both Active and Standby HA Got Reloaded Simultaneously With DHCP
On Cisco router running Release 2.1 HA software, both the active and standby HA got reloaded simultaneously when the **clear ip dhcp subnet** command was issued on the active HA immediately after closing the PMIP flows. This reload is not reproducible.
This behaviour is seen only if the HA is configured for ODAP client redundancy. Under normal conditions, no issues seen.
Workaround: none.
- CSCsa44961—Standby HA with DHCP Configs Reloaded During HSRP State-change.
On Cisco router running Release 2.1 HA software, the standby HA got reloaded when the HA is configured for DHCP. This reload is not reproducible.
This behaviour is seen only if the HA is configured for ODAP Client redundancy. Under normal scenarios, no issues were seen.
Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.3(11)YF

The following Cisco Mobile Wireless Home Agent Release 2.0 caveats are unresolved in Cisco IOS Release 12.3(8)XW3:

- CSCed50040—Memory Leak While Opening 8000 MOIP Tunnels
On a Cisco 7200/7600 router running Home Agent R2.0 Software, a memory leak is observed on both active and standby HA, while opening 8000 MOIP tunnels.
Workaround: none.
- CSCee19678—Tracebacks on MWAM HA When Interface is Shut While Running Load Test
On a Cisco MWAM based module acting as Home agent and handling calls and traffic to simulate background load conditions, when a processor acting as active is forcibly made standby by shutting down the interface NULLIDB, tracebacks appear of the processor on which the transition is made.
This condition exists when the interface is shut or the PI link flaps.
Workaround: No known workaround exists. Any conditions that trigger the switchover will expose the tracebacks.

- CSCee26364—MN SA Deleted on **clear ip mobile binding** CLI on HA

The Security-Association for the NAI is deleted when one of the flows are closed on HA. This symptom has been observed on a router that is running Cisco IOS release 12.3T.

The following conditions exist:

- Configure the “load-sa” config on HA and open multiple flows for same NAI.
- Close one of the flows and subsequently, the Security Association for the NAI is deleted, even though the other MIP flow is active.
- If any other new flow is opened, new security association is again invoked from AAA.

Workaround: none.

- CSCee34368—Standby HA Crashed in this Scenario

A Cisco router running Home Agent R2.0 software and configured as Standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA.

This condition exists when the bindings on the standby HA are cleared after reloading the active HA.

This problem is very rare and was seen only once during testing.

Workaround: none.

- CSCee37327—HA Reloaded Upon Clearing Bindings in this Scenario

On a Cisco 7200/7600 router running Home Agent R2.0 software, alignment and spurious memory errors occur and HA may reload when bindings are cleared after a stress test.

The errors are seen only when NAI related CLI (**ip mobile host nai**) is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the radius server.

Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.

- CSCee52886—Proxy DHCP: Active HA Releases the DHCP Address on Standby Interface

The active HA releases the DHCP address for the binding when the HSRP interface of the standby HA goes down, when proxy DHCP allocation is configured.

This condition is observed when the standby HA’s HSRP interface is shut down while the active and standby has active Mobileip bindings with dynamic allocation using proxy DHCP.

Workaround: none.

- CSCee56692—Spurious Memory Access Observed While Opening Bindings With DHCP

On a Cisco 7200/7600 router running Home Agent R2.0 Software, spurious memory access is observed on the standby HA while opening and closing of bindings using DHCP.

This condition exists when opening and closing Mobile IP bindings using DHCP, and the HA is configured with redundancy.

Workaround: none.

- CSCee60087—Tracebacks Observed While Opening Bindings With DHCP

On a Cisco 7200/7600 router running Home agent R2.0 Software tracebacks observed while opening bindings with DHCP.

This condition exists when opening and closing 30000 MOIP bindings with 30 calls/sec using DHCP, then opening 30000 MOIP bindings with DHCP and accounting configuration. Tracebacks are observed on the active HA after opening of bindings.

Workaround: none.

- CSCee60490—Standby HA Crashed After Unconfig And Config Of IP Mobile Host

On a Cisco 7200/7600 router running Home agent R2.0 software, the standby HA crashed after unconfiguring and configuring ip mobile host.

Workaround: none.
- CSCef86760—Standby HA Reloads on Bindupdate from Active HA When Pre-emption is Configured

The standby Home Agent reloads on receiving a bind update from the active when pre-emption is configured

The reload is observed only after repeating the switchover more than once .

Workaround: none.
- CSCin70125—PDSN/HA Should Use Registration Revocation in MIPv4 Based on STC

On a Cisco PDSN/Home agent running R2.0 image, PDSN/HA doesnt use the STC attribute value received in the Access-Accept message from AAA to enable/disable registration revocation capability for the user. The revocation capability can be enabled/disabled for all sessions on the box using CLI.

Workaround: none.
- CSCin79571—HA Cannot Install SA for RRQ With Unknown Extension

The HA drops RRQ under following conditions:

 - RRQ has an unknown extension.
 - HA downloads MHAЕ Shared Key for the user from radius server in 3gpp2-mn-ha-shared-key format.

Workaround: ensure that the MN and FA do not send an unknown extension in RRQ.
- CSCin79585—**show run** Displays Invalid Commands

When **ip mobile home-agent nat traversal keepalive 10** is configured, the following configurations appear:

```
ip mobile home-agent revocation traversal keepalive 10
ip mobile home-agent nat traversal keepalive 10
```

This has no effect on revocation or NAT traversal feature behavior, but, when the HA is reloaded, revocation may get disabled.

Workaround: remove **ip mobile home-agent revocation traversal keepalive 10** from the startup configuration, or reconfigure revocation manually on reload.

Unresolved Caveats Prior to IOS 12.3(8)XW3

The following caveats are unresolved in Cisco IOS Release 12.3(8)XW2:

- CSCed50040—Memory Leak While Opening 8000 MOIP Tunnels

On a Cisco 7200/7600 router running Home Agent R2.0 Software, a memory leak is observed on both active and standby HA, while opening 8000 MOIP tunnels.

Workaround: none.

- CSCee16329—Tracebacks in HA on Performing Overnight Tests With SW Upgrade

On a Cisco MWAM module acting as Home Agent, when software upgrade is performed while background load is handled by MWAM module in a redundant setup tracebacks appear.

The tracebacks seem to interrupt the call processing and data processing capabilities of the MWAM on which the tracebacks appear.

Workaround: no known workaround exists. Attempts could be made to handle only small set of calls of about 20k calls in order to ensure all bindings as successfully transferred to standby HA (which has gone through s/w upgrade)
- CSCee18252—Active and Standby HA Crashed While Flapping MOIP Bindings

On a Cisco 7200/7600 router running Home Agent R2.0 Software, during flapping of MOIP bindings, both active and standby HA are crashed.

This condition occurs when flapping of MOIP bindings at 100 bindings/sec for about 4 hours.

Workaround: none.
- CSCee19678—Tracebacks on MWAM HA When Interface is Shut While Running Load Test

On a Cisco MWAM based module acting as Home agent and handling calls and traffic to simulate background load conditions, when a processor acting as active is forcibly made standby by shutting down the interface NULLIDB, tracebacks appear of the processor on which the transition is made.

This condition exists when the interface is shut or the PI link flaps.

Workaround: No known workaround exists. Any conditions that trigger the switchover will expose the tracebacks.
- CSCee26364—MN SA Deleted on **clear ip mobile binding** CLI on HA

The Security-Association for the NAI is deleted when one of the flows are closed on HA. This symptom has been observed on a router that is running Cisco IOS release 12.3T.

The following conditions exist:

 - Configure the “load-sa” config on HA and open multiple flows for same NAI.
 - Close one of the flows and subsequently, the Security Association for the NAI is deleted, even though the other MIP flow is active.
 - If any other new flow is opened, new security association is again invoked from AAA.

Workaround: none.
- CSCee34368—Standby HA Crashed in this Scenario

A Cisco router running Home Agent R2.0 software and configured as Standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA.

This condition exists when the bindings on the standby HA are cleared after reloading the active HA.

This problem is very rare and was seen only once during testing.

Workaround: none.

- CSCee37327—HA Reloaded Upon Clearing Bindings in this Scenario

On a Cisco 7200/7600 router running Home Agent R2.0 software, alignment and spurious memory errors occur and HA may reload when bindings are cleared after a stress test.

The errors are seen only when NAI related CLI (**ip mobile host nai**) is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the radius server.

Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.
- CSCee52886—Proxy DHCP: Active HA Releases the DHCP Address on Standby Interface

The active HA releases the DHCP address for the binding when the HSRP interface of the standby HA goes down, when proxy DHCP allocation is configured.

This condition is observed when the standby HA's HSRP interface is shut down while the active and standby has active Mobileip bindings with dynamic allocation using proxy DHCP.

Workaround: none.
- CSCee56692—Spurious Memory Access Observed While Opening Bindings With DHCP

On a Cisco 7200/7600 router running Home Agent R2.0 Software, spurious memory access is observed on the standby HA while opening and closing of bindings using DHCP.

This condition exists when opening and closing Mobile IP bindings using DHCP, and the HA is configured with redundancy.

Workaround: none.
- CSCee60087—Tracebacks Observed While Opening Bindings With DHCP

On a Cisco 7200/7600 router running Home agent R2.0 Software tracebacks observed while opening bindings with DHCP.

This condition exists when opening and closing 30000 MOIP bindings with 30 calls/sec using DHCP, then opening 30000 MOIP bindings with DHCP and accounting configuration. Tracebacks are observed on the active HA after opening of bindings.

Workaround: none.
- CSCee60490—Standby HA Crashed After Unconfig And Config Of IP Mobile Host

On a Cisco 7200/7600 router running Home agent R2.0 software, the standby HA crashed after unconfiguring and configuring ip mobile host.

Workaround: none.
- CSCef83013—Proxy DHCP:Home Agent Stops DHCP-Proxy Lease After One Iteration

The Home Agent stops DHCP-proxy lease after one iteration of active standby switchover for a Proxy Mobileip binding when dynamic address allocation is configured for the user.

Workaround: none.
- CSCef86760—Standby HA Reloads on Bindupdate from Active HA When Pre-emption is Configured

The standby Home Agent reloads on receiving a bind update from the active when pre-emption is configured

The reload is observed only after repeating the switchover more than once .

Workaround: none.

- CSCin79571—HA Cannot Install SA for RRQ With Unknown Extension
The HA drops RRQ under following conditions:
 - RRQ has an unknown extension.
 - HA downloads MHAЕ Shared Key for the user from radius server in 3gpp2-mn-ha-shared-key format.

Workaround: ensure that the MN and FA do not send an unknown extension in RRQ.
- CSCin79585—**show run** Displays Invalid Commands
When **ip mobile home-agent nat traversal keepalive 10** is configured, the following configurations appear:


```
ip mobile home-agent revocation traversal keepalive 10
ip mobile home-agent nat traversal keepalive 10
```

This has no effect on revocation or NAT traversal feature behavior, but, when the HA is reloaded, revocation may get disabled.

Workaround: remove **ip mobile home-agent revocation traversal keepalive 10** from the startup configuration, or reconfigure revocation manually on reload.
- CSCin81895—HA Does Not Change Tunnel When PATed Address and Port Changes
When the PATed address or port changes, the HA does not change the remote tunnel endpoint. As a result, subsequent traffic does not get encoded correctly.

Workaround: none.

Unresolved Caveats Prior to IOS 12.3(8)XW2

The following caveats are unresolved in Cisco IOS Release 12.3(8)XW1:

- CSCed50425—Interface Drops on NPE-G1 Leading To Performance Hit on HA
On a 7200 VXR NPE-G1 functioning as Home Agent, significant drops are observed on Gigabit interface thereby causing a drop in performance of the product.

Workaround: none.
- CSCed92442—New Session Hotlining Not Applied for PMIP Flows
On a Cisco router running Home Agent release 2.0, Proxy Mobile IP flow fails to come up for “New Session” Hot-lining.

Workaround: none.
- CSCed94887—Process Received Unknown Tracebacks Found During RF Lost its Peer
Flapping of MOIP bindings, the RF lost its peer. After some time the process received unknown tracebacks were observed on console.

Workaround: none.
- CSCee01788—Clearing the VRF Routing Table Should Not Delete the MN’s address
Clearing the VRF routing table using the clear ip route command also deletes the route corresponding to the Mobile Node.

Workaround: do not clear IP routes using the **clear ip route** command.

- CSCee18252—Active and Standby HA Crashed While Flapping MOIP Bindings
While opening and closing bindings on Home Agent (HA) at a high rate, both active and standby HAs reloaded.
The following sequence of events caused both the active and standby HAs to reload:
 - Flap large number of bindings at high rate.
 - After some time the active HA is reloaded from SUP.
 - Standby HA became active. Open MIP Bindings.
 - Old active HA became standby.
 - After some time both standby and active HA reloaded.**Workaround:** none.
- CSCee19678—Tracebacks on MWAM HA When Interface is Shut While Running Load Test
When a Home Agent is handling calls and traffic to simulate background load conditions, and a processor acting as active is forcibly made standby by shutting down the interface, NULLIDB Tracebacks will appear.
Workaround: none.
- CSCee22616—**show ip mobile binding vrf summary** Command Shows Incorrect Bind Count
The **show ip mobile binding vrf summary** command displays the wrong value under the following conditions:
 - Without VRF configuration, open a binding.
 - After the above step, configure VRF.
 - Clear the binding in HA.
 - Observe that the sh ip mob bin vrf sum command displays the wrong value.**Workaround:** ensure that VRF configuration exists before opening bindings.
- CSCee25439—Proxy DHCP: Active HA Reloads on Unconfig IP Address on HSRP Interface
The active HA reloads on unconfiguring the HSRP interface address, after opening a binding for a user with dhcp-proxy-client.
The following conditions exist
 - a. Bring up HA1. HA2 with Home Agent redundancy configured.
 - b. Configure Proxy DHCP client for a user for dynamic address allocation (with loopback configuration).
 - c. Bring up a flow for the user.
 - d. The binding comes up and both HAs are in sync.
 - e. Go to the interface where HSRP is configured on HA1 and configure no ip address.
 - f. HA1 crashes.**Workaround:** unconfigure the HSRP interface IP address only if there are no active flows.

- CSCee26364—MN SA Deleted on clear ip mobile binding CLI on HA

Security-Association for the NAI is deleted when one of the flows are closed on HA under the following conditions:

- Configure the load-sa configuration on the HA and open multiple flows for same NAI.
- Close one of the flows and subsequently, the security association for the NAI is deleted, even though the other MIP flow is active.
- If any other new flow is opened, new security association is again invoked from AAA.

Workaround: none.

- CSCee31554—Miscellaneous Problems with ODAP Lease Renewal

Lease time is not in sync on the active and standby HAs. This will result in the active and standby HAs being out of sync.

The following conditions exist:

- Open large number of bindings on active and standby HA
- Reload active MWAM
- Standby HA becomes active, and try to renew lease, some subnets are out of sync with server. Unable to renew lease. Server is deleting subnets after lease expiry. Because of this both active and standby bindings are deleted.

Additional issues causing subnet renewal problem after switchover include:

- a. Bulk sync is started before the system clock is synchronized. Because of this, after the system clock is synchronized, there will be DHCP server bindings with inaccurate expiration timestamp.
- b. When DHCP proxy client syncs the subnet leases, the client-id's may be different for subnet leases for the same poolname. This is because the client-id is derived from the router's hostname and in box-to-box redundancy, the hostname may differ between the two redundant units. DHCP subnet allocation server uses the client-id to identify binding, hence, incorrect client-id leads to DHCPNAK being sent from the subnet allocation server.

Workaround: avoid getting into the first condition by not switching over until the new active has a chance to renew the leases.

Once the first condition manifests itself, manually clear the affected subnet from the active and standby units.

- CSCee32072—Subnets Are Not Synced on Standby ODAP Server After Reload

Subnets do not sync from Active ODAP server to standby, after standby is reload.

When you open a large number of bindings, the leased subnets are available on both active and standby ODAP servers. Reload the standby server using the reload command. After the standby comes back it is not syncing subnets from active.

Workaround: none.

- CSCee32075—Active and Standby HAs Keep Reloading by RF Induced One After Other

Both active and standby HAs keeps reloading with Redundancy Framework (RF) induced reload, one after the other. This behavior started after the active HA reloaded and preempted.

Workaround: none.

- CSCee34368—Standby HA Crashed in this Scenario

The standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA. This problem is very rare and was seen only once during testing. The bindings on the standby HA are cleared after reloading the active HA.

Workaround: none.
- CSCee35970—Spurious Memory access when aaa user-password configured

Spurious memory access is seen when the **ip mobile home-agent aaa user-password** command is configured, and a user with default password “cisco” tries to download a security association from AAA.

Workaround: use default password “cisco”.
- CSCee37245—CLI **ip mobile secure aaa-download rate 100** Not Working

Security Associations are not downloaded when the **ip mobile secure aaa-download rate 100** command is configured.

Workaround: do not use the **ip mobile secure aaa-download rate 100** command on the HA image.
- CSCee37327—HA Reloaded Upon Clearing Bindings in This Scenario

Alignment and spurious memory errors occur, and the HA may reload when bindings are cleared after a stress test as explained in the conditions below.

The errors are seen only when NAI related CLI (**ip mobile host nai**) is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the RADIUS server.

Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.
- CSCee40397—Standby ODAP Server Reloading Without Any Preempt on Active Server

The standby ODAP server reloads without any Preempt configuration on active with RF interdev config.

The ODAP servers are configured with redundancy (HSRP and RF interdev configured). On reload of an active MWAM card, the standby processor will become active. After some time the current active server reloads without any preempt configured on original active processor.

Workaround: none.
- CSCee43739—Bulk Synch Fails When One of the Redundant HAs is Upgraded to R2.0 Load

In a redundant HA setup, during an upgrade, when the standby HA is brought down with the new R2.0 load and brought back to service with the active HA still running the R1.2 load, bindings do not get synched to the HA with R2.0 load.

The active HA complains about unsupported VendorID in the BindInfo Request Bulk synch message sent by the standby HA, and sends back BindInfo Reply with unknown CVSE-Type error.

Workaround: upgrade when no active bindings are present.
- CSCee48909—Hotlining is Not Enabled For a NAI with Static Address Allocation

Hot Lining is not enabled for a NAI-based MN with static IP address allocation.

If the **ip mobile host** command is configured with **nai**, instead of configuring **realm** and specifying static IP address allocation, as below, Hot-lining is not enabled for that host.

Workaround: none.

- CSCee56692—Spurious Memory Access Observed While Opening Bindings with DHCP

On a Cisco router running Home Agent Release 2.0 Software in a redundant network, spurious memory access is observed on standby HA while opening and closing of bindings using DHCP. The problem only occurs when IP address allocation is from DHCP.

Workaround: none.
- CSCee60087—Tracebacks Observed While Opening Bindings with DHCP

On a Cisco router running Home Agent Release 2.0 Software “Null IDB” tracebacks are observed while opening bindings with DHCP.

The following sequence of actions lead to this issue:

 - Open large number of MOIP Bindings using DHCP.
 - Close all the bindings.
 - Reopen the bindings, with accounting configured using DHCP.
 - After opening of bindings Tracebacks observed on Active HA.

Workaround: none.
- CSCee60490—Standby HA Crashed After Unconfig and Config of ip mobile host

On a Cisco router running Home Agent Release 2.0 Software in a redundant mode, the standby HA reloads intermittently when unconfiguring and configuring **ip mobile host** command.

Workaround: none.
- CSCee74444—Ignore-spi Option is Not Synched From Active to the Standby HA

In a redundant Home Agent network, the option to use RFC2002bis or RFC2002 style of authentication calculation (learned by the active HA on a per-PDSN basis) is not relayed to the standby HA.

Workaround: none.
- CSCee79934—Cannot Remove **tunnel route-map** Command

When a *routemap name* is configured for mobile ip tunnels using the **ip mobile tunnel route-map** command, you cannot unconfigure the route-map using **no ip mobile tunnel route-map**.

Workaround: There is no workaround to unconfigure the route-map configuration. However, if the running-config with the this CLI has not been saved to the memory, the router can be reloaded.
- CSCin58815—HA Crashes While Processing 32 Byte Key in 3gpp2 Format

The HA reloads while processing 32-byte key in 3gpp2 format. Currently, the HA accepts MN-HA-SHARED-KEY or hex format key in Cisco Av-pair attribute of length 16 bytes only. The expected behavior for other length keys in this format is to reject the RRQ.

Workaround: Use the MN-HA-SHARED-KEY of max 16 bytes
- CSCef16369—Active HA Reloads on HA Failover Due to Interface Shutdown

In an Active-Standby configuration, where both active and standby has equal priority, after an active to standby transition, when a MIP flow is closed, the active HA reloads.

Workaround: none.

Unresolved Caveats Prior to IOS 12.3(8)XW

The following caveats were unresolved in Cisco IOS Release 12.3(7)XJ1, which was the release branch just prior to IOS 12.3(8)XW:

- CSCed50425—Interface Drops on NPE-G1 Leading To Performance Hit on HA

On a 7200 VXR NPE-G1 functioning as Home Agent, significant drops are observed on Gigabit interface thereby causing a drop in performance of the product.

Workaround: none.
- CSCed91609—Memory Leak While Opening And Closing IPSEC Bindings

When bindings are brought up and torn down on IPSEC tunnels for an extended periods of time using multiple iterations, a is seen.

Workaround: none.
- CSCed92442—New Session Hotlining Not Applied for PMIP Flows

On a Cisco router running Home Agent release R2.0, Proxy Mobile IP flow fails to come up for “New Session” Hot-lining.

Workaround: none.
- CSCed94849—RF-induced Lost Peer During Opening and Closing of MIP Bindings

When flapping (Open and Closing) of Mobile IP Bindings with ODAP, the RF lost its peer. This happens only under stressed conditions.

Workaround: configure path-retransmit, assoc-transmit timeouts to avoid this problem.
- CSCed94887—Process Received Unknown Tracebacks Found During RF Lost its Peer

Flapping of MOIP bindings, the RF lost its peer. After some time the process received unknown tracebacks were observed on console.

Workaround: none.
- CSCed95076—IPSEC Tunnel Goes Down After 5 Hours Even If Bindings Exist

When mobile IP bindings are opened over different tunnels, and each over IPSEC tunnel, if the router loaded with HA is left idle for around 5 hours, the IPSEC tunnel goes down.

Workaround: none.
- CSCee01788—Clearing the VRF Routing Table Should Not Delete the MN’s address

Clearing the VRF routing table using the **clear ip route** command also deletes the route corresponding to the Mobile Node.

Workaround: do not clear IP routes using the **clear ip route** command.
- CSCee10809—ODAP HA Redundancy: Subnet Not Synced on Lease Expiry

When ODAP with HA redundancy is configured, the subnets on the Standby and Active may not match as observed from **show ip dhcp pool**.

Workaround: clear the mismatched subnets manually using **clear ip dhcp pool pool-name subnet** command.

- CSCee16186—Crypto Map Removed in Interface Configuration on Linkstate Changes
When the interface configured with crypto map has interface link state changes (due to administratively shutting the interface, or link connectivity issues), crypto map is removed from the interface. The problem is observed when the **ip mobile tunnel crypto map** *map-name* command is configured.
Workaround: remove the **ip mobile tunnel crypto map** configuration.
- CSCee18252—Active and Standby HA Crashed While Flapping MOIP Bindings
While opening and closing bindings on Home Agent (HA) at a high rate, both active and standby HAs reloaded.
The following sequence of events caused both the active and standby HAs to reload:
 - Flap large number of bindings at high rate.
 - After some time the active HA is reloaded from SUP.
 - Standby HA became active. Open MIP Bindings.
 - Old active HA became standby.
 - After some time both standby and active HA reloaded.**Workaround:** none.
- CSCee19678—Tracebacks on MWAM HA When Interface is Shut While Running Load Test
When a Home Agent is handling calls and traffic to simulate background load conditions, and a processor acting as active is forcibly made standby by shutting down the interface, NULLIDB Tracebacks will appear.
Workaround: none.
- CSCee22616—**show ip mobile binding vrf summary** Command Shows Incorrect Bind Count
The **show ip mobile binding vrf summary** command displays the wrong value under the following conditions:
 - Without VRF configuration, open a binding.
 - After the above step, configure VRF.
 - Clear the binding in HA.
 - Observe that the **sh ip mob bin vrf sum** command displays the wrong value.**Workaround:** ensure that VRF configuration exists before opening bindings.

- CSCee25439—Proxy DHCP: Active HA Reloads on Unconfig IP Address on HSRP Interface

The active HA reloads on unconfiguring the HSRP interface address, after opening a binding for a user with dhcp-proxy-client.

The following conditions exist

- Bring up HA1. HA2 with Home agent redundancy configured
- Configure Proxy DHCP client for a user for dynamic address allocation (with loopback configuration).
- Bring up a flow for the user.
- The binding comes up and both HAs are in sync.
- Go to the interface where HSRP is configured on HA1 and configure **no ip address**.
- HA1 crashes.

Workaround: unconfigure the HSRP interface IP address only if there are no active flows.

- CSCee26364—MN SA Deleted on **clear ip mobile binding** CLI on HA

Security-Association for the NAI is deleted when one of the flows are closed on HA under the following conditions:

- Configure the **load-sa** configuration on the HA and open multiple flows for same NAI.
- Close one of the flows and subsequently, the security association for the NAI is deleted, even though the other MIP flow is active.
- If any other new flow is opened, new security association is again invoked from AAA.

Workaround: none.

- CSCee31554—Miscellaneous Problems with ODAP Lease Renewal

Lease time is not in sync on the active and standby HAs. This will result in the active and standby HAs being out of sync.

The following conditions exist:

- Open large number of bindings on active and standby HA
- Reload active MWAM
- Standby HA becomes active, and try to renew lease, some subnets are out of sync with server. Unable to renew lease. Server is deleting subnets after lease expiry. Because of this both active and standby bindings are deleted

Additional issues causing subnet renewal problem after switchover include:

- Bulk sync is started before the system clock is synchronized. Because of this, after the system clock is synchronized, there will be DHCP server bindings with inaccurate expiration timestamp.
- When DHCP proxy client syncs the subnet leases, the client-ids may be different for subnet leases for the same poolname. This is because the client-id is derived from the router's hostname and in box-to-box redundancy, the hostname may differ between the two redundant units. DHCP subnet allocation server uses the client-id to identify binding, hence, incorrect client-id leads to DHCPNAK being sent from the subnet allocation server.

Workaround: avoid getting into the first condition by not switching over until the new active has a chance to renew the leases.

Once the first condition manifests itself, manually clear the affected subnet from the active and standby units.

- CSCee32072—Subnets Are Not Synced on Standby ODAP Server After Reload

Subnets do not sync from active ODAP server to standby, after standby is reload.

When you open a large number of bindings, the leased subnets are available on both active and standby ODAP servers. Reload the standby server using the **reload** command. After the standby comes back it is not syncing subnets from active.

Workaround: none.
- CSCee32075—Active and Standby HAs Keep Reloading by RF Induced One After Other

Both active and standby HAs keeps reloading with Redundancy Framework (RF) induced reload, one after the other. This behavior started after the active HA reloaded and preempted.

Workaround: none.
- CSCee34368—Standby HA Crashed in this Scenario

The standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA. This problem is very rare and was seen only once during testing. The bindings on the standby HA are cleared after reloading the active HA.

Workaround: none.
- CSCee35970—Spurious Memory access when aaa user-password configured

Spurious memory access is seen when the **ip mobile home-agent aaa user-password** command is configured, and a user with default password “cisco” tries to download a security association from AAA.

Workaround: use default password “cisco”.
- CSCee37245—CLI **ip mobile secure aaa-download rate 100** Not Working

Security Associations are not downloaded when the **ip mobile secure aaa-download rate 100** command is configured.

Workaround: do not use the **ip mobile secure aaa-download rate 100** command on the HA image.
- CSCee37327—HA Reloaded Upon Clearing Bindings in This Scenario

Alignment and spurious memory errors occur, and the HA may reload when bindings are cleared after a stress test as explained in the conditions below.

The errors are seen only when NAI related CLI (**ip mobile host nai**) is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the RADIUS server.

Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.
- CSCee40397—Standby ODAP Server Reloading Without Any Preempt on Active Server

The standby ODAP server reloads without any Preempt configuration on active with RF interdev config.

The ODAP servers are configured with redundancy (HSRP and RF interdev configured). On reload of an active MWAM card, the standby processor will become active. After some time the current active server reloads without any preempt configured on original active processor.

Workaround: none.

- CSCee43739—Bulk Synch Fails When One of the Redundant HAs is Upgraded to R2.0 load

In a redundant HA setup, during an upgrade, when the standby HA is brought down with the new R2.0 load and brought back to service with the active HA still running the R1.2 load, bindings do not get synched to the HA with R2.0 load.

The active HA complains about unsupported VendorID in the BindInfo Request Bulk synch message sent by the standby HA, and sends back BindInfo Reply with unknown CVSE-Type error.

Workaround: upgrade when no active bindings are present.
- CSCee48909—Hotlining is Not Enabled For a NAI with Static Address Allocation

Hot Lining is not enabled for a NAI-based MN with static IP address allocation.

If the **ip mobile host** command is configured with **nai**, instead of configuring **realm** and specifying static IP address allocation, as below, the Hot lining is not enabled for that host.

Workaround: none.
- CSCee56692—Spurious Memory Access Observed While Opening Bindings with DHCP

On a Cisco router running Home Agent R2.0 Software in a redundant network, spurious memory access is observed on standby HA while opening and closing of bindings using DHCP.

The problem only occurs when IP address allocation is from DHCP.

Workaround: none.
- CSCee59345—Basic HSRP Stops Working After Interface on Active SHUT

On a Cisco router running Home Agent software R2.0 in a redundant mode, HSRP operation stops working after changing interface on active HA into Shutdown state. When the HSRP interface on active HA is shutdown, the HRSP state of standby HA does not change to Active. The original active HA also still remains in the active state.

Workaround: none.
- CSCee60087—Tracebacks Observed While Opening Bindings with DHCP

On a Cisco router running Home agent R2.0 Software 'Null IDB' trace backs are observed while opening bindings with DHCP.

The following sequence of actions lead to this issue:

 - Open large number of MOIP Bindings using DHCP.
 - Close all the bindings.
 - Reopen the bindings, with accounting configured using DHCP.
 - After opening of bindings Tracebacks observed on Active HA.

Workaround: none.
- CSCee60490—Standby HA Crashed After Unconfig and Config of **ip mobile host**

On a Cisco router running Home agent R2.0 Software in a redundant mode, the standby HA reloads intermittently when unconfiguring and configuring **ip mobile host** command.

Workaround: none.

- CSCee60979—Hotlined Packets Are Not Redirected When the Packet Size is Small

On Cisco router running Home Agent software release R2.0, for small sized data packet (example 36, 48 bytes), the packets do not get redirected even though the flow is actively hotlined. This problem is observed only for small sized packets and is not seen if the packet is of size 100 or greater.

Workaround: none.
- CSCee74444—**ignore-spi** Option is Not Synched From Active to the Standby HA

In a redundant Home Agent Network, the option to use RFC2002bis or RFC2002 style of Authentication calculation (learned by the active HA on a per-PDSN basis) is not relayed to the standby HA.

Workaround: none.
- CSCin75665—Cannot Unconfigure And Re-configure **mobileip route map**

On Cisco router running Home Agent software release R2.0, Mobile IP route-map cannot be unconfigured and then re-configured using the **ip mobile tunnel route-map** command.

Workaround: none.
- CSCin58815—HA Crashes While Processing 32 Byte Key in 3gpp2 Format

The HA reloads while processing 32-byte key in 3gpp2 format. Currently, the HA accepts MN-HA-SHARED-KEY or hex format key in **Cisco Av-pair** attribute of length 16 bytes only. The expected behavior for other length keys in this format is to reject the RRQ.

Workaround: Use the MN-HA-SHARED-KEY of max 16 bytes

Open Caveats Prior to Cisco IOS Release 12.3(7)XJ1

The following caveats are unresolved in Cisco Release 12.3(7)XJ:

- CSCec80327—With NAI-based Debug Cond, AE Debugs Not Printed While Parsing RRQ

With NAI-based debug condition set, the debugs pertaining to Parsing of authentication extension in MIP RRQ are not printed.

The problem is observed when a NAI based condition is set to filter the debugs.

Workaround: either set the ip address based condition to filter debugs, or do not set any debug conditions.
- CSCed24163—Standby Not Renewing Lease Time When Proxy DHCP is Configured

Once an active HA is reloaded, the standby HA is not able to renew the DHCP lease, and eventually the Mobile ip binding gets deleted on the HA.

On reload the active HA returns the address to the DHCP server. This happens after the standby renews the lease time, to which DHCP binding gets deleted from the Server; thus further renewals fail.

Workaround: none.

- CSCed91609—Memory Leak While Opening and Closing IPSEC Bindings
When bindings are brought up and torn down on IPSEC tunnels for an extended periods of time using multiple iterations, memory leak of 0.8MB to 1MB is seen.
When 235k bindings are opened and closed, a memory leak of 0.8 MB is observed in each iteration. The 235k bindings are opened over 40 IPSEC tunnels (and 40 Mobile IP tunnels).
Workaround: none
- CSCed94849—RF-induced Lost Peer During Opening and Closing of MIP Bindings
When flapping (Open and Closing) of Mobile IP Bindings with ODAP, the RF lost its peer. This happens only under stress conditions.
Workaround: to avoid this problem, configure path-retransmit and assoc-transmit timeouts.
- CSCed94887—Process Received Unknown Tracebacks Found During RF Lost its Peer
Flapping of MOIP bindings, RF lost its peer. After some time, process received unknown tracebacks observed on console.
Workaround: none.
- CSCed95076—IPSEC Tunnel Goes Down After 5 Hours Even if Bindings Exist
When an HA that has MobileIP bindings, opened over different Mobile IP tunnels and also over different IPSEC tunnels, is left idle for 5 hours, the IPSEC tunnel goes down while Mobile IP binding and tunnel still exist.
Workaround: none.
- CSCee10809—ODAP HA Redundancy: Subnet Not Synced on Lease Expiry
When ODAP with HA redundancy is configured, the subnets on the standby and active may not match as observed from **show ip dhcp pool**.
Workaround: clear the mismatched subnets manually using the **clear ip dhcp pool *pool-name* subnet** command.
- CSCee01788—Clearing the VRF Routing Table Should Not Delete the MNs Address
Clearing the VRF routing table with the **clear ip route** command also deletes the route corresponding to the Mobile Node.
Workaround: Do not clear IP routes with the **clear ip route** command.
- CSCee16186—Crypto Map Removed in Interface Configuration on Linkstate Changes
When an interface with crypto map has interface link state changes (for example, administratively shutting the interface, or link connectivity issues), **crypto map** is removed from the interface and the **crypto map** CLI is deleted from the interface. The **crypto map** command should not be removed from the interface.
Workaround: none.

- CSCee18252—Active and Standby HA Reloads While Flapping MOIP Bindings
While opening and closing bindings on Home Agent (HA) at a high rate, both active and standby HAs reloaded.
The following sequence of events result in a reload of both Active and Standby HA:
 - a. Flap bindings at a high rate.
 - b. After some time Active HA is reloaded from SUP.
 - c. Standby HA became active. Opening MIP Bindings.
 - d. Old active HA became standby.
 - e. After some time, both the standby and active HA reloaded.

Workaround: none.
- CSCee19678—Tracebacks on MWAM HA when interface is shut while running load test
When a Home Agent is handling calls and traffic to simulate background load conditions, and a processor acting as active is forcibly made standby by shutting down the interface, NULLIDB Tracebacks will appear.
Workaround: do not shut the active interfaces, such as interface between the HA-FA, and the HA-RADIUS.
- CSCee25439—Proxy DHCP: Active HA Reloads on Unconfig **ip address** on HSRP Interface
After you open a binding for a user with dhcp-proxy-client, the active HA reloads if you unconfigure the hsrp interface address.
The following conditions exist:
 - a. Bring up HA1 HA2 with Home Agent redundancy configured.
 - b. Configure Proxy dhcp client for a user for dynamic address allocation (with loopback configuration).
 - c. Bring up a flow for the user.
 - d. The binding comes up and both the HAs will be in sync.
 - e. Go to the interface where HSRP is configured on HA1 and configure **no ip address**.
 - f. HA1 crashes.

Workaround: Unconfigure the hsrp interface IP address only if there are no active flows.
- CSCee22616—**show ip mobile binding vrf summary** Command Shows Incorrect Bind Count
The **show ip mobile binding vrf summary** command displays the wrong value under the following conditions:
 - Without VRF configuration, open a binding.
 - Configure VRF.
 - Clear the binding in HA.
 - Observe that the **show ip mob bin vrf sum** command displays the wrong value.

Workaround: ensure that VRF configuration exists before opening bindings.

- CSCee26076—Binding Not Deleted When MN Address is Returned to Pool Due to DHCP Lease Expiry

When dhcp-proxy-client address allocation is used on lease expiry, although the address is returned back to the pool, the Mobile IP binding is not deleted.

Workaround: none.
- CSCee26364—MN SA Deleted on **clear ip mobile binding** Command on HA

Security-Association for the NAI is deleted when one of the flows are closed on the HA.

The following conditions exist:

 - Configure the **load-sa** command on the HA and open multiple flows for same NAI.
 - Close one of the flows: subsequently, the Security Association for the NAI is deleted, even though the other mip flow is active.
 - If any new flow is opened, a new security association is invoked from AAA.

Workaround: none.
- CSCee31554—ODAP Lease Renewal Out of Sync on Active and Standby

Lease time is not in sync on active and standby HAs. This causes the active and standby HAs to be out sync.

The following conditions exist:

 - Open 25 k bindings on active and standby HA.
 - Reload active MWAM.
 - The standby HA becomes active, and when it tries to renew lease, some subnets are out of sync with server, and are unable to renew lease. The server is deleting subnets after lease expiry, and thus both active and standby bindings are deleted

Workaround: none.
- CSCee32072—Subnets Are Not Synced on Standby ODAP Server After Reload

Subnets do not sync from active ODAP server to standby, after standby is reloaded.

This condition exists when you open 25 k bindings. Leased subnets are available on both the active and standby ODAP server. Reload the standby server using the **reload** command. After the standby comes back up it is not syncing subnets from the active.

Workaround: none.
- CSCee32075—Active and Standby HA Keep Reloading by RF-induced, One After the Other

Both active and standby HAs keep reloading with RF-induced reload, one after the other. This behavior started after active HA reloaded and Preempted.

Workaround: none.
- CSCee34368—Standby HA Crashed in this Scenario

The standby HA reloads when bindings are cleared while the standby exchanges HSRP state information with the active HA. This problem is very rare and was seen only once during testing.

The bindings on standby HA are cleared after reloading the active HA.

Workaround: none.

- CSCee35970—Spurious Memory Access When AAA User-password Configured

Spurious memory access is seen when the **ip mobile home-agent aaa user-password** command is configured, and a user with default password “cisco” tries to download a security association from AAA.

Workaround: use default password “cisco”.
- CSCee37236—Unable to Unconfigure Non-Nai with Virtual-network CLI

Unconfiguring the **ip mobile host** command fails when configured for a Non-NAI user on a virtual-network. This condition arises only when you unconfigure the command specifying the whole CLI.

Workaround: use only a partial configuration (for example, **no ip mobile host x.x.x.x** to unconfigure the command).
- CSCee37327—HA Reloaded Upon Clearing Bindings in This Scenario

Alignment and spurious memory errors occur and the HA may reload when bindings are cleared after a stress test.

The errors are seen only when the NAI-related **ip mobile host nai** command is configured and unconfigured while mobiles are sending messages, traffic is flowing upstream through the sessions established by these nodes, and Change of Authorization messages are sent by the RADIUS server.

Workaround: do not change the NAI related configuration for a mobile while sessions are being brought up or down.
- CSCee37245—CLI **ip mobile secure aaa-download rate 100** not working

Security Associations are not downloaded when the **ip mobile secure aaa-download rate 100** command is configured.

Workaround: Do not use the **ip mobile secure aaa-download rate 100** command on the HA image.
- CSCee40397—Standby ODAP Server Reloading Without any Preempt on Active Server

The standby ODAP server reloads without any Preempt configuration on active with RF interdev configuration.

The ODAP Servers are configured with redundancy (HSRP and RF interdev configured). On reload of the active MWAM card, the standby processor will become active. After some time the current active server reloads without any preempt configured on original active processor.

Workaround: none.
- CSCee43739—Bulk Synch Fails When One of the Redundant HA Upgraded to R2.0 Load

In a redundant HA setup during an upgrade, when the standby HA is brought down with the new R2.0 load and brought back to service with the Active HA still running R1.2 load, bindings do not get synched to the HA with R2.0 load.

The Active HA complains about unsupported VendorID in the BindInfo Request Bulk synch message sent by the Standby HA and sends back BindInfo Reply with unknown CVSE-Type error.

Workaround: upgrade when no active bindings are present.
- CSCee52886—Proxy DHCP: Active HA Releases the DHCP Address on Standby Interface

The active HA releases the DHCP address for the binding when the HSRP interface of standby HA goes down (when proxy DHCP allocation is configured).

This condition is observed when the Standby HA’s HSRP interface is shut down, while the active and standby has active Mobileip bindings with dynamic allocation using proxy DHCP.

Workaround: none

- CSCin58815—HA Reloads While Processing 32 Byte Key in 3gpp2 Format**

The HA reloads while processing 32-byte key in 3gpp2 format. Currently, the HA accepts MN-HA-SHARED-KEY or hex format key in “Cisco Av-pair” attribute of length 16 bytes only. The expected behavior for other length keys in this format is to reject the RRQ.

Workaround: Use MN-HA-SHARED-KEY of max 16 bytes
- CSCin72654—RRQs With Non-zero HA Addr Not Supported With SLB in Dispatched Mode**

When HA-SLB operates in dispatched mode, it forwards MIP RRQs to the real HAs without changing the destination IP address. So when HAs receive RRQs with non-zero Home-agent address the destination IP address will be that of the SLB virtual server. The binding is established but the HA sends back an RRP with the destination ip address of the received packet as the home-agent address regardless of the home-agent address in the RRQ. So the tunnel is established between the FA and the vserver addr.

Subsequent re/de-registrations are sent to HA-SLB instead of the HA. The SLB drops the de-registrations as the lifetime is zero and can forward the re-registrations to some other HA. So the concerned HA may/will not get the re/de-registrations.

Workaround: Do not use HA-SLB in dispatched mode when the incoming RRQs have a non-zero home-agent address.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.3(11)YF:

- CSCed65017—MWAM: Config CLI That Fail Batch Mode Copy Fail config-mode sup**

Some configuration commands fail, do not operate properly, or cause dead memory when using batch mode config download or config-mode supervisor.

This problem occurs when the MWAM processor is configured for “supervisor” config-mode.

Workaround: use config-mode local on MWAM..
- CSCee45296—MWAM Does Not Retrieve its Configuration From the Supervisor**

When using config on supervisor with the MWAM, the processors are not able to retrieve their configurations from the supervisor.

This problem was first seen when using supervisor release 122-18.2.2.SX. This defect would be present in all future supervisor releases when mated with an MWAM IOS image that did not contain this fix.

Workaround: configure an arbitrary tftp-server (for example, tftp-server nvram:startup-config) on the supervisor. It does not matter what file you serve up, even one of the mwam configs. If you do serve up one of the MWAM configs, be sure to add the alias: “tftp-server bootflash:SLOTxPCy.cfg alias SLOTxPCy.cfg”.

Supervisor release 122-18.2.2.SX changed the mechanism used by the MWAM processors to retrieve their configurations. This ddts changed the mechanism used by the MWAM processors to be compatible with the supervisor IOS change. This ddts is also backwards compatible with previous supervisor images.
- CSCeg23873—TACACS+ Authorization Does Not Work For Mobile IP**

Authorization for Mobile IP subscribers does not work using TACACS+.

Workaround: authorize using RADIUS or locally configured security associations.

- CSCeg26637—Standby HA Crashed While Opening a Binding.
Removing the **ip mobile host** configuration command from the standby Home Agent may cause the agent to reload if registration requests are concurrently being received for those mobile hosts.
Workaround: deconfigure from the active home agent first.
- CSCin84717—Standby HA Does Not Clear the Binding When Interface is Shut
The standby HA does not clear bindings when the HSRP interface on the standby is shut.
This problem occurs under the following conditions:
 - Open a binding.
 - Binding is open on both active and standby HAs
 - Shut the standby HSRP interface
 - Binding still exists on standby and is not cleared.**Workaround:** Bindings on the standby HA cannot be cleared manually through CLI.
- CSCin83939—All Bindings Do Not Get Synced With Reload of Active HA
If bindings are opened with finite lifetime, the active HA can not bulk sync 235k bindings to the standby HA.
Workaround: open bindings with infinite lifetime.
- CSCin83952—**inforeq** and **inforeply** of IP Mobile CLI Are Not nvgened
The **ip mobile redundancy** command options **inforeq** and **inforeply**, when configured, are not written into NVRAM.
Workaround: re-configure the **ip mobile redundancy** command with the **inforeq** and **inforeply** options, on every reload of the Home Agent.

Resolved Caveats Prior to 12.3(11)YF

The following Cisco Mobile Wireless Release 2.0 caveats are resolved in Cisco Release 12.3(8)XW3:

- CSCed92442—New Session Hotlining Not Applied For PMIP Flows
On the Home Agent, Packet of Disconnect is enabled even if the STC value downloaded in the Access-Accept message has the value 2 for Proxy Mobile IP flows.
On the Home Agent, the Hotlining feature is not enabled for a new session Hotlining. When Hotlining is enabled in the Access-Accept message during the authentication phase for the Proxy Mobile IP flow, it is disabled.
This condition occurs only for Proxy Mobile IP flows.
Workaround: none.
- CSCee18252—Active & Standby HA crashed while flapping MOIP Bindings
On a Cisco 7200/7600 router running Home Agent R2.0 software, during flapping of MOIP bindings both active and standby HA are crashed.
This condition occurs when flapping of MOIP Bindings at 100 bindings/sec for about 4 hours.
Workaround: none.

- CSCef37978—Conditional Debugging Support for UDP Tunnel Debug Messages

When conditional debugging is enabled on HA and mobileip debugs are enabled, UPD tunneling related debugs are not filtered based on condition.

Workaround: none.
- CSCef77084—Router Reload When ODAP is Deconfigured While Subnet Expires

In some rare timing scenario, the router may reload when the On Demand Address Pool is deconfigured while the subnet failed to be renewed.

Workaround: First, clear all subnets in the DHCP pool and ensure that all of them have been released. The ODAP may automatically request and receive another subnet after the last one has been released. At this time the DHCP pool can be deleted. The new subnet will automatically be released back to the subnet allocation server.
- CSCef83013—Proxy Dhcp :Home Agent Stops DHCP-Proxy Lease After One Iteration

The Cisco Home Agent stops dhcp-proxy lease , after one iteration of active standby switchover for a Proxy Mobileip binding when dynamic address allocation is configured for the user.

This condition is seen after one iteration of active standby switch over.

Workaround: none.
- CSCef89392—Issue With MIP Binding Sync With HA Redundancy

When the MIP flow is deleted and then the interface on HA is brought back up, the HA becomes active and updates its stale bindings to the standby HA.

This condition occurs when the interface on Active HA is shutdown and standby becomes active. And later, the interface is brought up to make this HA as active.

Workaround: Specify the HA IP address in the **ip mobile homeagent address** *ha-ip-addr* command. This will help clear the bindings when interface is shut on HA.
- CSCin63246—MWAM-HA Assumes Challenge of 4-bytes From Client in CCoA Mode.

On the Cisco c6svcmwam-h1is-mz MWAM Home Agent image, when the HA receives MFCE (Mobile Foreign Agent Challenge Extension), the HA performs authentication using the CHAP challenge in MFCE. While sending Access-Request to AAA, the HA truncates the challenge to 4 byte value. This results in authentication failure.

Workaround: none.
- CSCin81895—HA Does Not Change Tunnel When PATed Address and Port Changes

When NAT Traversal is enabled on Home Agent, and the NAT device in the path deletes the previous NAT mapping and allocates a new NAT mapping with a different source address and port number for a re-registration request from the mobile node, the Home Agent continues to tunnel traffic to old NAT mapping.

Workaround: none.

- CSCin82739—Show Command to Display HHAE Info on Home Agent

The show ip mobile secure command is introduced in 12.3(8)XW3 and displays active standby home agent security associations. Here is the CLI and a sample output:

HA#show ip mobile secure ?

foreign-agent Foreign agent security associations
home-agent Home agent security associations
host Mobile host security associations
summary Summary of SAs

```
HA#show ip mobile secure hom
HA#show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
    SPI 100, MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'red'
HA#
HA#
```

- CSCin83266—Virtual Mobile Routes Dissappear From Routing Table on i/f shut/no-sh

On a Cisco router running HA R2.0 software, the mobile virtual network routes disappear after an interface is shut and no-shut.

The ondition occurs when two HSRP groups are configured on two different interfaces and the non-HA interface is shut and no-shut.

Workaround: none.

- CSCin83952—Inforeq and Inforeply of **Ip Mobile** CLI are not Nvgened

When configured, the **ip mobile redundancy** command options **inforeq** and **inforeply** are not written into NVRAM

Workaround: Re-configure the **ip mobile redundancy** command with the **inforeq** and **inforeply** options on every reload of the Home Agent.

- CSCin83939—All Bindings Dont Get Synced With Reload of Active HA

If bindings are opened with a finite lifetime, the active HA can not bulk sync 235k bindings to the standby HA.

Workaround: Open bindings with infinite lifetime.

Resolved Caveats Prior to 12.3(8)XW3

The following caveats are resolved in Cisco Release 12.3(8)XW2:

- CSCee25439—Proxy DHCP: Active HA Reloads On Unconfig IP Address on HSRP Interface
The active HA reloads when you unconfigure the HSRP interface address after opening a binding for a user with dhcp-proxy-client.
The following conditions exist:
 - a. Bring up HA1, HA2 with Home Agent redundancy configured.
 - b. Configure Proxy dhcp client for a user for dynamic address allocation (with loopback configuration).
 - c. Bring up a flow for the user.
 - d. The binding come up and both the HAs will be in sync.
 - e. Now go to the interface where HSRP configured on HA1 and configure **no ip address**
 - f. HA1 crashes.

Workaround: unconfigure the HSRP interface IP address only if there are no active flows.
- CSCee28326—HA Reloads on Executing **show ip mobile host** command
A Cisco 7200/7600 router running Home Agent R2.0 software may reloads when the **show ip mobile host** command is executed.
The security association needs to be downloaded from the RADIUS server when the binding is created. Additionally, the node that is currently being displayed using the **show ip mobile host** command is being deleted, then the Home Agent may reload.
This problem is very rare and was seen only once during testing.
Workaround: use the **show ip mobile binding** command to display the details of the host or binding.
- CSCee31554—ODAP Lease Renewal Out of Sync on Active and Standby
On Cisco 7600 running HA Release 2.0 image, lease time is not sync on Active and Standby HA's. This will result into out of sync between Active and Standby HA.
Open 25 k bindings on active and standby HA reload active mwam standby HA become active, and try to renew lease, some subnets are out of sync with server. Unable to renew lease. Server is deleting subnets after lease expiry. Due to this both active and standby bindings are deleted
Workaround: none.
- CSCee43739—Bulk Synch Fails When One of the Redundant HAs Upgraded to R2.0 Load
In a redundant Cisco Home Agent (HA) network, when the standby HA is upgraded from a R1.2 to R2.0 load, bindings do not get synched to the Standby HA.
This problem is only seen when the redundant HA with an R2.0 load tries to synch bindings from the HA with R1.2 load.
Workaround: upgrade when no active bindings are present.
- CSCee91930—Proxy DHCP: Bind Deletion Info Needs to be Updated to Standby HA
Mobileip bind deletion information is not synced to the standby in lease expiry when Address allocation used is the dhcp-proxy-client.
This problem occurs when proxy DHCP is used, and the lease renewal fails to happen.
Workaround: none.

- CSCef18987—POD Debugs Display NACK Error Message For a Valid POD Request

A Cisco PDSN running R2.0 S/W incorrectly displays a NACK message being sent even though it correctly sends an ACK message to RADIUS server in response to a POD request.

This condition occurs when the POD feature is enabled, and the PDSN receives a POD request from RADIUS server with only NAI and NAS-ID and no session identification attributes in it.

Workaround: none

- CSCef19117—**ip tcp adjust-mss** Command Fails to Set Value For Outbound Packets

Cisco router configured with the **ip tcp adjust-mss** command may fail to set the value for outbound packets.

The command works on 12.3(7)T2 code, but fails on 12.3(8)T code. This issue has currently been seen on a 3700 router.

Workaround: disable cef.



Note Disabling cef can affect the router performance, however, this issue is not seen with cef disabled on the router.

- CSCef29763—HA Redundancy Operation Fails For Dynamic Users With Local SA Config

A mobileip re-registration request is rejected in the following scenarios:

- Bindings established on active and synched to standby
- Failover happens
- Re-registration request received by new active.

This condition occurs when the Home Agent is deployed in active-standby redundant mode.

Workaround: reload both active and standby at the same time.

- CSCef50822—Sibyte HANG After Overnight High Rate of IPPDP Open/Close

The Sibyte processor can hang when RF induced reload occurs.

This condition occurs when the active and standby switchover is required, RF induces reload.

Workaround: none. Use the **reload all** command from PC to bring the processor back to normal state.

- CSCef57825—Home Agent Redundancy Sync Issue For AAA Load-SA User

On a standby Home Agent mobileip binding is not synched after reconfiguration of **ip mobile home-agent redundancy** CLI.

This condition is observed for users with **aaa load-sa** configured

Workaround: use local authentication on home agent

- CSCef59046—Reloaded By Bus Error When Issuing IP Mobile

The router reloaded by bus error when the customer issued **no ip mobile host nai @xxx.xxx.xxx.xxx address pool local ha-pool interface FastEthernet x/x aaa** command after configuring **ip mobile host nai @xxx.xxx.xxx.xxx address pool local ha-pool interface FastEthernet x/x aaa**.

Workaround: none.

- CSCin80289—**ip mobile home-agent unknown-ha** Configuration Problem
On a Cisco HomeAgent router when the **ip mobile home-agent** command is configured with the **unknown-ha** option (along with another home-agent option), the **show running** command does not display the whole command line interface.
Workaround: configure the **ip mobile home-agent unknown-ha** command on a separate line and the remaining commands on a separate line.
- CSCin81015—Access-group in ACLs Are Not Applied For UDP Tunnel
The **ip access-group group in** command, configured on tunnel template, does not get applied to mobileip tunnels, when UDP tunneling is used.
Workaround: use the **ip access-group group out** command instead.

Resolved Caveats Prior to 12.3(8)XW2

The following caveats were resolved in Cisco Release 12.3(8)XW1:

- CSCin80483—Overlapping Physical Address of CPU in SiByte Causes Reload in HA
Cisco Cat6500/7600 MWAM platform running XW Home Agent (HA) image may reload while it is loading with startup configuration having large configurations (for example, ip localpool configurations).
Workaround: Unconfigure the local pool configuration from the startup configuration. This will help prevent the CPUs from reloading. However, with large configurations on MWAM after startup, the CPU can reload later when configured.

Resolved Caveats Prior to 12.3(8)XW1

The following caveats are resolved in Cisco Release 12.3(8)XW:

- CSCee10809—ODAP HA Redundancy: Subnet Not Synced on Lease Expiry
When ODAP with HA redundancy is configured, the subnets on the standby and active may not match as observed from the **show ip dhcp pool** command.
Workaround: clear the mismatched subnets manually using **clear ip dhcp pool pool-name subnet** command.
- CSCee16186—Crypto Map Removed in Interface Configuration on Linkstate Changes
When the interface configured with crypto map has interface link state changes (due to administratively shutting the interface, or link connectivity issues), crypto map is removed from the interface. The problem is observed when the **ip mobile tunnel crypto map map-name** command is configured.
Workaround: remove the **ip mobile tunnel crypto map** configuration.
- CSCee60979—Hotlined Packets Are Not Redirected When the Packet Size is Small
On Cisco router running Home Agent software release 2.0, for small sized data packet (example 36, 48 bytes), the packets do not get redirected even though the flow is actively hotlined.
This problem is observed only for small sized packets and is not seen if the packet size is 100 or greater.
Workaround: none.

- CSCee82340—Lifetime Value of the Mobileip Binding Gets Reset on Standby HA
In a redundant HA setup when standby HA come up and downloads the bind info from active HA, the Lifetime remaining on standby HA is reset back to the initial value. This leads to discrepancies in lifetime values on the active and standby HAs. This problem is seen when a bulksync happens between the standby and active HA.
Workaround: none.
- CSCee06722—CPU Hog Observed While Mobile IP is Processing Mobile Bindings
On a Cisco 7200/7600 router running Home Agent Release 2.0 Software, CPU HOG is observed when synching of subnets from active to standby. The problem is observed in a redundant HA setup with a preempt configuration, and with address allocation from ODAP.
Workaround: none.

Resolved Caveats Prior to Cisco IOS 12.3(8)XW

The following caveats are resolved in Cisco Release 12.3(7)XJ1, which was the branch release just prior to the Cisco IOS 12.3(8)XW release:

- CSCec80327 With NAI-Based Debug Cond, AE Debugs Not Printed While Parsing RRQ
On the Cisco HA image, with NAI based debug condition set, the debugs pertaining to parsing of authentication extension in MIP RRQ are not printed.
The above-mentioned problem is observed when a NAI-based condition is set to filter the debugs.
Workaround: The workaround is as follows:
 - a. Set the IP address based condition to filter debugs, or
 - b. Do not set any debug condition.
- CSCed24163—Standby Not Renewing Lease Time When Proxy DHCP is Configured
Once the active HA is reloaded, the Standby HA is not able to renew the DHCP lease, and eventually the Mobile IP binding gets deleted on the HA.
On reload, the active HA returns the address to DHCP server. This happens after the standby renews the lease time due to which DHCP binding gets deleted from the Server. Thus further renewals fail.
Work around: none.
- CSCee06278—Binding Not Cleared on Standby HA When Active Ha Receives POD Msg
The problem is seen on Cisco routers running Home Agent R2.0 software in a redundant network. When a binding is deleted on the active Home Agent due to receipt of Radius Disconnect message, it does not automatically delete the corresponding binding on standby Home Agent.
Workaround: none.
- CSCee23500—Clearing Bindings on Active HA Do Not Get Synched to Standby HA
A Cisco router running the Home Agent in a redundant mode does not synch the bindings deleted due to **clear** command to the peer HRSP Home Agent.
Workaround: none.

- CSCee26076—Proxy DHCP: MIP Binding Does Not Get Deleted on Lease Expiry and Address
On a Cisco MWG Home Agent running R2.0 image, when dhcp-proxy-client address allocation is used (on lease expiry), although the address is returned back to the pool, the Mobile IP binding is not deleted.

Workaround: none.
- CSCee33437—Prefix Length NVSE Should Not be Added when ZECC Not in Use
Mobile nodes which can not ignore NVSE may fail initial registration because of the inclusion of a Prefix length NVSE.

Workaround: none.
- CSCee49350—The HA Rejects RRQ When HA Address is Specified on Loopback Interface
Home Agent rejects Registration Request (RRQ) from mobile when Home Agent address is configured on Loopback interface and address allocation for the mobile is done from local pool.

Workaround: do not configure the Home Agent address as a Loopback address.

The problem is seen because configuring the Home Agent address under Loopback interface treats the redundancy setup in a peer-to-peer mode. In this mode, loop pool is not allowed for redundancy. This issue is solved by adding a new **mode active-standby** variable in the **ip mobile home-agent redundancy** command.
- CSCee58458—HA Should Support RFC 3002 Authenticator Extn on Per PDSN Basis
A Cisco router running the Cisco Home Agent (HA), always sends out Registration revocation message with Authentication extension (AE) as described in RFC 3012bis. The HA should be able to append the AE in RFC 3012 or RFC 3012bis format on a per PDSN basis.

Workaround: none.
- CSCee59479—Standby HA Crashes When Processing bindupdate From Active Unit
In a redundant Home Agent network, the standby HA intermittently reloads while processing the Bindupdate from the active unit during sync process.

Workaround: none.
- CSCee78149—Clock Summer-time not Synced To Processor While Clock Timezone Does
The clock summer-time configuration is not synced from supervisor to MWAM processor, while clock timezone is being synced alright. So, the timezone on the MWAM processor is wrong during daylight savings time.

This problem occurs when the **clock summer-time** command is configured on the supervisor.

Workaround: none.
- CSCee82340—Lifetime Value of the Mobile IP Binding Gets Reset on Standby HA
In a redundant HA setup, when standby HA come up and downloads the bind info from Active, the lifetime remaining on Standby HA is reset back to the initial value. This leads to discrepancy in lifetime values on Active and standby HA.

This problem is seen when a bulk synch happens between the standby and active.

Workaround: none.

- CSCee82344—Tracebacks seen while opening a PMIP session

Tracebacks, due to alignment error, can be seen on Home Agent while opening Proxy Mobile IP flows when ip mobile debugging is turned on.

The problem is observed only for Proxy Mobile IP flows and IP mobile debugging is turned on.

Workaround: do not enable IP mobile debugging.
- CSCee82571—HomeAgent Reloads When Revocation is Triggered Without FHAE

The Cisco Home Agent reloads on receiving Registration Revocation message when the Revocation feature is enabled, but the Foreign Home (FH) Security Association (SA) is not configured.

Workaround: configure FH SA when enabling the registration revocation feature.
- CSCee84947—Active HA Reloads Due To Corrupted Program Counter

In a redundant Home Agent network, the active HA reloads when the standby downloads mobileip bindings and security associations after it goes down and comes back up. The program counter gets corrupted and causes the Home Agent to reload.

Workaround: none.
- CSCin72654—RRQs With Non-zero HA Addr Not Supported With SLB in Dispatched Mode

When HA-SLB operates in dispatched mode, it forwards MIP RRQs to the real HAs without changing the destination IP address. So, when the HAs receive RRQs with non-zero Home-agent addresses, the destination IP address will be that of the SLB virtual server.

The binding is established, but the HA sends back an RRP with the destination IP address of the received packet as the *home-agent address* regardless of the *home-agent address* in the RRQ. So the tunnel is established between the FA and the vserver address.

Subsequent re/de-registrations are sent to HA-SLB instead of the HA. The SLB drops the de-registrations as the lifetime is zero, and can forward the re-registrations to some other HA. So the concerned HA may or will not get the re/de-registrations.

Workaround: Do not use HA-SLB in dispatched mode when the incoming RRQs have a non-zero home-agent address.
- CSCin73111—RRQ With Incorrect HA Field Requires Better Debug Msg

Requirement 1: When not using the *unknown-ha* CLI option, debug error message displayed for RRQ (where the Home Agent address is not right) is incorrect. Proper debug message needs to be printed under such conditions.

Requirement 2: In this case, the HA should return to the PDSN with “unknown HA” as the error code in RRP.

Workaround: none.
- CSCin73113—Better Debugs for RRP and Options That Are Sent to be Printed

Better debug messages are required on the HA to display the details about the registration reply message contents and options sent back in the reply.

Workaround: none.
- CSCin73831—Support for Resource Revocation with HA Redundancy

In the current implementation on R2.0 HA, Mobile IP Registration Revocation feature is not supported with HA redundancy. Support for the Resource Revocation feature with HA redundancy is required.

Workaround: none.

- **CSCin75173—Incorrect Value Sent for STC Attribute in Radius Access-Request**
On a Cisco router running Release 2.0 Home Agent software, in rare situations, an incorrect value is sent for the STC attribute in a Radius Access-Request message, when RADIUS disconnect capability is enabled on PDSN.
Workaround: none.
- **CSCin74799—HA Should Support Hex Key of Length Less Than 16 Bytes**
If configured in hex format, the MN-HA shared key should always be 16bytes long. A hex key with length less than 16 bytes results in authentication failure.
Workaround: Use key format as *string* instead of hex.
- **CSCin75572—HA should Enable/Disable POD Per Binding and Parse STC in Access-Accept**
As per IS835C, the HA should provide enable or disable radius disconnect capabilities for a session based on the STC attribute value authorized for the user by the AAA. In the current implementation, the STC attribute received in the Access-Accept message from AAA is not used to enable or disable the radius disconnect capability per user. Currently, the capability can be enabled or disabled at the box level.
Workaround: none.
- **CSCin76846—unknown-ha Option Not Working on HA**
The **unknown-ha accept** option in the **ip mobile home-agent unknown-ha accept** CLI is not working as expected. The Home Agent rejects the Mobile IP registration request (RRQ) with error code “Unknown HA”, instead of accepting the RRQ.
Workaround: none.

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 40](#)
- [Platform-Specific Documents, page 41](#)
- [Feature Modules, page 41](#)
- [Cisco IOS Software Documentation Set, page 41](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3(8)XW:

- *Cisco Mobile Wireless Home Agent* at the following url:
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xw/index.htm>

The following documents are specific to Release 12.3 and are located on CCO :

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cisco IOS Release 12.3: Cross-Platform Release Notes

- *Caveats for Cisco IOS Release 12.3 T*

See *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2 and Release 12.2 T.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Caveats



Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II**, or at <http://www.cisco.com/support/bugtools>.

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

Platform-Specific Documents

Documentation specific to the Cisco 7206 Router is located at the following locations:

- On CCO at: <http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/index.htm> and at <http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm>

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

- On CCO at: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/index.htm>

Documentation specific to the Cisco Catalyst 6500 Switch is located at the following location:

- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

Feature Modules

Feature modules describe new features supported by Release 12.3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

Technical Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: New Feature Documentation

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References

Release 12.3 Documentation Set



Note

You can find the most current Cisco IOS documentation on CCO. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO at:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/index.htm>



Note

Cisco Management Information Base (MIB) User Quick Reference is no longer published. If you have an account with CCO, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to CCO, press **Login: Technical Support: Software Center: Network Mgmt Software: Cisco Network Management Toolkit: Cisco MIBs**.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section on page 40.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

Copyright © 2004, Cisco Systems, Inc.
All rights reserved.