



CHAPTER 2

Planning to Configure the Home Agent

This chapter provides information that you should know before configuring a Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

- [Supported Platforms, page 2-1](#)
 - [Prerequisites, page 2-1](#)
 - [Configuration Tasks, page 2-3](#)
 - [Upgrading a Home Agent Image, page 2-3](#)
 - [Required Base Configuration, page 2-7](#)
 - [Configuration Examples, page 2-9](#)
 - [Restrictions, page 2-13](#)
 - [Supported Standards, MIBs, and RFCs, page 2-13](#)
 - [Related Documents, page 2-14](#)

Supported Platforms

The Cisco HA is available on Cisco's 7206VXR NPE-400 router, 7206VXR NPE-G1 router, 6500 series switch and 7600 series router. The HA supports Fast Ethernet and Gigabit Ethernet interfaces on these platforms.



Note

Cisco Mobile Wireless Release 3.0, Cisco IOS Release 12.3(14)YX and later, supports both the standard MWAM 512 MB per processor memory option, and the 1 GB per processor memory option.

Prerequisites

- [Catalyst 6500 / Cisco 7600 Series Platform Prerequisites, page 2-2](#)

Cisco 7200 Series Platform Prerequisites

Home Agent on the Cisco 7206VXR NPE-400

following URL on Cisco.com:

http://www.cisco.com/en/US/products/hw/routers/ps341/products_installation_guide_book09186a008007daa6.html

The supported configuration on a Cisco 7206VXR with NPE-400 processor is with 512MB DRAM and one PA-2FE-TX FE port adopter, or two PA-FE-TX port adaptors. PA-2FE-TX port adaptor has two 10/100 based Ethernet ports. PA-FE-TX port adapter has one 10/100 based Ethernet port. The I/O controller on the NPE-400 processor supports two more 10/100 based Ethernet ports. Because the PA-FE-TX is end-of-sale, new configurations require the PA-2FE-TX port adaptor.

For IPSec support, a service adaptor (SA-ISA or SA-VAM2) is required. Because SA-ISA is end-of-sale, new configurations utilizing IPSec will require the NPE-G1 with SA-VAM2.

Home Agent on 7206VXR NPE-G1

Catalyst 6500 / Cisco 7600 Series Platform Prerequisites

Home Agent on 6500 Series Switch

Home Agent on 7600 Series Router

Configuration Tasks

-
-
-

Upgrading a Home Agent Image

Step 1

```
router #hw-module module 3 reset cf:1
Device BOOT variable for reset = cf:1 Warning: Device list is not verified.
>
> Proceed with reload of module? [confirm] % reset issued for module 3
>router#
```

Step 2

```
copy tftp tftp file location pclk# linecard #
```

```

router #copy tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin pcli#3-fs:
Destination filename [c6svcmwam-c6is-mz.bin]?
Accessing tftp://172.31.219.33/images/c6svcmwam-c6is-mz.bin...
Loading images/c6svcmwam-c6is-mz.bin from 10.102.16.25 (via Vlan1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 29048727/58096640 bytes]

29048727 bytes copied in 1230.204 secs (23616 bytes/sec)
router #
2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has started>
2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Do not reset the module till upgrade completes!!>
router #

2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <Application upgrade has succeeded>
2d21h: %SVCLC-SP-5-STRRECVD: mod 3: <You can now reset the module

```

Step 3

```
router#hw-module module 3 reset
```

Upgrading the HA Image From XW-based Image to YX-based Image



Upgrading the Supervisor Image

Step 1

Step 2

boot system disk0 *SUP image name*". Here is an example:

```
boot system disk0 c6k222-pk9sv-mz.122-18.SXD2.bin
```



Perform a "write memory" so that running configuration is saved on both active and standby SUP.

Step 4 reload

Step 5



Note

reload command

Upgrading the HA Image on MWAM

Step 1

hw-module module *slot #* reset cf:1

copy tftp:

plc#

-fs

Step 6



Note

The downgrade process is similar to the upgrade process; the SUP image should be downgraded first, followed by the HA image.



For SXD-based SUP images, if **config-on-SUP**



```
config-local
config-on-sup
```

Changing Configuration on Home Agent in a Live Network

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

reload command to bring the active



Note



Note

Loading the IOS Image to MWAM

Configuration Note

Cisco Multi-processor WAN Application Module Installation and

Required Base Configuration

-
-
-
-

Basic IOS Configuration on MWAM

	Command	Purpose
Step 1	<code>vlan database</code>	
	<code>vlan <i>vlan-id</i></code>	
	<code>exit</code>	
	<code>mwam module port allowed-vlan <i>vlan_range</i></code>	
	<code>MWAM module processor processor <i>number</i></code>	<i>Processor number is from 2 to 6</i>
	<code>int gigabitEthernet</code>	
Step 7	<code>no shut</code>	



	Command	Purpose
Step 8		
Step 9	<code>dot1Q 401</code>	Enables IEEE 802.1Q encapsulation of traffic on a specified sub interface in virtual LANs.
Step 10		
Step 11		



MWAM modules synchronize their timing functions from the Supervisor engine's clock timers. Do not configure the timers on each individual MWAM.

Configuring AAA in the Home Agent Environment

Cisco IOS Security Configuration Guide

	Command	Purpose
Step 1	<code>aaa authentication ppp default group radius</code>	
	<code>aaa authorization network default group radiu</code>	

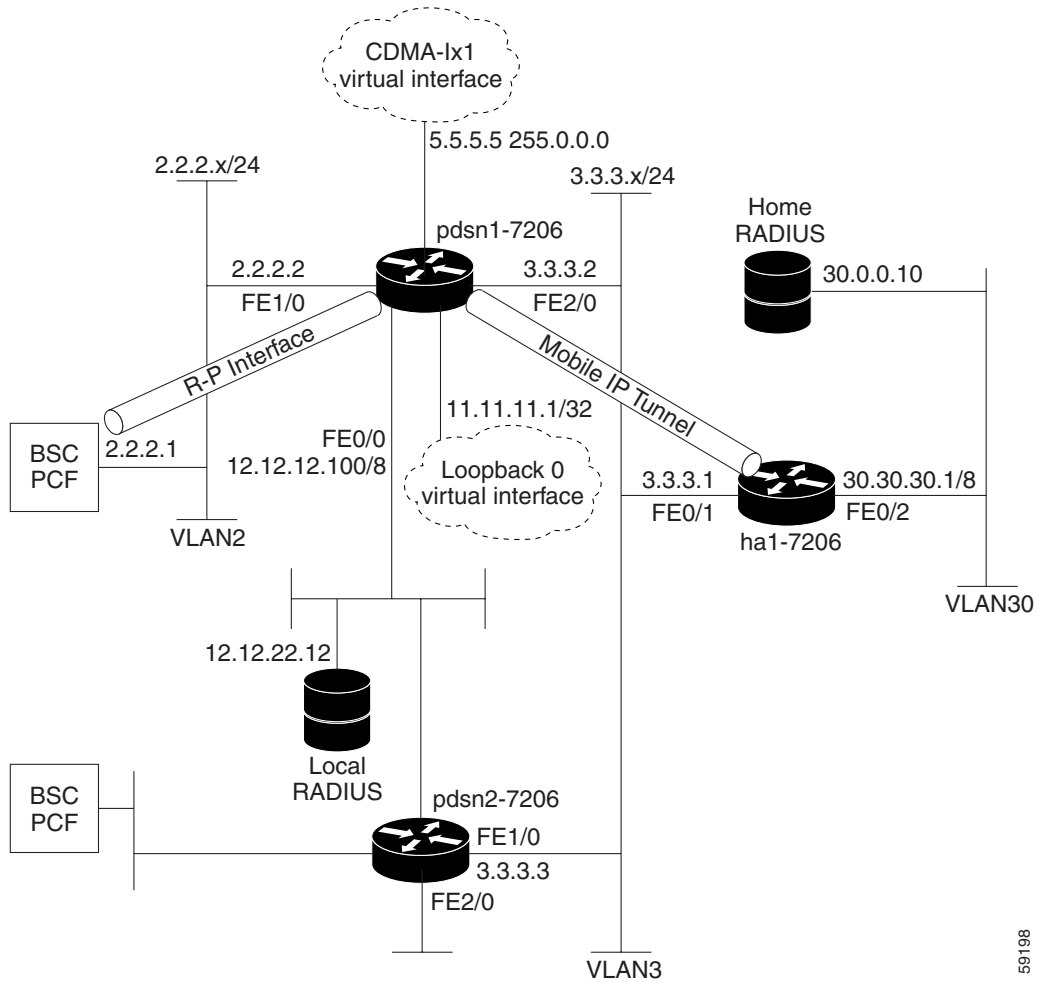


Configuring RADIUS in the Home Agent Environment

	Command	Purpose
Step 1	<code>sharedsecret</code>	

Configuration Examples

Figure 2-1 Home Agent –A Network Map



59198

Example 1

```

aaa authentication login CONSOLE none
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
interface FastEthernet0/1
description To FA/PDSN
ip address 3.3.3.1 255.255.255.0
!
interface FastEthernet0/2
description To AAA
ip address 10.30.30.1 255.0.0.0
!
router mobile
!

```

```
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 10.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
line con 0
  exec-timeout 0 0
  login authentication CONSOLE
```

Example 2-1 Home Agent Configuration

```
Cisco_HA#sh run
Building configuration...

Current configuration : 4532 bytes
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
hostname USER_HA
!
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa session-id common
!
username simulator password 0 cisco
username userc-moip password 0 cisco
username pdsn password 0 cisco
username userc password 0 cisco
username USER_PDSN
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
!!
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.0
!
interface Tunnell
 no ip address
!
```

```
interface FastEthernet0/0
 ip address 10.15.68.14 255.255.0.0
 duplex half
 speed 100
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex half
 speed 10
 no cdp enable
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet1/1
 ip address 10.5.5.3 255.255.255.0 secondary
 ip address 10.5.5.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
!
router mobile
!
 ip local pool ha-pool 10.0.0.1 10.0.15.254
 ip local pool ha-pool1 10.4.4.100 10.4.4.255
 ip default-gateway 10.15.0.1
 ip classless
 ip route 10.3.3.1 255.255.255.255 FastEthernet1/1
 ip route 10.100.0.1 255.255.255.255 9.15.0.1
 ip route 10.17.17.17 255.255.255.255 FastEthernet1/0
 no ip http server
 ip pim bidir-enable
 ip mobile home-agent
 ip mobile host nai userc-moip address pool local ha-pool interface FastEthernet1/0
 ip mobile host nai userc address pool local pdsn-pool interface Loopback0 aaa
 ip mobile secure host nai userc-moip spi 100 key hex ffffffffffffffffffffffffffffffff
 replay timestamp within 150
!
!
radius-server host 10.15.200.1 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

Restrictions

Simultaneous Bindings

Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

Supported Standards, MIBs, and RFCs

RFCs

-
-
-
- The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006
- Reverse Tunneling for Mobile IP, RFC 3024
- Mobile IPv4 Challenge/Response Extensions, RFC 3012
- Mobile NAI Extension, RFC 2794
- Generic Routing Encapsulation, RFC 1701
- GRE Key and Sequence Number Extensions, RFC 2890
- IP Mobility Support for IPv4, RFC 3220, Section 3.2 Authentication
- The Network Access Identifier, RFC 2486, January 1999.
An Ethernet Address Resolution Protocol, RFC 826, November 1982
The Internet Key Exchange (IKE), RFC 2409, November 1998.
Cisco Hot Standby Routing Protocol (HSRP), RFC 2281, March 1998

Cisco IOS Mobile Wireless Home Agent Release 3.0 supports the following standards:

TIA/EIA/IS-835-B, TIA/EIA/IS-835-C and TIA/EIA/IS-835-D

MIBs

- CISCO- MOBILE-IP-MIB—provides enhanced management capabilities.
- Radius MIB—as defined in RADIUS Authentication Client MIB, RFC 2618, June 1999.

The HA implements SNMPv2 as specified in the suite of protocols: RFC 1901 to RFC 1908. The HA supports the MIB defined in The Definitions of Managed Objects for IP Mobility Support Using SMIv2, RFC 2006, October 1995.

A full list of MIBs that are supported on the 7200, 7600 and 6500 series platforms can be found on Cisco web at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Session counters maintained in the MIB cannot be reset using SNMP or CLI. The Home Agent CPU and Memory Utilization counters are accessible using the CISCO-PROCESS-MIB.

The following additional counters will be supported in the Cisco Mobile Wireless Home Agent Release 3.0 MIB:

- Number of Bindings for FA/CoA
- Number of registration requests received per FA/CoA
- Failure counters per FA/CoA—HA Release 2.0 and above supports global failure counters. A per-FA/CoA counter will be added for each of those counters

Related Documents

Cisco IOS Software Documentation

- *Cisco IOS Dial Technologies Configuration Guide*
Cisco IOS Dial Technologies Command Reference
Cisco IOS Interface Configuration Guide
Cisco IOS Interface Command Reference
Cisco IOS IP Configuration Guide
Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services

Cisco IOS Quality of Service Solutions Configuration Guide
Cisco IOS Quality of Service Solutions Command Reference
Cisco IOS Security Configuration Guide

Cisco IOS Security Command Reference

Cisco IOS Switching Services Configuration Guide

Cisco IOS Switching Services Command Reference

Cisco Multi-Processor WAN Application Module Installation and Configuration Note

