



CHAPTER 6

Home Agent Redundancy

This chapter discusses several concepts related to Home Agent redundancy, how Home Agent redundancy works, and how to configure redundancy on the Cisco Mobile Wireless Home Agent.

This chapter includes the following sections:

- [Overview of Home Agent Redundancy, page 6-1](#)
- [Home Agent Session Redundancy Infrastructure, page 6-3](#)
 - [Limitations of Home Agent 4.0 Session Redundancy, page 6-3](#)
 - [Supported Redundancy Events, page 6-3](#)
 - [Bulk Sync Events, page 6-4](#)
 - [Single IP Considerations, page 6-5](#)
- [Geographical Redundancy, page 6-5](#)
- [Redundancy with Radius Downloaded Pool Names, page 6-6](#)
- [HSRP Groups, page 6-6](#)
- [How HA Redundancy Works, page 6-7](#)
- [Physical Network Support, page 6-8](#)
- [Virtual Networks, page 6-9](#)
- [Support for Discontinuous IP Address Pools for the Same Realm, page 6-10](#)
- [Configuring HA Redundancy, page 6-11](#)
- [Home Agent Redundancy Configuration Examples, page 6-13](#)

Overview of Home Agent Redundancy

Cisco Home Agents can be configured to provide 1:1 redundancy. Two Home Agents are configured in hot-standby mode, based on Cisco Hot Standby Routing Protocol (HSRP in RFC 2281). This enables the active Home Agent to continually copy mobile session-related information to the standby Home Agent, and maintains synchronized state information at both Home Agents. In case an active Home Agent fails, the standby Home Agent takes over without service disruption.



Note

NAI support in the Mobile IP HA redundancy feature provides capabilities specific to CDMA2000 for Home Agent redundancy. The CDMA2000 framework requires address assignment based on NAI, and support of multiple static IP addresses per user NAI.

The Home Agent redundancy feature is supported for Static IP Address assignment and IP Address assignment by AAA. Starting in Release 2.0, the Home Agent redundancy feature is supported for Dynamic IP Address assignment using local IP address pools and Dynamic IP Address assignment using Proxy DHCP.

When Home Agent redundancy is configured with Dynamic IP Address assignment using Proxy DHCP, the DHCP information is not synced with the standby while the bindings are brought up, even though the bindings are synced to the standby HA. However, when the standby HA becomes active, a DHCP request for each existing binding is sent out to the DHCP server in order to update the DHCP related information on this Home Agent.

The Hot-lining feature is not supported with HA redundancy.

During the Mobile IP registration process, an HA creates a mobility binding table that maps the home IP address of an MN to the current care-of address of the MN. If the HA fails, the mobility binding table is lost and all MNs registered with the HA lose connectivity. To reduce the impact of an HA failure, Cisco IOS software supports the HA redundancy feature.

**Note**

On configurations based on the Cisco 7600 series platform, the backup Home Agent image is configured on a different SAMI card from the primary.

The functionality of HA redundancy runs on top of the Hot Standby Router Protocol (HSRP). HSRP is a protocol developed by Cisco that provides network redundancy in a way that ensures that user traffic immediately and transparently recovers from failures.

**Note**

HA Session Redundancy is not supported on the Cisco 7301 Series Router.

**Note**

In Cisco Home Agent Release 5.0, the supported redundancy features that are the same as those supported in Release 4.0, except for the MIP-LAC, Mobile Router, VRF, Home Agent as LNS, and Home Agent Accounting features. The Change of Authorization and Packet of Disconnect features are still supported as they are independent of the accounting feature. The active / standby redundancy interaction is between the control processors of the active and standby service blades. There is no need for inter-traffic processor redundancy as the Home Agent accounting feature is not supported in this release.

**Note**

HA Release 5.0 supports both intra-chassis and inter-chassis redundancy.

Home Agent Session Redundancy Infrastructure

Limitations of Home Agent 4.0 Session Redundancy

Home Agent stateful session redundancy till release 4.0 was implemented over HSRP. In that implementation the transport between active and standby HA was implemented by home agent application. The UDP/IP-based transport implementation posed the following limitations:

- Inconstancies in bulk sync scenarios. For example while bulk sync is going on, if bindings are deleted on the active, then at the end of bulk sync completion the number of bindings seen on active and standby is inconsistent.
- Inability to sync multi packet sync data. This is seen during syncing hot-lining rules. When hot lining rules are large in number, the length of data required to be synced is larger to contain in one packet. The ability of syncing such data which is fragmented in multiple packets is inconsistent due to lack of packet sequencing, fragmentation and de-fragmentation support implemented in redundancy transport.

In the Session Redundancy infrastructure enhancement, the previously mentioned limitations are eliminated. In the Home Agent 5.0 release, HA SR infrastructure is implemented over a Component Cluster Manager (CCM). CCM software is built on top IOS High Availability infrastructure which contains (Redundancy Framework) RF/RF-Interdev and CF (Check-Pointing Facility)/SCTP (Stream Control Transport Protocol). RF/RF-Interdev take care of redundancy control signaling and CF/SCTP provides transport mechanism. This HA SR rework brings the advantages of the IOS High Availability feature such as robust transport, inter-chassis/intra-chassis redundancy support.

Supported Redundancy Events

Existing HA 4.0 redundancy events are discussed below. New redundancy events that occur as a result of new features implemented by 5.0 features are discussed in the section appropriate to that feature.

Dynamic Sync Events

Binding Creation

This sync is conveyed by using IPMOBILE_BINDUPDATE_REQ message from active to standby. Standby acknowledges successful recreation of binding using PMOBILE_BINDUPDATE_ACK.

Binding Deletion

This sync is conveyed by using IPMOBILE_BINDDELETE_REQ message from active to standby. Standby acknowledges successful deletion of bindings using IPMOBILE_BINDDELETE_ACK message to active.

Binding Update

Due CoA as a result of hotline status update. When the active HA receives a CoA message in which the hotline status of binding is updated, then the update in the existing binding date is conveyed to standby using IPMOBILE_BINDINTERIM_REQ message. The standby receives the above message, updates the existing binding, and conveys the update status using IPMOBILE_BINDINTERIM_ACK.

Binding Update as a Result of Accounting Counter Sync

When accounting counters are updated during the lifetime of a call then every accounting update message triggers IPMOBILE_BINDSYNC_REQ message to standby which contains updated counters to standby. Standby updates the counters for the bindings on it, and updates the status of updation using IPMOBILE_BINDSYNC_ACK message.

Table 6-1 lists the new sync events implemented for dynamic sync events mentioned above.

Table 6-1 Dynamic Sync Events

Current Event Name	New Event Name	Comment
IPMOBILE_BINDUPDATE_REQ, IPMOBILE_BINDUPDATE_ACK	IPMOBILE_BIND_CREATE	Used to sync Binding creation.
IPMOBILE_BINDINTERIM_REQ, IPMOBILE_BINDINTERIM_ACK	IPMOBILE_BIND_HOTLINE_UPDATE	Used to sync binding update due CoA processing.
IPMOBILE_BINDDELETE_REQ, IPMOBILE_BINDDELETE_ACK	IPMOBILE_BIND_DELETE	This event is synced in presence of De-Registration, PoD, or Revocation. Binding deletion is conveyed using this message.
IPMOBILE_BINDSYNC_REQ, IPMOBILE_BINDSYNC_ACK	Not supported in this release	This event is used to sync accounting counters. But HA accounting counter synchronized is not going to be supported in 5.0.
IPMOBILE_BINDINTERIM_EXTND_REQ	Not Supported	This request is used to sync when the sync message size is large and needs to be sent in multiple packets. This will not be needed new SR

Bulk Sync Events

When a router comes up as the standby it sends IPMOBILE_BINDINFO_REQ to existing active to retrieve all the existing bindings. Active replies in IPMOBILE_BINDINFO_RSP messages which contains binding information. Standby processes IPMOBILE_BINDINFO_RSP messages to recreates bindings on it and replies the status of recreation in IPMOBILE_BINDINFO_ACK message to active. The number of bindings which active can host are to the tune of 500K. Hence during bulk sync process multiple IPMOBILE_BINDINFO_RSP and IPMOBILE_BINDINFO_ACK messages are exchanged between active and standby. In the new implementation active is going to sync IPMOBILE_BIND_CREATE event for each binding to standby which contains bind sync information.

The CCM software implements the bulk sync process through bundling mode during sync of binding from active to standby. This process is completely transparent to HA application. In bundling mode, CCM sends more than one binding info per sync packet to standby CCM. Also CCM provides a CLI to control the bulk sync process. Should the bulk sync process hog cpu operator can make use of CLI redundancy rate

subscriber redundancy rate *# of Sessions Per Unit Time*

This command controls the bulk sync process. In case of number of bindings to be synced during bulk sync process is large then no more than #Sessions Per unit time will be synced. This command ensures that the CPU is not overloaded by the bulk sync process.

Sync Event Behavior

In the new SR Infrastructure, the standby acts as a receiver of the events and messages from the active. The standby does not send any status or acknowledgement message to the active to convey the status of processing any sync event from the active. Hence IPMOBILE_BINDUPDATE_ACK, IPMOBILE_BINDINTERIM_ACK, IPMOBILE_BINDDELETE_ACK messages from standby are discontinued in new framework. This is a significant change from HA 4.0 release. The active HA assumes that the standby is successfully able to decode sync messages, and able to recreate, update, or delete a binding.

Single IP Considerations

With the Home Agent single IP architecture, the SAMI blade is divided in to two logical entities namely Control Plane (CP) and Traffic Plane (TP). Physically, the CP functionality resides on the first of the 6 PPCs on the SAMI blade with the following 5 PPCs taking care of TP processing. The CP processor takes care of all the control signaling (registration, de-registration, CoA, PoD, etc. associated with all the bindings), while the Traffic-Plane Processors (TP) handle traffic distributed across 5 PPCs.

From the SR perspective, redundancy contexts are present on the CP on both the active and standby. So redundancy control signaling and SCTP channel occurs between two CP on the active and standby. It is the responsibility of the CP on the active to dynamically sync binding creation, updates and deletion, on the CP on standby. Upon receiving sync messages it is the responsibility of the CP on the standby to propagate the binding on the TP similar to the way the active CP propagates bindings to the TP.

Although the Single IP feature is built into the HA software, it is tied to the architecture and is a platform specific feature. The Mobile IP redundancy design is agnostic to any architecture-specific aspects.

Geographical Redundancy

Home Agents in a redundant pair can be placed at geographically separate locations using a VPN solution (such as one based on MPLS) instead of a LAN/VLAN between Home Agent pairs. Such a deployment needs to implement correct routing logic in the network to route traffic to one of the Home Agents in the pair. If there is a network failure, both the HAs could transition to HSRP active state in such a deployment. The Home Agent Redundancy feature recovers from such a failure gracefully with minimal loss of bindings. The following scenario describes the failure recovery process:

1. HA1 (high priority) and HA2 (low priority) are deployed in redundant mode over a WAN link. HSRP is running between the home agents over the WAN link.
2. HA1 is active and HA2 is standby.
3. WAN connectivity to HA1 is lost, due to a network fault, so the HSRP link between HA1 and HA2 is lost.

4. HA2 does not receive hello packets, and transitions to active. HA1 remains active as well, for the same reason (the box itself is functional). If this feature is enabled, both HA1 and HA2 lower their priority.
5. Mobile traffic and signaling messages are routed to HA2. HA2 updates its binding table accordingly and if the feature is enabled, increases its priority back to the original value. But the changed home agent state information on HA2 do not get synched to HA1 (which is unreachable).
6. Network fault is corrected, and hello packets exchanged between HA1 and HA2.
7. Without this feature, HA1 remains active and HA2 moves to become standby, leading to loss of latest state information as created on HA2 at step #5. If this feature is enabled, HA1 moves to become standby and HA2 remains active. Hence latest information on HA2 gets synched to HA1. Once state information is replicated, HA1 moves back to its normal priority. This leads to HA1 becoming active and HA2 becoming standby.

As described above, the latest state information is maintained after network fault is corrected. To enable this feature, following commands should be configured on the HA:

track tracking object id application home-agent

This command creates a tracking object to track the home-agent state.

standby track tracking object id decrement priority

This command enables lowering priority as required by step #4 in the above failure scenario.



Note

If preemption is configured, the *priority* value should be greater than the difference in priorities of the active and standby Homeagents.

Redundancy with Radius Downloaded Pool Names

The Cisco Mobile Wireless HA supports AAA downloadable pool names for address allocation. The radius pool-name attributes returned in an access accept for address allocation are “ip-pool” for dynamic address allocation, and “static-ip-pool” for static address authorization. The pool name returned in an access accept to the Home Agent will be synched to standby Home Agent during normal and bulk sync operation. This enables address allocation from the same pool on the standby Home Agent as well.

HSRP Groups

Before configuring HA Redundancy, you must understand the concept of HSRP groups.

An HSRP group is composed of two or more routers that share an IP address and a MAC (Layer 2) address and act as a single virtual router. For example, your Mobile IP topology can include one active HA and one or more standby HAs that the rest of the topology view as a single virtual HA.

You must define certain HSRP group attributes on the interfaces of the HAs so that Mobile IP can implement the redundancy. You can use the groups to provide redundancy for MNs with a home link on either the interface of the group (a physical network) or on virtual networks. Virtual networks are logical circuits that are programmed and share a common physical infrastructure.

How HA Redundancy Works

The HA Redundancy feature enables you to configure an active HA and one or more standby HAs. The HAs in a redundancy group may be configured in an active HA-standby HA role if the HAs are supporting physical networks, or in a Peer HA-Peer HA role if they are supporting virtual networks.

In the first case, the active HA assumes the lead HA role, and synchronizes the standby HA. In the case of virtual network support, Peer HAs share the lead HA role and “update” each other. The Peer HA configuration allows for load balancing of the incoming RRQs, as either HA may receive RRQs. In either scenario, the HAs participating in the redundancy group should be configured similarly. The current support structure is 1 to 1 to provide the maximum robustness and transparency in failover.

HA functionality is a service provided by the router and is not interface specific. Therefore, the HA and the MN must agree on which HA interface the MN should send its registration requests and, conversely, on which HA interface the HA should receive the registration requests. This agreement must factor in the following two scenarios:

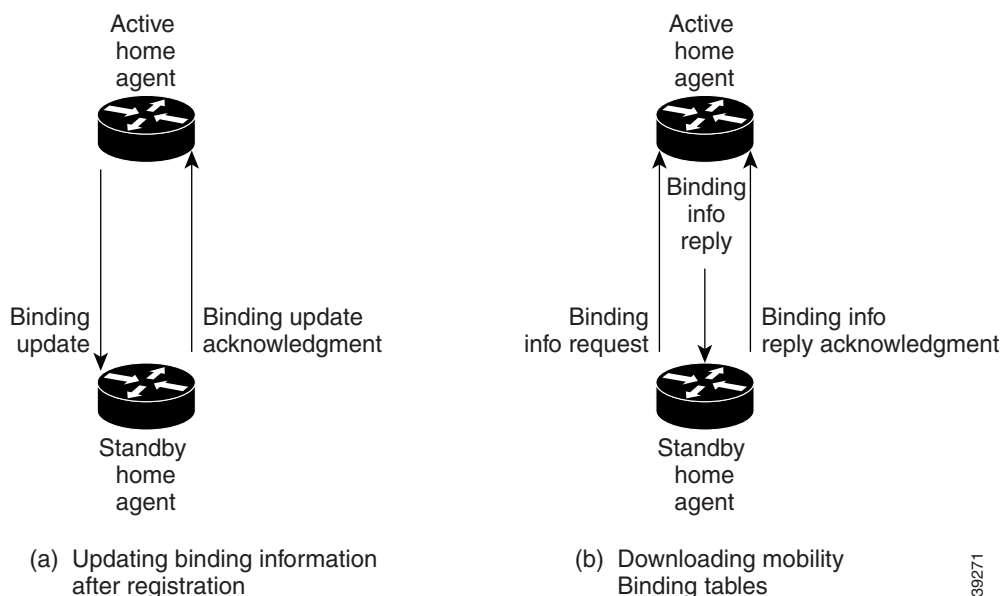
- An MN that has an HA interface (HA IP address) that is not on the same subnet as the MN.
- An MN that requires the HA interface to be on the same subnet as the MN; that is, the HA and the MN must be on the same home network.

For MNs on physical networks, an active HA accepts registration requests from the MN and sends binding updates to the standby HA. This process keeps the mobility binding tables on the active and standby HAs synchronized.

For MNs on virtual networks, the active and standby HAs are peers—either HA can handle registration requests from the MN and update the mobility binding table on the peer HA.

When a standby HA comes up, it must request all mobility binding information from the active HA. The active HA responds by downloading the mobility binding table to the standby HA. The standby HA acknowledges that it has received the requested binding information. [Figure 1](#) illustrates an active HA downloading the mobility bindings to a standby HA. A main concern in this stage of the process is which HA IP interface the standby HA should use to retrieve the appropriate mobility binding table, and on which interface of the standby HA the binding request should be sent.

Figure 1 Overview of HA Redundancy and Mobility Binding Process



**Note**

The active HA-standby HA can also be in peer HA-peer HA configuration.

Physical Network Support

For MNs on physical networks, the HAs are configured in the active HA-standby HA configurations as shown in Figure 2 and Figure 3. The MNs that are supported on this physical network are configured with the HSRP virtual group address as the HA address. Hence, only the active HA can accept RRQs from the MN because it is the owner of the HSRP virtual group address. Upon receipt of an authenticated RRQ, the active HA sends a binding update to the standby HA.

HA Redundancy for physical networks can support multiple HAs in the redundancy group, although only one HA can be in active state, and only one HA can be in standby state. For example, consider the scenario in which there are four HAs in the redundancy group (that is, one active HA, one standby HA, and two HAs in listen state). If the active HA fails, the standby HA becomes the active HA, and the HA in listen state with higher priority becomes the standby HA.

Figure 2 Virtual Network Support Using One Physical Network (Peer HA-Peer HA)

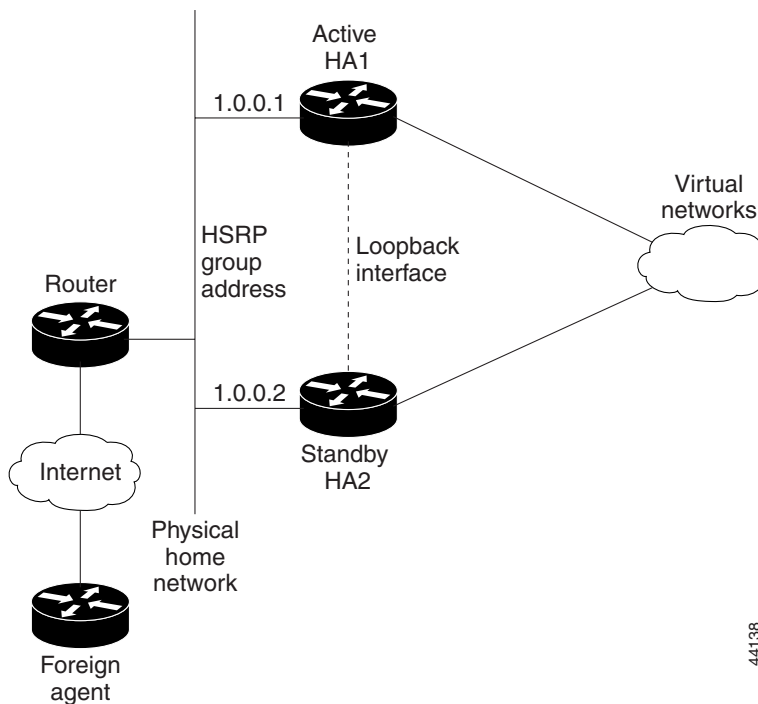
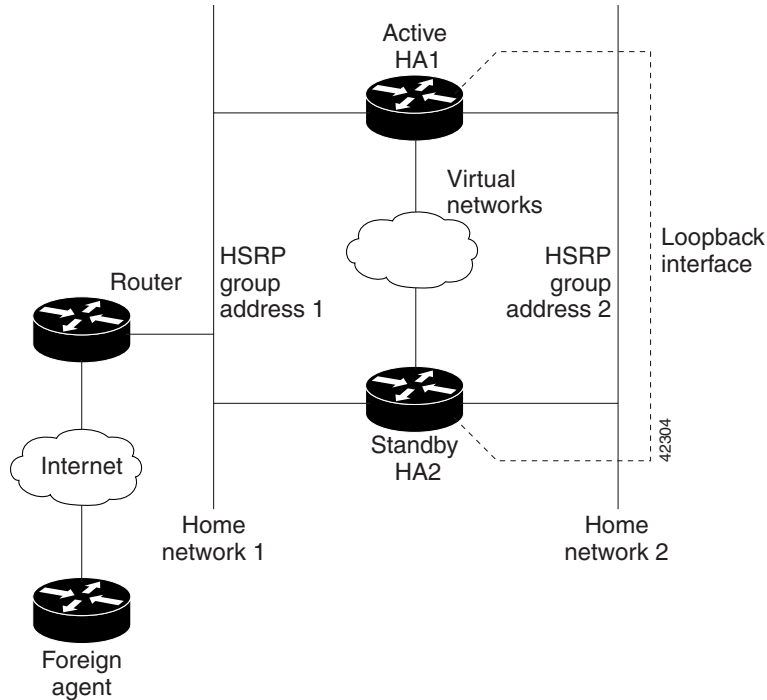


Figure 3 Virtual Network Support Using Multiple Physical Networks (Peer HA-Peer HA)



Virtual Networks

Mobile IP calls for each MN are associated with the home network from which the MN's home IP address is allocated. It is often assumed that this should be a physical network, but there are many cases in deployment where it does not make sense to have each MN attached to a physical network. IOS Mobile IP supports the creation of a software interface called a virtual network. A virtual network is very similar to a loopback interface, but it is owned by the Mobile IP process. Using virtual networks saves Interface Descriptor Blocks (IDBs), and allows Mobile IP specific control over how packets are dropped. When using virtual networks the mobile node is always considered roaming, it can never be attached to its home network. In real world deployments, this can cause some semantic problems. For example in cellular deployment a user may be in their home calling area, but will be roaming from a Mobile IP perspective.

Virtual networks are configured and referenced by a network number and mask pair. It is also possible to associate the virtual network with a Home Agent address for redundancy purposes. Here is an example:

```
ip mobile virtual-network 10.0.0.0 255.255.255.0 address 192.168.100.1
ip mobile host 10.0.0.1 10.0.0.254 virtual-network 10.0.0.0 255.255.255.0
```

Virtual network routes are owned by the Mobile IP routing process and therefore must be redistributed into other routing protocols in order to be propagated. Here is an example:

```
router rip
 redistribute mobile
```

Support for Discontinuous IP Address Pools for the Same Realm

This feature allows the user to specify discontinuous IP address pools for the same realm so that mobiles with NAI can have home addresses assigned from a pool of discontinuous IP address ranges. This will allow the Home Agent to accept Mobiles belonging to multiple virtual networks for the same host group.

This is achieved by configuring a local pool on HA covering the IP address ranges for multiple virtual-networks, and specifying one of the virtual-networks as the home network for the given realm.

The following configuration can be used to allow the HA to accept MNs belonging to multiple virtual networks for the same host group.

```
ip local pool pool1 10.1.1.1 1.1.1.250
ip local pool pool1 10.1.2.1 1.1.2.250

ip mobile home-agent
ip mobile virtual-network 10.1.1.0 255.255.255.0
ip mobile virtual-network 10.1.2.0 255.255.255.0
ip mobile host nai @xyz.com address pool local pool1 virtual-network 10.1.1.0
255.255.255.0 aaa lifetime 65535
```

In the above configuration, two virtual networks are configured and the local pool (pool1) is configured to include the IP addresses for both the virtual networks. By specifying one of the virtual networks and the local pool name in the **ip mobile host** command, the HA will accept MNs belonging to both the networks for the same realm.

Priority Metric for Local Pool

In order to support the ability to change addressing schemes dynamically, a priority metric on a local address pool is introduced. This allows you to create a high priority address pool with the new address scheme. New bindings utilize this new address pool. Existing subscribers continue to use their current address until they disconnect, and upon reconnect they are allocated an address from the new pool. When all subscribers age out of the old address pool, it can be removed.

Currently, different addressing schemes (range of addresses) are configured under the same pool name, and the IP address will be assigned from the pool in the order of configuration. Initially, the first configured range of addresses is used to assign the IP Address, and when all the addresses have been utilized, the subsequent range is then used to assign IP Address, and so on.

To override the above default behavior and configure subscribers to have different address scheme, a priority value is introduced with the pool. This allows you to use the higher priority pool over the lower priority one so that when a new registration request comes, the IP address is assigned from the desired pool.

By default, a priority value of 255 (high priority) is assigned to a newly created local pool. The pool priority value takes a value of 1 to 255, where 0 is less, and 255 is the higher priority.

Here is an example:

```
ip local pool hapool 1.0.0.0 1.0.0.255
ip local pool hapool 2.0.0.0 2.0.0.255
```

This example creates local pools with the priority of 255. An IP address is assigned in the order of configuration if more than one address scheme has the same priority. Initially, all 255 hosts are assigned from the first pool, and the second one will be used for subsequent requests.

```
ip local pool hapool 1.0.0.0 1.0.0.255 priority 200
ip local pool hapool 2.0.0.0 2.0.0.255 priority 100
```

This example creates local pools with the priority of 255. In this case, the IP address is assigned in the order of priority. Initially all 255 hosts are assigned from the second pool (which has a higher priority 100), and the first pool (priority 200) is used for subsequent requests.

Configuring Local Pool Priority Values

To configure a priority value for a local pool, perform the following task:

	Command	Purpose
Step 1	Router(config)# ip local pool {default poolname} [low-ip-address [high-ip-address]] [group group-name] [cache-size size] [priority 1-255] [threshold low-threshold high-threshold]	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, to generate traps when pool utilization reaches a high or low threshold in percentage. The new option priority 1-255 allows you to assign a priority to a newly created pool, and this priority is used to assign IP addresses.

Configuring HA Redundancy

Home Agent Redundancy Tasks (Required for Mobile IP)

To configure your routers for Mobile IP HA redundancy, perform the required tasks described in the following sections:

- [Enabling Mobile IP, page 6-11](#) (Required)
- [Enabling HSRP, page 6-11](#) (Required)
- [Configuring HSRP Group Attributes, page 6-12](#)
- [Enabling HA Redundancy for a Physical Network, page 6-12](#) (Required)
- [Configuring Geographical Redundancy, page 6-13](#)
- [Configuring HA Load Balancing, page 6-13](#)

Enabling Mobile IP

To enable Mobile IP on the router, use the following command in global configuration mode:

	Command	Purpose
Step 1	Router(config)# router mobile	Enables Mobile IP on the router.

Enabling HSRP

To enable HSRP on an interface, use the following command in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# standby [group-number] ip ip-address	Enables HSRP.

Configuring HSRP Group Attributes

To configure HSRP group attributes that affect how the local router participates in HSRP, use either of the following commands in interface configuration mode:

	Command	Purpose
Step 1	<pre>Router(config-if)#standby [group-number] priority priority [preempt [delay [minimum sync] delay]]</pre> <p>or</p> <pre>Router(config-if)#standby [group-number] [priority priority] preempt [delay [minimum sync] delay]</pre>	<p>Sets the Hot Standby priority used in choosing the active router. By default, the router that comes up later becomes standby. When one router is designated as an active HA, the priority is set highest in the HSRP group and the preemption is set. Configure the preempt delay min command so that all bindings will be downloaded to the router before it takes the active role. The router becomes active when all bindings are downloaded, or when the timer expires, whichever comes first.</p>
Step 2	<pre>Router(config-if)# standby group-number follow group-name</pre>	<p>Specifies the number of the follow group and the name of the primary group to follow and share status. We recommend that the specified group number is the same as the primary group number.</p>

Enabling HA Redundancy for a Physical Network

To enable HA redundancy for a physical network, use following commands beginning in interface configuration mode:

	Command	Purpose
Step 1	<pre>Router(config-if)#standby [group-number] ip ip-address</pre>	Enables HSRP.
Step 2	<pre>Router(config-if)# standby name hsrp-group-name</pre>	Sets the name of the standby group.
Step 3	<pre>Router(config)#ip mobile home-agent redundancy</pre>	Enables the Home Agent for redundancy.
Step 4	<pre>Router(config)# redundancy inter-device scheme standby hsrp-group-name</pre> <pre>ipc zone default association 1 no shutdown protocol sctp local-port local-port-no local-ip local-ip-address remote-port remote-port-no remote-ip remote-ip-address</pre>	Configures RF-Interdev on the HA. HA redundancy is built on top of RF-Interdev.

Configuring Geographical Redundancy

To enable Geographical redundancy on the Home Agent, perform the following tasks:

	Command	Purpose
Step 1	Router(config)# track <i>tracking object id</i> application home-agent	Creates a tracking object to track the home-agent state.
Step 2	Router(config)# standby track <i>tracking object id</i> decrement priority	Enables HAs to lower their priority as required in a failure scenario.

Configuring HA Load Balancing

To enable the HA Load Balancing feature, perform these tasks:

	Command	Purpose
Step 1	Router(config)# ip mobile home-agent dynamic-address <i>ip address</i>	Sets the Home Agent Address field in the Registration Response packet. The Home Agent Address field will be set to <i>ip address</i> .

Home Agent Redundancy Configuration Examples

Active-HA Configuration

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
scheme standby cisco
!
!
!
redundancy
no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
association 1
no shutdown
protocol sctp
local-port 5000
local-ip 10.0.0.2
remote-port 5000
remote-ip 10.0.0.3
!
!
aaa new-model

```

```

!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
no auto-sync all
!
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby priority 110
standby preempt delay min 100
standby name cisco
!
interface GigabitEthernet0/0.172
description to AAA
encapsulation dot1Q 172
ip address 172.16.1.8 255.255.0.0
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.254
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
line con 0
line aux 0
line vty 0 4
!
end

```

Standby-HA Configuration

```

~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!

```

```
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby name cisco
!
interface Ethernet2/2
description to AAA
ip address 172.16.1.7 255.255.0.0
no ip route-cache
no ip mroute-cache
duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy algorithm md5 mode
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

Redundancy Support for Hotlining

**Note**

Home Agent Release 5.0 does not support redundancy for the hot-lining feature.

Redundancy Support for QoS

HA release 4.0 and above does not support flow-based QoS policing involving continuous updates of dynamic runtime policymap information between active and standby HA. Since the HA only supports normal and bulk sync, any periodic updates of policing data or counter statistics will not be accurate.

Redundancy Support for Call admission Control (CAC)

At present there is no requirement to support redundancy for Call admission control (CAC). However, the backup Home Agent maintains its own state.

Redundancy Support for Framed-pool Standard

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for Priority-metric for Local Pool

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for Mobile IPv4 Host Configuration Extensions

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

Redundancy Support for WiMAX AAA Attributes

Redundancy is supported with this feature. No additional commands need to be enabled to support this feature.

When HA redundancy is enabled, all attributes included in Access-Request and Accounting messages from the active are also present in the corresponding messages from the standby after switchover. Additionally, interim accounting messages are sent from the standby in the same interval as they are sent from the active. In order to achieve this, the values of the following attributes are synced to the standby.

- Chargeable User Identity (89)
- Acct-Multi-Session-Id (50)
- Acct-Interim-Interval (85)

Redundancy Support for SAMI Migration

It is necessary to have redundancy set up for seamless migration, and to prevent disruption in service. Please refer to the User Migration section in [Planning to Configure the Home Agent](#) chapter for details on how to migrate to the SAMI platform.

