CHAPTER 4

IOS Mobile IP in the Lab

This chapter highlights the major concepts of IOS Mobile IP configuration in a simple lab topology. It presents in detail the most important concepts in IOS Mobile IP configuration. We start out by using six routers to examine each component individually. Several alternatives requiring fewer routers are presented at the end of the chapter. The idea here is to introduce Mobile IP configuration in its simplest form. All of the solutions presented in upcoming chapters are built on the information presented here. The topology presented here was not created just for this example, but is used by the authors as a baseline for most of their Mobile IP lab work.

Building the Baseline Topology

Figure 4-1 shows the basic topology, which is designed to demonstrate all the basic functionality in clearly separated components. It consists of Mobile IP entities—a single Home Agent, two Foreign Agents (FAs), and a Mobile Node—and non-Mobile IP entities—a Correspondent Node (CN) and an intermediate system (IS). Each of these devices is a router capable of running IOS software, as shown in Table 4-1. Feature navigator on Cisco.com can ensure that all features are available on the selected platform.

Figure 4-1 *Basic Lab Topology*

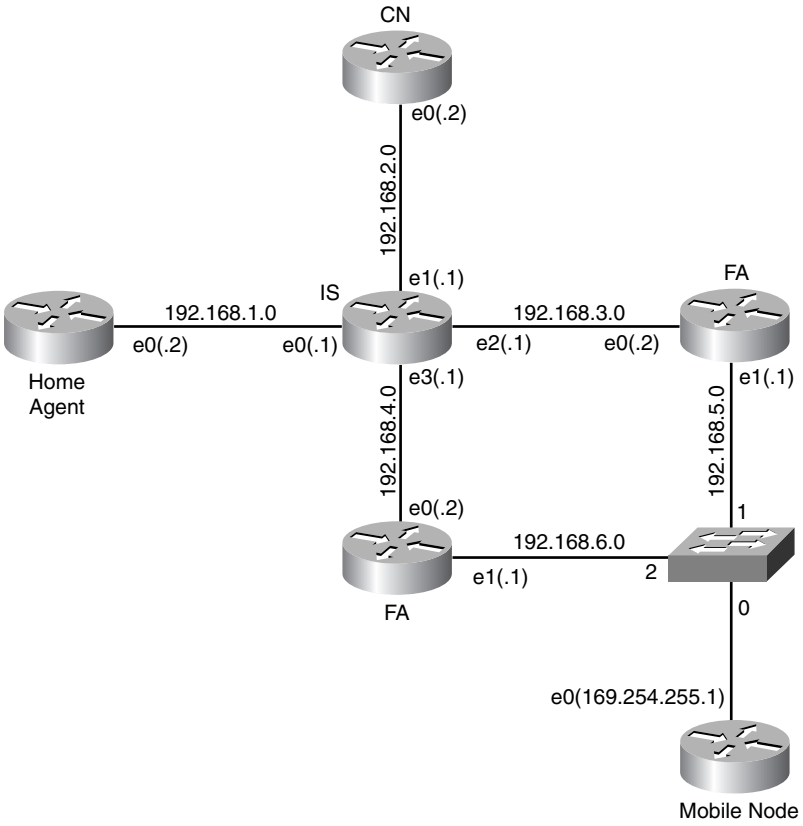


Table 4-1 *Required IOS Software Versions*

Device	Software Version*
Home Agent	IOS Release 12.0(1)T or higher
FAs	IOS Release 12.0(1)T or higher
Mobile Node	IOS Release 12.2(4)T or higher
CN	Any IOS version
IS	Any IOS version with OSPF

*If possible, IOS Release 12.3 or higher should be used in the Mobility Agents—Home Agents and FAs—so that all the features covered in this book are available.

Note that the Mobile Node in this topology is a "mobile router" (see Chapter 7, "Metro Mobility: Cisco Mobile Networks"). Although the mobile router is covered later in this book, it is used in this example to provide a complete solution that is independent of a specific Mobile Node client. The mobile router has essentially the same basic configuration attributes as a simple Mobile Node and thus provides not only a Mobile Node example but also a mobile router example for later reference.

Intermediate System Configuration

The IS shows the interaction between Mobile IP and traditional routing protocols and, as such, has no Mobile IP–specific configuration. However, inclusion of the ISs more accurately models real-world scenarios and allows better understanding of a Mobile IP deployment. In Example 4-1, each interface is assigned an IP address, and the Open Shortest Path First (OSPF) routing protocol is configured for all interfaces.

Example 4-1 *Intermediate System Final Configuration*

```
hostname IS
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet2/0
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet3/0
 ip address 192.168.4.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 1
!
end
```

Correspondent Node Configuration

The CN is used as a peer for traffic from the Mobile Node. Many Mobile IP labs are built without a CN and IS; while this allows basic functionality testing, it does not demonstrate real-world behavior. The use of a CN demonstrates the routing infrastructure as well as the Mobile IP infrastructure, and the interaction of the two. The CN needs only to be configured with an IP address on the interface. Although the CN is a router in Example 4-2, it could easily be replaced with a computer.

Example 4-2 *CN Final Configuration*

```
hostname CN
!
interface Ethernet0/0
 ip address 192.168.2.2 255.255.255.0
!
end
```

Home Agent Configuration

Home Agent configurations entail the following three basic tasks:

- Enabling the Home Agent
- Configuring the home networks
- Configuring the Mobile Nodes that are supported by the Home Agent

We will step through the three tasks and introduce the IOS configuration commands that are needed on the router. The configuration shown in this section demonstrates the base configuration of the Home Agent. Later chapters introduce more features, but keep in mind that you should always keep the configurations as short as possible and enable only the necessary features.

The foremost task is to simply enable the Mobile IP functionality. Note that regardless of which Mobile IP entity the router is functioning as, the Mobile IP routing process needs to be configured as follows:

```
router mobile
```

When the Mobile IP process is running, one or more Mobility Agents can be enabled. To configure this router as a Home Agent, use the following command:

```
ip mobile home-agent
```

The next step is to configure the home networks and Mobile Nodes that are to be supported by the Home Agent. IOS Mobile IP supports two types of home networks, physical home networks and virtual home networks. Each Mobile Node that is supported by a Home Agent must reside on one of these types of home networks.

Physical Home Network Configuration

When a Home Agent supports physical home networks, it allows Mobile Nodes to attach directly to their home network. The physical home networks are defined on a Home Agent's physical interface. When a Mobile Node is attached to its home network, all Mobile IP functionality is inactive for that Mobile Node, and normal IP routing delivers traffic. When the Mobile Node is not attached to the home network, the Home Agent uses proxy Address Resolution Protocol (ARP) to divert traffic to the Mobile Node in its current location. Route propagation for a physical home network is handled directly by interior routing protocols, just as it would be for an interface with no Mobile Nodes. To use a physical home network, simply assign the interface an IP address and ensure that it is not shut down.

NOTE When using physical home networks, if the interface is down, Mobile Nodes cannot register with the Home Agent.

Virtual Home Network Configuration

A Home Agent also supports Mobile Nodes that reside on a virtual home network. Virtual home networks are similar to loopback interfaces, but they are Mobile IP specific. Similar to a loopback interface, a virtual network is always up and not susceptible to physical failures, thereby ensuring higher availability. Virtual networks only support nodes that never physically come home. Virtual networks are expressed as a network number and mask. To define a new virtual network on the Home Agent, use the following configuration command with *address* as the network number and *mask* as the network mask:

```
ip mobile virtual-network address mask
```

Unlike physical interfaces, however, routing information about virtual networks can only be originated by the Home Agent when mobile routes are redistributed into the interior gateway protocol. Redistribution of Mobile IP routes only redistributes the virtual networks; it does not redistribute the individual host routes that reach the Mobile Nodes. The section "Examining the Routing Table," later in this chapter, shows how Mobile IP routes appear in the routing table and how redistribution works.

NOTE Redistribution allows routes from one routing domain to be translated and injected into another routing domain. Use care when redistributing routes to maintain a functional routing topology.

Specific configuration of redistribution varies from protocol to protocol, but generally, it should be configured on the Home Agent as follows:

```
redistribute mobile
```

The next step is to configure Mobile Nodes to reside on a particular home network.

Mobile Host Configuration

The essence of a Home Agent configuration centers around configuring the Mobile Nodes that it supports and appears on one or more lines beginning with the **ip mobile host** command. This command defines which Mobile Nodes are allowed to register, which services they are allowed to use, and how to authenticate them. (The security association itself is configured separately, as described in the next section of this chapter.) The **ip mobile host** command requires a Mobile Node or group of Mobile Nodes to be defined and associated with a home network.

In the following example command, we consider a simple case—defining a range of Mobile Nodes identified by their home address (192.168.100.10 through 192.168.100.20) and associating them with a virtual network (192.168.100.0 with mask 255.255.255.0):

```
ip mobile host 192.168.100.10 192.168.100.20 virtual-network 192.168.100.0
  255.255.255.0
```

The Home Agent also needs to be configured with the Mobile-Home security association for each Mobile Node. The security association can be configured either in a AAA server or on the command line, as described in the examples of the next section.

Security Association Configuration

The security association between the Home Agent and a Mobile Node is mandatory; it is also the only one used in this chapter. A security context is configured on the Home Agent one per line, and each line is usually associated with one Mobile Node. (Remember a security association is made up of one or more security contexts.) In some cases, several Mobile Nodes can share the same security key, but this is generally not recommended. At a minimum, one Mobile Node-Home Agent (MN-HA) security context is configured for each mobile host entry, but the standard allows for far more. If multiple security contexts, which are differentiated by using different security parameter index (SPI) values, are configured for a single mobile host, the IOS mobile router implementation will round-robin through all keys. In this case, each Registration Request (RRQ) uses a different security context going from the lowest to the highest SPI value and then starting over again. The Home Agent always uses the same security context that was used in the RRQ by the Mobile Node when the Mobile Node sends a Registration Reply (RRP).

NOTE Configuration of security associations for IOS Mobile IP is always done from the perspective of the agent that is to use that security association. For example, the **ip mobile secure foreign-agent…** command configures an Home Agent-FA security association on the Home Agent. If the same command were configured on the Mobile Node, it would imply an MN-FA security association.

In the case of a router serving as both a Home Agent and FA, the configuration of keys for Mobile Nodes is slightly different. Specifically, you must be able to differentiate the Mobile Node-Foreign Agent (MN-FA) and MN-HA keys in this hybrid case. Because IOS uses the **host** command to refer to the Mobile Node in Home Agent configurations and the **visitor** command to refer to the Mobile Node in FA configurations, the same is done for security associations. Thus, the **ip mobile secure host** command configures the Home Agent-Mobile Node (HA-MN) security association, while the **ip mobile secure visitor** command configures the FA-MN security association.

As with all security context, the HA-MN security context must be indexed with an SPI. The SPI in IOS is specified as a hexadecimal value. Finally, the key, algorithm, and mode must be specified. You can specify keys as an ASCII value or a hexadecimal value. To avoid errors, hexadecimal keys are recommended because the use of ASCII keys is not standardized. A complete HA-MN security association is as follows:

```
ip mobile secure host 192.168.100.10 spi 100 key hex
  1234567890abcdef1234567890abcdef algorithm hmac-md5
```

Home Agent Final Configuration

Example 4-3 shows the final configuration of a router serving as a Home Agent. The Home Agent supports Mobile Nodes (192.168.100.10 through 192.168.100.20) residing on virtual network 192.168.100.0. The only Mobile Node configured with a security association is 192.168.100.10, and thus, it is the only Mobile Node allowed to register and roam.

Example 4-3 *Home Agent Final Configuration*

```
hostname HA
!
interface Ethernet0/0
 ip address 192.168.1.2 255.255.255.0
!
router mobile
!
router ospf 1
 redistribute mobile subnets
 network 192.168.0.0 0.0.255.255 area 1
!
ip mobile home-agent
ip mobile virtual-network 192.168.100.0 255.255.255.0
ip mobile host 192.168.100.10 192.168.100.20 virtual-network 192.168.100.0
  255.255.255.0
ip mobile secure host 192.168.100.10 spi 100 key hex
  1234567890abcdef1234567890abcdef algorithm hmac-md5
!
end
```

Foreign Agent Configuration

The FA configuration used in this lab is simple and represents the most common implementation. Complex FA configurations are typically only used in mobile Internet service provider deployments of Mobile IP. A basic FA configuration requires the definition of the Care-of Address (CoA) and activation of roaming interfaces.

Recall that for any Mobile IP entity, the IOS Mobile IP process must be started before any Mobile IP commands can be accepted on the router. Again, this is accomplished with the **router mobile** command.

FA functionality is enabled with a single global statement that also specifies the interface to be used as the CoA. In the following example command, Ethernet interface 1/0 is configured with FA functionality:

```
ip mobile foreign-agent care-of Ethernet1/0
```

When the FA service has been enabled on the router, each interface that can accept Mobile Nodes needs to be configured. The interface-level command is as follows:

```
ip mobile foreign-service
```

Finally, because Mobile IP agent advertisements are part of Internet Control Message Protocol (ICMP) Router Discovery Protocol (IRDP) advertisements, IRDP must be configured. The default timers for IRDP are long and do not facilitate timely handovers unless solicitation is used. In Example 4-4, the timers have been lowered because no link state triggers exist. Three relevant values exist for IRDP configuration: **maxadvertinterval**, **minadvertinterval**, and **holdtime**. If the *min* and *max* values are used together, a random value in between the two is generated for each advertisement. The holdtime should typically be three times the maximum to ensure that the agent is truly gone and not just experiencing a brief packet loss. Configuration values for IRDP timers are in seconds. Note that the advertisement timers can also be adjusted on the Home Agent with similar IRDP commands. Unless specified through configuration commands, the default IRDP values are a maximum interval of 5 minutes and a holdtime of 15 minutes.

Examples 4-4 and 4-5 show the configuration of routers serving as FAs. In Example 4-4, the FA allows Mobile Nodes to roam on interface E1/0 with FA–Care-of Agent (FA-CoA) 192.168.5.1. In Example 4-5, the FA allows Mobile Nodes to roam on interface E1/0 with FA-CoA 192.168.6.1. In both examples, the IRDP agent advertisement timers are adjusted.

Example 4-4 *FA1 Final Configuration*

```
hostname FA1
!
interface Ethernet0/0
 ip address 192.168.3.2 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.5.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 9
 ip mobile foreign-service
!
router mobile
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 1
!
ip mobile foreign-agent care-of Ethernet1/0
!
end
```

Example 4-5 *FA2 Final Configuration*

```
hostname FA2
!
interface Ethernet0/0
 ip address 192.168.4.2 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.6.1 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 9
 ip mobile foreign-service
router mobile
!
router ospf 1
 log-adjacency-changes
 network 192.168.0.0 0.0.255.255 area 1
ip mobile foreign-agent care-of Ethernet1/0
!
end
```

Mobile Node Configuration

In this chapter, the Mobile Node is an IOS router running the IOS Mobile Networks feature. For this example, only a small subset of the IOS Mobile Networks features is used; full coverage is available in Chapter 7. The Mobile IP client used in IOS Mobile Networks is built on the same standard as a Mobile IP client for a PC or personal digital assistant (PDA) and, thus, requires all the same basic configura-tion attributes. In general, each Mobile Node must be configured with its identification, Home Agent's IP address, and a security association shared with the Home Agent.

IOS Mobile Networks uses a static home address for identification that needs to be configured on an interface before it can be used by the Mobile IP client. You should configure the home address on a loopback interface so that the home address is always up. The home address is a host address and, as such, needs to be configured with a /32 mask. (If the loopback does not have a host mask, traffic for other nodes on the Mobile Node's home network cannot follow the default route, but is routed to the loopback and get dropped.)

The real mask of the home network is configured with the **ip mobile router address** command. One or more physical interfaces need to be specifically configured as roaming interfaces. These interfaces also must be configured with an IP address to enable IP traffic on that interface. Note that the IP address does not need to be valid and routable. Addresses are commonly used from the autoconf space, but you can pick any IP address.

As with all Mobile IP entities, the **router mobile** command is required to enable the Mobile IP process on the mobile router. After enabling Mobile IP, the Mobile IP client configuration is invoked with the **ip mobile router** command, setting the router in mobile router configuration mode. In this mode, the home address and home network subnet mask are configured with the

address subcommand, and the Home Agent address is configured with the **home-agent** subcommand, as shown in the following example:

```
router mobile
ip mobile router
 address 192.168.100.10 255.255.255.0
 home-agent 192.168.1.2
```

Finally, the mandatory security association with the Home Agent needs to be configured. This security association needs to *exactly match the one configured on the Home Agent, as follows:*

```
ip mobile secure home-agent 192.168.1.2 spi 100 key hex
  1234567890abcdef1234567890abcdef algorithm hmac-md5
```

Recall that the security association is configured from the perspective of the Mobile IP entity on which the command is invoked, that is, this line is configuring the MN-HA security association.

Example 4-6 shows a mobile router configuration with a home address of 192.168.100.10 and a Home Agent address of 192.168.1.2. Note that the home address is configured on the loopback interface, and interface E0/0 is configured as the roaming interface.

Example 4-6 *Mobile Node Final Configuration*

```
hostname MN
!
interface Loopback0
 ip address 192.168.100.10 255.255.255.255
!
interface Ethernet0/0
 ip address 169.254.255.1 255.255.255.0
 ip mobile router-service roam
!
router mobile
!
ip mobile secure home-agent 192.168.1.2 spi 100 key hex
  1234567890abcdef1234567890abcdef algorithm hmac-md5
!
ip mobile router
 address 192.168.100.10 255.255.255.0
 home-agent 192.168.1.2
!
end
```

Operation and Evaluation/Troubleshooting

In the lab environment, roaming is simulated by toggling the FA to which the mobile router's roaming interface is connected. This is typically done by assigning different virtual LAN (VLAN) numbers to each FA and changing the VLAN assignment for the roaming interface on the mobile router. After the mobile router's roaming interface is connected to a FA at Layer 2, the mobile router should automatically register with the Home Agent through the FA.

The different mobility entities can be probed to assess proper functioning of the Mobile IP process.

Home Agent

Even though Mobile IP is an edge-intelligent routing protocol (that is, all routing decisions are made by the Mobile Node), a network administrator often does not have access to the Mobile Node for troubleshooting. Because the Home Agent is the anchor point in the network, it is a logical starting point for evaluation. The first checklist task at the Home Agent is to verify that the Mobile Node indeed has a mobility binding using the **show ip mobile binding** command. If no binding exists for the Mobile Node, the **show ip mobile host** command can provide information about any previous failed registration attempts.

Example 4-7 shows the output if the security association on the Mobile Node (192.168.100.10) did not match the one configured on the Home Agent. The output of the **show ip mobile host** command displays the failure as "Last code," which in this example is a failed authentication. The output also shows when the Home Agent last accepted a registration from the Mobile Node, and when the registration was last denied. In this example, the Mobile Node had four failed registration attempts, and had never successfully registered with the Home Agent.

Example 4-7 **show ip mobile host** *Command*

```
HA#show ip mobile binding 192.168.100.10
Mobility Binding List:
HA#show ip mobile host 192.168.100.10
Mobile Host List:

192.168.100.10:
    Allowed lifetime 10:00:00 (36000/default)
    Roam status -Unregistered-, Home link on virtual network 192.168.100.0 /24
    Accepted 0, Last time -never-
    Overall service time 00:00:21
    Denied 4, Last time 07/24/03 13:43:29
    Last code 'MN failed authentication (131)'
    Total violations 4
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
HA#
```

Using the information learned through troubleshooting, the Mobile Node configuration can be corrected to send a proper RRQ message to the Home Agent. Upon successful authentication and validation of the RRQ, a mobility binding is established on the Home Agent, as shown in Example 4-8. A valid binding, however, might not indicate that everything is functioning correctly. Thus, you should also verify that the last accepted registration is more recent than the last denied registration using the **show ip mobile host** command.

Example 4-8 *Valid Mobility Binding*

```
HA#show ip mobile binding 192.168.100.10
Mobility Binding List:
192.168.100.10:
    Care-of Addr 192.168.6.1, Src Addr 192.168.4.2
    Lifetime granted 10:00:00 (36000), remaining 09:59:52
    Flags sbdmg-t-, Identification C2CA6BA8.4489393C
    Tunnel0 src 192.168.1.2 dest 192.168.6.1 reverse-allowed
    Routing Options -
HA#
```

Mobile Node

After looking at the Home Agent, the next best place to troubleshoot is at the Mobile Node. (The FA is often reserved for last, because the only deterministic way to identify the active FA is to look at the CoA that the Mobile Node is using.) Each Mobile IP client offers a different set of tools for troubleshooting, but the basic premise is the same as those available in IOS. Follow these troubleshooting steps:

1. Ensure that the Mobile Node has received agent advertisements from one or more FAs.
2. Determine which FA the Mobile Node has selected and whether the registrations are indeed accepted by the foreign and Home Agents. Also, the registration might be accepted, but the reply is dropped by the network.
3. Determine whether and how data traffic is flowing.

Example 4-9 shows the output of the **show ip mobile router agent** command, which lists all currently valid agent advertisements. Because this mobile router is only seeing one FA, you can easily determine which FA is being used. Note that most clients have some method of indicating which FA is being used. This is useful when proceeding to the FA for further troubleshooting. If no FAs have been heard, it is likely a physical layer problem or a FA configuration problem.

Example 4-9 *Current Agent Advertisements*

```
MN#show ip mobile router agent

Mobile Router Agents:

Foreign agent 192.168.5.1:
    Care-of address 192.168.5.1
    Interface Ethernet0/0, MAC aabb.cc00.6801
    Agent advertisement seq 30828, Flags rbhFmG-t, Lifetime 36000
    IRDP advertisement lifetime 9, Remaining 6
    Last received 07/20/03 19:49:07
    First heard 07/19/03 18:11:37
```

When you have determined that the Mobile Node has a valid FA, the next step is to look at the registration status. Example 4-10 shows the output of the **show ip mobile router** command. In

the Monitor section of the output, the status of the registration is displayed, along with the current FA and CoA.

Example 4-10 *Registration Status*

```
MN>show ip mobile router

Mobile Router
    Enabled 07/20/03 15:00:42
    Last redundancy state transition NEVER

Configuration:
    Home Address 192.168.100.10 Mask 255.255.255.0
    Home Agent 192.168.1.2 Priority 100 (best) (current)
    Registration lifetime 65534 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 120, Retry 3, Interval 10

Monitor:
    Status -Registered-
    Active foreign agent 192.168.6.1, Care-of 192.168.6.1
    On interface Ethernet0/0
    Tunnel0
```

Finally, if the registration looks good and matches what the Home Agent has for the registration, you likely have a data plane problem. Check the interface counters and verify that traffic is coming into an out of the Mobile Node. You often find outbound traffic, but no inbound traffic. In this case, you likely have a problem with the tunneling. A number of common tunneling problems and solutions are covered in Chapter 6, "Metro Mobility: Client-Based Mobile IP," and Chapter 8, "Deployment Scalability and Management."

FA

The FA stores the state of active Mobile Nodes in the visitor table. The output of the **show ip mobile visitor** command, shown in Example 4-11, is similar to the output of the **show ip mobile binding** command on the Home Agent. However, visitor entries in the FA can be misleading for troubleshooting. Entries are not flushed from the visitor table until the lifetime expires, so a Mobile Node could have briefly visited the FA, but the visitor entry can remain for many hours if the lifetime is long. Note that using the Registration Revocation mechanism, described in Chapter 6, alleviates this problem.

Example 4-11 *FA Visitor Table Entry*

```
FA1#show ip mobile visitor
Mobile Visitor List:
Total 1
192.168.100.10:
    Interface Ethernet1/0, MAC addr aabb.cc00.6a00
    IP src 192.168.100.10, dest 192.168.5.1, UDP src port 434
    HA addr 192.168.1.2, Identification C2EDFF2A.72710D54
    Lifetime 10:00:00 (36000) Remaining 08:16:14
    Tunnel0 src 192.168.5.1, dest 192.168.1.2, reverse-allowed
    Routing Options -
```

Mobile Nodes that have not successfully completed registration are kept in the pending visitor table, which is visible with the show ip mobile visitor pending command. If communication problems exist between the FA and Home Agent, several entries are often in the pending table. However, in most cases, entries do not stay in the pending table long enough to be visible.

Examining the Routing Table

You should also understand what the routing table will look like. All routes controlled by Mobile IP are marked with an *M* in the routing table. The Home Agent has two kinds of Mobile IP routes in its routing table, home networks and Mobile Nodes. If a home network is configured as a virtual network, it appears in the routing table as an M route; otherwise, it appears as a connected route. For each Mobile Node that has an active binding, you also find a host route in the routing table. As shown in Example 4-12, the Mobile Node route shows the tunnel that is being used as the next hop.

Example 4-12 *Routing Table on the Home Agent*

```
HA#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B – BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.4.0/24 [110/20] via 192.168.1.1, 01:52:00, Ethernet0/0
O    192.168.5.0/24 [110/30] via 192.168.1.1, 01:52:00, Ethernet0/0
O    192.168.6.0/24 [110/30] via 192.168.1.1, 01:52:00, Ethernet0/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
O    192.168.2.0/24 [110/20] via 192.168.1.1, 01:52:00, Ethernet0/0
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
M       192.168.100.10/32 [3/1] via 192.168.6.1, 01:51:55, Tunnel0
M       192.168.100.0/24 is directly connected
O    192.168.3.0/24 [110/20] via 192.168.1.1, 01:52:00, Ethernet0/0
```

Example 4-13 looks at the routing table of the IS. The point of including the IS in the topology explored in this chapter is to show that only the home network route is redistributed. In Example 4-13, the virtual network appears as a Type 2 external OSPF route.

NOTE The individual host routes for the Mobile Nodes are not redistributed. Isolation of the network from the host routes is a key feature of Mobile IP.

Example 4-13 *Routing Table on the IS*

```
IS>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Ethernet3/0
O    192.168.5.0/24 [110/20] via 192.168.3.2, 01:58:45, Ethernet2/0
O    192.168.6.0/24 [110/20] via 192.168.4.2, 01:58:45, Ethernet3/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
C    192.168.2.0/24 is directly connected, Ethernet1/0
O E2 192.168.100.0/24 [110/20] via 192.168.1.2, 01:58:45, Ethernet0/0
C    192.168.3.0/24 is directly connected, Ethernet2/0
```

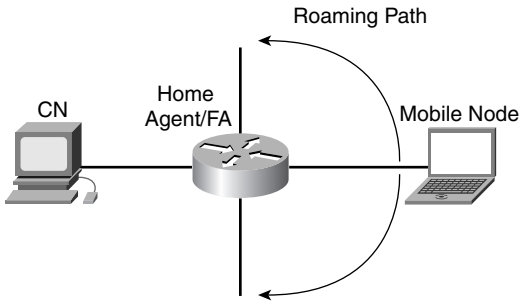
Alternative Topologies

While the topology presented in the previous sections is ideal for learning Mobile IP in the lab, it requires a significant number of routers and is beyond the facilities of many small labs. The following topologies present several methods for integrating different Mobile IP components.

Single-Router Topology

At the opposite end of the spectrum from the topology shown in Figure 4-1, Figure 4-2 demonstrates a lab scenario using only a single-router topology. Coupled with a pair of computers—one acting as a Mobile Node and the other acting as a CN—this solution has most of the capabilities but is more complex to understand because all the functions are integrated. One key behavior about this configuration is that IOS Mobile IP does not use tunneling when the Home Agent and FA are on the same router. Instead, the forwarding entries are updated based on the interface to which the Mobile Node is attached.

Figure 4-2 *Single-Router Test Topology*



Other Options for Single-Router Topology

In between these two topologies are a number of other options. Eliminating the IS and replacing the CN with a computer are good options that can have minimal impact on the testing. Without the IS, it will not be clear how the redistribution works, but Mobile IP still functions the same. You can also combine the two FAs into one FA with two interfaces, but it will not be clear when the Mobile Node changes links, because the CoA does not change using the configuration in Example 4-4. To ensure that a CoA change is seen, each interface where the Mobile Node attaches needs to be configured as a CoA and the **interface-only** option should be used. Normally with two CoAes configured, the FA would advertise both addresses out both interfaces. However, with the **interface-only** command, only the address of the physical interface is advertised.

Summary

This chapter presented a pedantic Mobile IP example as a learning tool and highlighted the major concepts of IOS Mobile IP configuration in a simple lab topology. We introduced IOS configuration commands and looked at basic configuration of the Home Agent, FA, and Mobile Node. We considered common troubleshooting areas on the different Mobile IP entities, and we showed how to evaluate the proper functioning of the Mobile IP process.

The remaining chapters build on the basic understanding of the protocol from Chapters 2 and 3—and the hands-on configuration in this chapter—to help build real-world solutions. Applying Mobile IP to real-world deployments enables a good understanding of the benefits and implications of Mobile IP. The solutions are broken down by the size of the roaming area and the client options.

Review Questions

1. Draw a basic Mobile IP topology.
2. Which command enables the Mobile IP process on a router?
3. What are virtual networks and why are they used?
4. Give an example of a basic Home Agent configuration with the following features: Home Agent address 192.168.1.2, virtual network 192.168.100.0/24, and Mobile Node 192.168.100.10 residing on the virtual network. Don't forget to include the Mobile-Home security association.
5. Give an example of a FA configuration with the following features: FA address 192.168.3.2 and CoA 192.168.5.1 on Ethernet 1/0.
6. Give an example of an IOS Mobile Networks configuration with Home Agent 192.168.1.2 and Home Address 169.254.255.1.
7. A router can serve as a Home Agent and FA at the same time.
   a. True
   b. False
8. Configuration of security associations for IOS Mobile IP is always done from the perspective of the agent that is to use that security association.
   a. True
   b. False
9. List two commands that are useful for troubleshooting on the Home Agent.
10. Name a command that is useful for troubleshooting on the FA.