CHAPTER 7

Static and Dynamic Collocated Care-of Address

A collocated care-of address (CCoA) terminates the tunnel from a home agent to a mobile device. This is in contrast to a care-of address (CoA), where a foreign agent is registered to a home agent, and the mobile device registers with the foreign agent. This allows the mobile device to roam to foreign networks where foreign agents are not deployed or where foreign agents are present, but foreign agent functionality is not available.

On the mobile access router, the IP address of the interface configured for roaming is also the CCoA address. This address can be a fixed IP address (Static CCoA), or it can be dynamically acquired (Dynamic CCoA) by using Point-to-Point Protocol (PPP)/IP Control Protocol (IPCP) or DHCP.

A Static CCoA is used where the mobile access router roaming interface IP address remains fixed, for example in Cellular Digital Packet Data (CDPD) wireless network. A Dynamic CCoA is used where the interface is configured to acquire its IP address by using DHCP and it is in **no shut** mode.

When mobile access router roams into a foreign network, first attempts to discover foreign agents. If the mobile access router discovers a foreign agent, the mobile access router with CoA configured attempts to register with the foreign agent. It sends a registration request (using an advertised CoA) to a foreign agent. The foreign agent relays the request to the home agent. The home agent process it and sends a reply to the foreign agent. The foreign agent relays the reply to mobile access router. The routing path between the home agent and the foreign agent (CoA) is set up after successful registration.

If it does not find a foreign agent, a mobile access router gets an address in the foreign network and sends a registration request directly to the home agent, using the address assigned to the mobile access router by the foreign network as the CCoA. The home agent process the request and sends a reply to the mobile access router. The routing path between the home agent and the mobile access router CCoA interface is set up after successful registration.

When the mobile access router detects that it is at home, it sends a deregistration request to its home agent.

The following events trigger a registration:

- A foreign agent advertisement is received, and the mobile access router has a reason to register.
- An active foreign agent advertisement (IRDP lifetime) expired, and the mobile access router chooses to register with another foreign agent.
- The registration timer expired due to the retransmission or lifetime aging.
- Recovery from the home agent that replied with a denial of service due to a mismatched ID.
- Recovery from a foreign agent, that replied with a denial of service as the result of a lower lifetime.
- After configuration (if the mobile access router has been configured for roaming and has a reason to register with a foreign agent).

A mobile access router might register with a foreign agent or a home agent for the following reasons:

- Movement is detected.
- A foreign agent reboot is detected.
- The mobile access router is isolated.
- A better interface on a reliable foreign agent is discovered.
- The mobile access router roams to on foreign network without an active foreign agent.
- The mobile access router roams on its home network when it has active foreign agent.

When a registration reply is received, the mobile access router processes it as if the reply message address equals the mobile access router interface IP address. The mobile access router finds the request in the registration table that corresponds to the reply. It authenticates the reply and sets a routing path between the mobile access router and the home agent. Also, it creates a default route through the foreign network.

Enabling CCoA

The **ip mobile router-service collocated** command configures the interface for CCoA. The interface must first be configured as a roaming interface by using the **ip mobile router-service roam** command; otherwise, an error message is displayed.

If the mobile access router is unable to register, it waits a default number of seconds and tries again. The default wait time is 60 seconds, can be configured by using an interface configuration command.

Default Gateway

If you change from a static IP address to DHCP address acquisition on a roaming interface, the static gateway address is not needed for CCoA. Instead, a default router address is obtained from DHCP when the IP address is acquired and the default router address is used as the CCoA gateway address. The gateway address is reset to 0.0.0.0 and the *gateway* keyword is no longer available on the CCoA command line.

When the interface acquires an IP address, the DHCP default router address is used as the CCoA gateway. In the opposite case, if a DHCP address configuration is changed from a DHCP-acquired IP address to a static IP address, the CCoA gateway address is set to 0.0.0.0 and you are warned that no CCoA default gateway is configured.

When a mobile access router is configured with a static IP address, the default gateway must be provided in the configuration by using the **ip mobile router-service collocated** command. This gateway address must be on the same network as the interface configured for static CCoA. The mobile access router uses this address as the next hop destination for Mobile IP Registration Request (RRQ)s, Upon receiving a successful Mobile IP Registration Reply (RRP), the mobile access router uses this address for the mobile access router default route and gateway.

CCoA Registration

When registering with its CCoA, the mobile access router sets decapsulation by the mobile node in the RRQ and uses the CCoA as the RRQ source address. The RRQ requests Generic Routing Encapsulation (GRE) tunneling if configured to do so. The RRQ is sent directly to the home agent. If, after the initial registration retries, the mobile access router has not successfully registered, it waits a set number of seconds and tries again. The default wait time is 60 seconds and can be configured by using the **ip mobile router-service collocated registration retry** interface command.

When the router is booted or when it is configured for roaming, an interface configured for dynamic CCoA attempts to find foreign agents on the link by soliciting and listening for agent advertisements. If a foreign agent is found, the mobile access router registers with the advertised CoA. If a foreign agent is not found, the mobile access router registers with the CCoA.

A roaming interface that has discovered (and possibly registered with) a foreign agent can be made to immediately register a static or dynamic CCoA by using the **ip mobile router-serv collocated ccoa-only** command.

The foreign agent registration remains if you configure the interface by using the **ip mobile router-serv collocated** command. This command permits a roaming interface to discover foreign agents when the interface first comes up. If foreign agents are discovered, CCoA registration remains disabled unless the **ip mobile router-serv collocated ccoa-only** command is invoked. If a foreign agent is not discovered, CCoA registration is automatically enabled.

An interface configured for both foreign agent CoA and CCoA registration always prefers foreign agent CoA registration. When foreign agent advertisements are heard, the interface registers the foreign agent CoA, even if it has registered a CCoA. Otherwise, when a CCoA is present or acquired, it is registered.

To facilitate faster roaming, the interface registers a foreign agent CoA when an advertisement is heard or it registers a CCoA when an address is acquired, depending on which event occurs first. (Previously, the router waited to hear several advertisements before registering a foreign agent CoA.)

When a DHCP interface is **no shut**, or when an interface that is **up** is first configured for DHCP, DHCP IP address acquisition (discovery) begins. Address discovery attempts are repeated at increasingly longer intervals (up to 60 seconds) until an address is acquired. During discovery the interface is IP-enabled, so IP packets can be processed in support of IRDP and MIP registration even though the interface has no IP address.

A roaming interface configured for foreign agent CoA support sends solicits immediately and, if an advertisement is heard, the interface registers a CoA through the foreign agent. If the interface is also configured for CCoA registration and no advertisements have been heard, DHCP triggers CCoA registration. If the interface is configured **ccoa-only** (ignoring foreign agents, if any) no solicits are sent when the interface comes up. When an IP address is acquired, the interface attempts to register the newly acquired CCoA.

Even if the interface registries through a foreign agent, an IP address can be acquired through DHCP, though it does not affect the foreign agent registration. A foreign agent-registered interface retains the acquired IP address, to be used for a subsequent CCoA registration.

When a linkUp trap is received on a DHCP roaming interface, one or more attempts are made to renew the current IP address. If the attempts fail, the interface attempts to acquire a new DHCP address. This is done by invoking the renew/release/discover function.

When a CCoA-registered interface ends its registration in response to a linkDown trap event, the CCoA registration retry timer is started. If no linkUp event occurs before the timer expires, the interface makes one or more attempts to renew its current DHCP IP address or it attempts to acquire a new IP address. This is also done by invoking the renew function.

Foreign-Agent Discovery

Unless configured for **ccoa-only**, a roaming interface with static IP address or DHCP address begins soliciting as soon as the interface comes up. If it has a DHCP address, solicts can be sent and advertisements heard even without an IP address having been acquired. If the interface acquired its IP address by using IPCP, the interface must acquire an IP address before it can solicit.

To support CCoA, a default gateway address is required. This address is used as the default gateway for CCoA registrations and as a default route after the interface is registered. For Static CCoA on an Ethernet interface, a default gateway address must be provided through the roaming interface CCoA configuration. For DHCP interfaces, DCCOA registration use the DHCP default router address and, once the interface is registered, the address is also used for the mobile access router default route and gateway.

When a roaming interface is configured to acquire an IP address by using PPP/IPCP and it is in no shut mode, address negotiations with a peer begin. After the interface acquires an IP address, it attempts to solicit foreign agents or to register the acquired IP address as the CCoA.

If the solicit messages end and no foreign agent advertisements have been heard, further solicit messages are disabled and advertisements from foreign agents are ignored. Advertisements from home agents are still processed to determine whether the mobile access router has returned home. Disabling CCoA again enables solicit and foreign agent advertisement processing.

CCoA Tunneling

When registered using a CCoA, the mobile access router CCoA becomes the endpoint of a tunnel from the home agent. The mobile access router de-encapsulates the packet from the home agent sent through the tunnel to the CCoA.

This home agent-to-CCoA tunnel is in addition to the home agent-to-mobile access router home address tunnel that is created on the mobile access router when registering with mobile networks. To avoid the use of two tunnels and the resulting double encapsulation, the mobile access router optimizes tunneling by creating only one of the tunnels. On the home agent side, only the home agent-to-CCoA tunnel is certain to be created, because the home agent-to-mobile access router tunnel is not created until a mobile access router's mobile networks are added to the routing table, so tunnel optimization uses only the home agent-to-CCoA tunnel.

The single home agent-to-CCoA tunnel created during registration is used to reverse tunnel packets to the home agent, if the mobile access router is configured for reverse tunneling.

Mobile Access Router Configured as a Foreign-Agent

A mobile access router might also be configured as a foreign agent. If the mobile access router is configured as a foreign agent using the CCoA as the foreign agent CoA, the mobile access router sends an agent advertisement when that CCoA changes. An advertisement is sent even if the mobile access router is not configured for periodic advertisements to notify mobile nodes on attached networks to register using the new CoA.

Movement Detection and Layer 2 Signaling

Previously, only interface up/down signals or interface IP address changes on the roaming interface could trigger mobile access router CCoA roam processing. But some roaming scenarios require other internal or external signaling to detect movement and perform timely hand-offs. For example, an Ethernet interface connected to a WLAN through an 802.11 bridge. The wireless link might go up or down, but without some kind of signalling, a mobile access router Ethernet interface is not aware of the change. A mobile access router foreign agent CoA interface must wait until the foreign agent advertisement holdtime expires. In a CCoA-only scenario, the mobile access router would receive no indication that the status of the interface is changed.

The Wireless Mobile Interface Card (WMIC) connects to the mobile access router thought the Fast Ethernet interfaces. The 802.11 Layer 2 transitions (associations and disassociations) that take place on the WMIC are signaled by using SNMP messaging, specifically the Interface MIB linkUp and linkDown traps are sent to the mobile access router Ethernet or VLAN interface.

Mobile Access Router SNMP Message Processing

The mobile access router interface must be configured for roaming (foreign agent CoA registration by default) and if desired, CCoA registration. The mobile access router must also be configured to receive SNMP trap messages. The SNMP process receives the traps and invokes a registry permitting the mobile access router to examine the trap information. The mobile access router determines:

- If the trap was received on a roaming interface
- If the trap is a linkUp or linkDown event, ignoring others
- If the trap is from the Dot11Radio0 interface
- If this is a linkDown trap, examine the locIfReason information, processing only **down** or **administratively down** traps

DHCP and mobile access router processing occurs each time a valid linkUp trap or linkDown trap is received, even if the previous trap received was also linkUp. The mobile access router keeps no history of traps.

linkUp Trap Processing

When a linkUp trap event occurs, the DHCP client must either renew the current IP address or acquire a new IP address as quickly as possible. If a DHCP interface is without an IP address, address acquisition (Discover) is started.

The **ip dhcp client mobile renew count** <*num*> **interval** <*msec*> command permits you to configure the number of renew attempts and the interval between attempts when DHCP Renew is invoked. The configured values override any values passed by the DHCP Renew caller.

If IP address Discovery has started and it is between attempts (waiting for the next retry), address discovery immediately begins again.

If the interface already has a DHCP-acquired IP address, the mobile access router does not know if it is on the same subnet as before, so the mobile access router attempts to renew the current address. This reduces DHCP messaging if the mobile access router is reassociated to the same subnet. If a DHCP NACK message is received from a DHCP server on another subnet, or no DHCP ACK is received, the interface releases the current IP address and uses Discover to acquire a new IP address.

When a linkUp trap is received on a roaming interface, the event is handled as if the roaming interface just came up. For example, solicits are sent if appropriate and the mobile access router determines if this interface, compared to other roaming interfaces, should register. Dynamic address acquisition can trigger DCCoA registration.

Subsequent linkUp traps are processed the same way. However, if the interface is already registered, and nothing else has changed that affects the registration decision, the router does not attempt a new registration.

linkDown Trap Processing

The interface keeps any DHCP-acquired IP address. Receipt of a valid linkDown trap starts a reassociation hold-down timer. This timer is configurable timer with a range of 0-5000 ms. The default is 1000 ms.

This hold-down period delays the response to the trap, typically an attempt to register using the next best mobile access router interface, until the WMIC bridge has had time to reassociate on a new subnet. The timer value should reflect the worst case time expected to reassociate in a particular environment. The mobile access router remains registered during this hold-down period and foreign agent data is retained.

If a linkUp trap arrives before the hold-down timer expires, the mobile access router remains registered and foreign agent data is retained. Solicits are sent to find foreign agents and the DHCP IP address renewal and discovery process begins.

If the hold-down timer expires or the hold-down delay was 0, mobile access router processing proceeds as if the interface just went down. Any foreign agents heard on this interface are deleted from the foreign agent list and, if registered on the interface, the mobile access router deletes the current registration and tries to register by using the next best roaming interface. Solicits are sent to find foreign agents and the DHCP IP address renewal begins.

If a linkUp trap does not arrive after a linkDown event has been processed, the mobile access router may register by using a another lower priority interface. Even without a linkUp trap, a foreign agent advertisement triggers foreign agent registration again and DHCP address acquisition triggers a CCoA registration.

Example Configurations

This section provides CCoA and DHCP configuration examples.

SNMP Trap Configuration Example

SNMP linkup trap and linkdown trap are used for Layer 2 signaling on a roaming interface in DCCoA environment. Whenever the WMIC is associates or disassociates, a SNMP trap is sent to the router and the DCCoA roaming interface is notified.

WMIC

```
arp 85.85.85.1 000b.4681.0d40 ARPA BVI1
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 85.85.85.1 version 2c l2sig
```

Note 85.85.85.1 is the loopback IP address of the router. 000b.4681.0d40 is the MAC address of the F0/0 interface on the router (assuming that the WMIC F0 interface is connect to router F0/0 interface).

Mobile Access Router

```
    snmp-server manager
!
```

CCoA Configuration Example

The following is an example of the mobile access router configuration for CCoA:

Static CCoA

```
interface Serial1/0
    ip address 11.0.0.1 255.255.255.0
    ip mobile router-service roam
    ip mobile router-service collocated
```

Dynamic CCoA using PPP/IPCP

```
interface Serial2/0
    ip address negotiated
    encapsulation ppp
    ip mobile router-service roam
    ip mobile router-service collocated
```

Mobile Access Router

```
ip mobile secure home-agent 43.0.0.3 spi 100 key hex 11223344556677881122334455667788
ip mobile router
    address 20.0.4.1 255.255.255.0
    home-agent 43.0.0.3
```

Workgroup Bridge Example Configuration

The following example show a workgroup bridge configured to use SNMPv2 link traps:

Workgroup Bridge (WMIC)

```
arp 85.85.85.1 0000.abcd.1111 ARPA BVI1
snmp-server trap-source Dot11Radio0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 85.85.85.1 version 2c l2sig
```

Mobile Access Router

```
interface Loopback0
ip address 85.85.85.1 255.255.0.0
!
snmp-server community public RO
snmp-server enable traps ttyy
```

The following example shows a DHCP and SNMPv3 configuration example for DCCoA.

Mobile Access Router

```
interface FastEthernet0
    ip dhcp client mobile renew count 3 interval 20
    ip address dhcp
    ip mobile router-service roam
    ip mobile router-service collocated
    ip mobile router-service hold-down reassociate 2000
!
! Receive v1 or v2 traps
snmp-server community public RO
snmp-server enable traps tty
!

! Receive v3 traps
snmp-server engineID remote 85.85.85.3 1234
snmp-server user labusr labgrp remote 85.85.85.2 v3 auth md5 <SNMP user password on WGB>
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout 25
```

noauth Mode Example

The WMIC supports only SNMPv3 in **noauth** and **authNoPriv** modes.

The following example show a workgroup bridge configured for SNMPv3 link traps in **noauth** mode:

Workgroup Bridge

```
interface Loopback0
ip address 1.2.3.4 255.255.0.0
no ip route-cache

snmp-server group labgrp v3 noauth
snmp-server user labusr labgrp v3
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server host 1.7.35.35 version 3 noauth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4
snmp-server user labusr labgrp remote 1.2.3.4 v3
snmp-server group labgrp v3 noauth
snmp-server manager
snmp-server manager session-timeout <num>
```

noauth and authNoPriv Modes Example

The WMIC supports only SNMPv3 in **noauth** and **authNoPriv** modes.

The following example show a workgroup bridge configured for SNMPv3 link traps in **authNoPriv** mode:

Workgroup Bridge

```
interface Loopback0
ip address 1.2.3.4 255.255.0.0
no ip route-cache

snmp-server group labgrp v3 auth
snmp-server user labusr labgrp v3 auth md5 MD5passwd
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server host 1.7.35.35 version 3 auth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4
snmp-server user labusr labgrp remote 1.2.3.4 v3 auth md5 MD5passwd
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout <num>
```

Note For faster roaming during address acquisition, pings from the DHCP server to the client should be disabled.

Related Commands

This section describes the following related commands:

- ip mobile router-service collocated Command
- ip mobile router-service collocated registration retry Command
- ip mobile router-service hold-down Command
- ip dhcp client mobile renew
- debug snmp packet Command
- show ip mobile router Command
- show ip mobile router agent Command
- show ip mobile router interface Command
- show ip mobile router binding Command

ip mobile router-service collocated Command

The **ip mobile router-service collocated** command enables or disables CCoA processing on the interface. The interface primary IP address is used as the CCoA. The interface must already be configured as a roaming interface (**ip mobile router-service roam)**; otherwise, an error message is displayed.

Use the **ip mobile router-service collocated** interface command to enable or disable CCoA processing on the interface.

```
ip mobile router-service collocated [gateway <ipaddress>] [ccoa-only]
```

where:

gateway <*ipaddress*> is required for Ethernet interfaces with static IP addresses. The IP address specifies the default gateway to use when registering the CCoA on Ethernet. The default gateway IP address must be on the same link as the interface configured for static CCoA.

This address must not be 0.0.0.0 or 255.255.255.255 or the parameter will be rejected. Changing this gateway address while the mobile access router is registered triggers a new registration by using the new address.

When a roaming interface comes up the interface solicits foreign agent advertisements and if an advertisement is heard, it registers with a foreign agent CoA. If no advertisements are received, CCoA registration is enabled on the interface.

ccoa-only turns off agent discovery and the interface is immediately enabled for CCoA. Enabling CCoA by using this option on an interface already registered with a foreign agent CoA causes the mobile access router to immediately register with a CCoA.

Disabling CCoA by using the **no ip mobile router-service collocated** command on an interface already registered with a CCoA causes the interface to deregister its CCoA and begin foreign agent discovery.

If an Ethernet interface is configured with a static IP address, a gateway address must be configured. If the IP address configuration is changed acquire the IP address dynamically, the gateway address is the CCoA. The gateway address is reset to 0.0.0.0. If a configuration is changed to a static address, you are warned that CCoA processing will be disabled until CCoA is enabled with the specified gateway address.

The primary interface address is used as the CCoA, but registrations are rejected by the home agent if the CCoA and the home address are the same. So attempts to configure the addresses in this way trigger a warning message. Address checks are performed when interface IP addresses or CCoA gateway addresses are configured, or acquired dynamically, or when a home address is configured. If necessary, warnings are issued but **the configuration is still accepted**. At the time of registration, if the CCoA and home address are still the same, the mobile access router does not send the request and an error message is displayed.

ip mobile router-service collocated registration retry Command

CCoA interfaces use an interval timer to retry registration after a failed attempt.

Use the **ip mobile router-service collocated registration retry** interface command to set the interval for retrying CCoA registrations.

```
ip mobile router-service collocated registration retry <1-65535>
```

where *1-65565* is the number of seconds after a registration failure that the device waits before again attempting to register. The default value is **60** seconds.

The retry interval value is displayed by using the **show ip mobile router agent** command. If the interval timer is running, the time remaining until the next registration attempt is also displayed.

Note: Entering this command does not enable or disable CCoA support. It merely sets the timer interval.

ip mobile router-service hold-down Command

The **ip mobile router-service hold-down** [**foreign-agent** <*sec*> | **reassociate** <*msec*>] Layer 2 hold-down configuration command may be used to set reassociation delays for a roaming interface attached to a wireless link. For example:

```
(config-if)#ip mobile router-service hold-down [foreign-agent | reassociate]
```

foreign-agent	Time to wait before recognizing a new foreign agent (0-3600 seconds, default 0)
reassociate	Time to wait for layer 2 link reassociation (0 - 5000 msec, default 1000)

ip dhcp client mobile renew

The **ip dhcp client mobile renew** interface configuration command is for use on mobile DHCP clients. Clients automatically attempt to renew an existing IP address in response to certain events, for example, moving between wireless access points. The number of renewal attempts and the interval between those attempts, depending on network conditions, can be modified.

To set the number of IP address renewal attempts before starting the discover process, use the **ip dhcp client mobile renew count** command:

```
ip dhcp client mobile renew count <count> interval <msec>
```

count	Number of renewal attempts before starting discover. The range is 0–10 attempts. The default is 2 attempts.
interval	Interval (*msec*) between renewal attempts. The range is 1–1000 msecs. The default is 50 msecs.

debug snmp packet Command

The **debug snmp packet** command displays information about every Simple Network Management Protocol (SNMP) packet sent or received by the router, use the debug snmp packet command in privileged EXEC mode.

```
Router#debug snmp packet
```

The following is sample output from the debug snmp packet command. In this example, the messages the router receives display the following messages if SNMP trap is configured correctly.

WMIC

```
Router# debug snmp packet
Mar  1 00:04:40.508: SNMP: Queuing packet to 85.85.85.1
*Mar  1 00:04:40.509: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 28051
snmpTrapOID.0 = snmpTraps.3
ifEntry.1.5 = 5
ifEntry.2.5 = Virtual-Dot11Radio0
ifEntry.3.5 = 71
lifEntry.20.5 = administratively down
*Mar  1 00:04:40.515: SNMP: Queuing packet to 85.85.85.1
*Mar  1 00:04:40.515: SNMP: V2 Trap, reqid 2, errstat 0, erridx 0
sysUpTime.0 = 28051
snmpTrapOID.0 = snmpTraps.3
ifEntry.1.1 = 1
ifEntry.2.1 = Dot11Radio0
ifEntry.3.1 = 71
lifEntry.20.1 = administratively down
*Mar  1 00:04:40.759: SNMP: Packet sent via UDP to 85.85.85.1
*Mar  1 00:04:41.009: SNMP: Packet sent via UDP to 85.85.85.1
```

Mobile Router

```
Router# debug snmp packet
*Mar  4 19:30:12.265: SNMP: Packet received via UDP from 40.20.0.12 on FastEthernet0/0
*Mar  4 19:30:12.513: SNMP: Packet received via UDP from 40.20.0.12 on FastEthernet0/0
```

show ip mobile router Command

The following is an example of the output from the **show ip mobile router** command when the interface is registered as DCCoA.

```
UUT1#sh ip mobile router

Mobile Router
   Enabled 03/01/02 02:44:14
   Last redundancy state transition NEVER

Configuration:
   Home Address 85.85.85.1 Mask 255.255.255.0
   Home Agent 30.10.0.2 Priority 100 (best) (current)
   Registration lifetime 60 sec
   Retransmit Init 1000, Max 5000 msec, Limit 3
   Extend Expire 120, Retry 3, Interval 10

Monitor:
   Status -Registered-
   Using collocated care-of address 40.20.0.11
   On interface FastEthernet0/0
   Tunnel0 mode IP/IP
```

The following is an example of the output from the **show ip mobile router** command when the interface is registered by using a CoA.

```
UUT1#sh ip mobile router

Mobile Router
   Enabled 03/01/02 02:44:14
   Last redundancy state transition NEVER

Configuration:
   Home Address 85.85.85.1 Mask 255.255.255.0
   Home Agent 30.10.0.2 Priority 100 (best) (current)
   Registration lifetime 60 sec
   Retransmit Init 1000, Max 5000 msec, Limit 3
   Extend Expire 120, Retry 3, Interval 10
```

```
Monitor:
   Status -Registered-
   Active foreign agent 40.20.0.2, Care-of 40.20.0.2
   On interface FastEthernet0/0
   Tunnel0 mode IP/IP
```

show ip mobile router agent Command

The following is an example of the output from the **show ip mobile router agent** command:

```
Router#show ip mobile router agent
Mobile Router Agents:
Foreign agent 45.0.0.2:
    Care-of address 42.0.0.2
    Interface Ethernet1, MAC 0030.9492.6627
    Agent advertisement seq 56649, Flags rbhFmGvt, Lifetime 36000
    IRDP advertisement lifetime 30, Remaining 29
    Last received 02/13/02 17:55:48
    First heard 02/13/02 11:21:46

Collocated Care-of address 11.0.0.1
    Interface Serial0/1
    Default gateway 11.0.0.2
    Registration retry interval 60
    Next CCoA reg attempt in 00:00:55 seconds
```

show ip mobile router interface Command

The **show ip mobile router interface** command output shows the Layer 2 link down hold-down value and the most recently processed link state trap.

```
mobrouter#show ip mobile router interface

Ethernet1:
    Priority 110, Bandwidth 10000, Address 55.0.0.8
    Periodic solicitation disabled, Interval 600 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Current 5000, Remaining 0 msec, Count 4
    Foreign agent hold down 0 sec
    Layer 2 reassociation hold down 5000 msec
    Last layer 2 link-state trap: linkDown
    Routing disallowed
    Collocated CoA 55.0.0.8 - Solicit FAs
```

show ip mobile router binding Command

The following is an example of the output from the **show ip mobile router binding** command on the home agent:

```
Router#show ip mobile binding
Mobility Binding List:
Total 1
20.0.4.1:
    Care-of Addr 12.0.0.1, Src Addr 12.0.0.1
    Lifetime granted 00:02:00 (120), remaining 00:01:54
    Flags sbDmgvt, Identification C05E97DB.167E8950
    Tunnel0 src 46.0.0.3 dest 12.0.0.1 reverse-allowed
    MR Tunnel0 src 46.0.0.3 dest 12.0.0.1 reverse-allowed
    MR mobile-network 20.0.4.1
    Routing Options - (D)Direct-to-MN
```

In the **Flags sbDmgvt** entry, the “D” indicates that the mobile node is registered using a CCoA. (A lower-case “d” indicates that the mobile node is registered using a foreign agent.)