CHAPTER 2

Configuring IPv4

This chapter describes how to configure Internet Protocol version 4 (IPv4), which includes addressing, Address Resolution Protocol (ARP), Reverse ARP, and Internet Control Message Protocol (ICMP), on Cisco 1000 Series Connected Grid Routers (*hereafter* referred to as the Cisco CG-OS router). The system software for the router is identified as the Cisco CG-OS software.

This chapter includes the following sections:

Information About IPv4

You can configure IP on the Cisco CG-OS router to assign IP addresses to network interfaces. When you assign IP addresses, you enable the interfaces and allow communication with the hosts on those interfaces. The Cisco CG-OS router supports the following interfaces: cellular (3G), WiMax, and Ethernet (Fast Ethernet and Gigabit Ethernet).

You can configure an IP address as primary or secondary on a Cisco CG-OS router. An interface can have one primary IP address and multiple secondary addresses. All networking devices on an interface must share the same primary IP address because the packets that are generated by the Cisco CG-OS router always use the primary IPv4 address. Each IPv4 packet is based on the information from a source or destination IP address. For more information, see the Multiple IPv4 Addresses, page 2-2.

You can use a subnet to mask the IP addresses. A mask determines to which subnet an IP address belongs. An IP address contains the network address and the host address. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. Subnet masks are 32-bit values that allow the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID portion of the IP address.

The IP feature is responsible for handling IPv4 packets that terminate on the Cisco CG-OS router, as well as forwarding of IPv4 packets, which includes IPv4 unicast and multicast route lookup, reverse path forwarding (RPF) checks, and software access control list and policy-based routing (ACL/PBR) forwarding. The IP feature also manages the network interface IP address configuration, duplicate address checks, static routes, and packet send and receive interface for IP clients.

This section includes the following topics:

Multiple IPv4 Addresses

The Cisco CG-OS router supports multiple IP addresses per interface. You can specify an unlimited number of secondary addresses for a variety of situations. The most common are as follows:

- When there are not enough host IP addresses for a particular network interface. For example, if your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you must have 300 host addresses, then you can use secondary IP addresses on the Cisco CG-OS router or access servers to allow you to have two logical subnets that use one physical subnet.
- Two subnets of a single network might otherwise be separated by another network. You can create a single network from subnets that are physically separated by another network by using a secondary address. In these instances, the first network is extended, or layered on top of the second network. A subnet cannot appear on more than one active interface of the Cisco CG-OS router at a time.

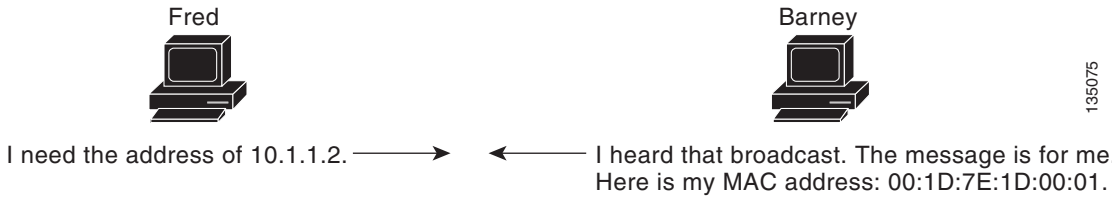
Note If any device on a network segment uses a secondary IPv4 address, then all other devices on that same network interface must also use a secondary address from the same network or subnet. The inconsistent use of secondary addresses on a network segment can quickly cause routing loops.

Address Resolution Protocol

Networking devices and Layer 3 switches and routers use Address Resolution Protocol (ARP) to map IP (network layer) addresses to (Media Access Control [MAC]-layer) addresses which enables IP packets to be sent across networks. Before a device sends a packet to another device, it looks in its own ARP cache to see if there is a MAC address and corresponding IP address for the destination device. If there is no entry, then the source device sends a broadcast message to every device on the network.

Each device compares the IP address to its own. Only the device with the matching IP address replies to the device that sends the data with a packet that contains the MAC address for the device. The source device adds the destination device MAC address to its ARP table for future reference, creates a data-link header and trailer that encapsulates the packet, and proceeds to transfer the data. Figure 2-1 shows the ARP broadcast and response process.

Figure 2-1 ARP Process



When the destination device lies on a remote network that is beyond another device, the process is the same except that the device that sends the data sends an ARP request for the MAC address of the default gateway. After the address is resolved and the default gateway receives the packet, the default gateway broadcasts the destination IP address over the networks connected to it. The device on the destination device network uses ARP to obtain the MAC address of the destination device and delivers the packet. ARP is enabled by default.

ARP Caching

ARP caching allows the Cisco CG-OS router to store information from previous ARP translations (IP to MAC address mappings for devices). The mapping of IP addresses to MAC addresses occurs at each hop (device) on the network for every packet sent over an internetwork.

By caching the network addresses and the associated data-link addresses in the memory for a period of time, the Cisco CG-OS router eliminates the need to reexamine each packet when it is broadcast. Instead, the Cisco CG-OS router can reference the ARP cache first and then apply the appropriate address to a packet that is destined for a known destination device. This process helps limit possible negative affects on network performance.

Static and Dynamic Entries in the ARP Cache

Static routing requires that you manually configure the IP addresses, subnet masks, gateways, and corresponding MAC addresses for each interface of each device. Static routing requires more work to maintain the route table. You must update the table each time you add or change routes.

Dynamic routing uses protocols that enable the devices in a network to exchange routing table information with each other. Dynamic routing is more efficient than static routing because the route table automatically updates unless you add a time limit to the cache. Although the default time limit is 25 minutes, you can modify the time limit when the network has a large number of additions and deletions of routes from the cache.

Devices That Do Not Use ARP

When a network is divided into two segments, a bridge joins the segments and filters traffic to each segment based on MAC addresses. The bridge builds its own address table, which uses MAC addresses only. A device has an ARP cache that contains both IP addresses and the corresponding MAC addresses.

Passive hubs are central-connection devices that physically connect other devices in a network. Hubs send messages out on all their ports to the devices and operate at Layer 1 but do not maintain an address table.

Layer 2 switches determine which port connects to the destination device for the message and forwards that message only to that port. However, Layer 3 switches build an ARP cache.

Proxy ARP

Proxy ARP enables a device that is physically located on one network to appear to be logically part of a different physical network that connects to the same device or firewall. Proxy ARP allows you to hide a device with a public IP address on a private network behind a router and still have the device appear to be on the public network in front of the router. By hiding its identity, the router accepts responsibility for routing packets to the real destination. Proxy ARP can help devices on a subnet reach remote subnets without configuring routing or a default gateway.

When devices are not in the same data link layer network but in the same IP network, they try to transmit data to each other as if they are on the local network. However, the router that separates the devices does not send a broadcast message because routers do not pass hardware-layer broadcasts and it cannot resolve the addresses.

When you enable Proxy ARP on the device and it receives an ARP request, it identifies the request as a request for a system that is not on the local LAN. The device responds as if it is the remote destination to which the broadcast is addressed by sending an ARP response that associates the MAC address of the device with the IP address of the remote destination. The local device believes that it is directly connected to the destination device, although their local device is forwarding packets from its local subnetwork to the destination subnetwork. By default, Proxy ARP is disabled.

Local Proxy ARP

You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet in which routing is not generally required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts do not communicate directly with one another by design. The devices that the hosts connect to are configured to prevent this direct communication.

Gratuitous ARP

Gratuitous ARP sends a request with an identical source IP address and a destination IP address to detect duplicate IP addresses.

Path MTU Discovery

Path maximum transmission unit (MTU) discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection. It is described in RFC 1191. Existing connections are not affected when this feature is turned on or off.

ICMP

You can use the Internet Control Message Protocol (ICMP) to provide message packets that report errors and other information that is relevant to IP processing. ICMP generates error messages, such as ICMP destination unreachable messages, ICMP Echo Requests (which send a packet on a round trip between two hosts), and Echo Reply messages. ICMP also provides many diagnostic functions and can send and redirect error packets to the host. By default, ICMP is enabled on the Cisco CG-OS router.

Some of the ICMP message types are as follows:

- Network error messages
- Network congestion messages
- Troubleshooting information
- Timeout announcements

Note ICMP redirects are disabled on interfaces on which the local proxy ARP feature is enabled.

Prerequisites for IPv4

IPv4 can only be configured on Layer 3 interfaces. The Cisco CG-OS router supports the following Layer 3 interfaces: cellular (3G), WiMax, and Ethernet (Fast Ethernet and Gigabit Ethernet).

Guidelines and Limitations for IPv4

You can configure a secondary IP address only after you configure the primary IP address.

Default Settings

Table 2-1 lists the default settings for IP parameters.

Table 2-1 Default IP Parameters

Parameters	Default
ARP timeout	1500 seconds
proxy ARP	Disabled

Configuring IPv4

This section includes the following topics:

Configuring IPv4 Addressing

You can assign a primary IP address for a network interface.

BEFORE YOU BEGIN

Be aware of the IPv4 addressing plan employed in the network.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.
Step 3	**ip address** *ip address mask* **[secondary]**	Specifies a primary or secondary IPv4 address for an interface. • The network mask can be a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means the corresponding address bit belongs to the network address. • The network mask can be indicated as a slash (/) and a number (a prefix length). The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash must precede the decimal value and there is no space between the IP address and the slash.
Step 4	**show ip interface**	(Optional) Displays interfaces configured for IPv4.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to assign an IPv4 address to an interface.

```
router# configure terminal
router(config)# interface ethernet 2/3
router(config-if)# ip address 192.168.1.1 255.0.0.0
router(config-if)# copy running-config startup-config
```

Configuring Multiple IP Addresses

BEFORE YOU BEGIN

Configure the primary IP address.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.
Step 3	**ip address** *ip address mask* **[secondary]**	Specifies the configured address as a secondary IPv4 address.
Step 4	**show ip interface**	(Optional) Displays interfaces configured for IPv4.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to assign multiple, secondary IPv4 addresses to an interface.

```
router# configure terminal
router(config)# interface ethernet 2/3
router(config-if)# ip address 192.168.1.1 255.0.0.0 secondary
router(config-if)# copy running-config startup-config
```

Configuring a Static ARP Entry

You can configure a static ARP entry on the device to map IP addresses to MAC hardware addresses.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.

	Command	Purpose
Step 3	**ip arp** *ip-address mac-address*	Associates an IP address with a MAC address as a static entry.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure a static ARP entry on an interface.

```
router# configure terminal
router(config)# interface ethernet 2/3
router(config-if)# ip arp 192.168.1.1 0019.076c.1a78
router(config-if)# copy running-config startup-config
```

Configuring Proxy ARP

You can configure Proxy ARP on the Cisco CG-OS router to determine the media addresses of hosts on other networks or subnets.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.
Step 3	**ip proxy-arp**	Enables Proxy ARP on the interface.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure Proxy ARP on the Cisco CG-OS router.

```
router# configure terminal
router(config)# interface ethernet 2/3
router(config-if)# ip proxy-arp
router(config-if)# copy running-config startup-config
```

Configuring Local Proxy ARP

You can configure local proxy ARP on a Cisco CG-OS router interface.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.
Step 3	**ip local-proxy-arp**	Enables Local Proxy ARP on the interface.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure local proxy ARP on an Ethernet interface.

```
router# configure terminal
router(config)# interface ethernet 2/3
router(config-if)# ip local-proxy-arp
router(config-if)# copy running-config startup-config
```

Configuring Gratuitous ARP

Although enabled by default on the Cisco CG-OS router, you can modify the request and update parameters for gratuitous ARP on the interface.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**interface ethernet** *slot/port*	Enters interface configuration mode.
Step 3	**ip arp gratuitous** {**request** | **update**}	Configures gratuitous ARP parameters on the interface. Gratuitous ARP is enabled by default. **request**—Enables sending of gratuitous ARP requests when the Cisco CG-OS router detects a duplicate address. **update**—Enables ARP cache updates for gratuitous ARP.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to enable sending of gratuitous ARP requests when the Cisco CG-OS router detects duplicate addresses:

```
router# configure terminal
router(config)# interface ethernet 2/3
```

```
router(config-if)# ip arp gratuitous request
router(config-if)# copy running-config startup-config
```

To disable gratuitous ARP requests or updates, use the **no ip arp gratuitous** command.

Configuring Path MTU Discovery

You can configure path MTU discovery to determine the maximum transmit unit (MTU) that you can transmit within the network without requiring fragmentation.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters configuration mode.
Step 2	**ip tcp path-mtu-discovery**	Enables path MTU discovery.
Step 3	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure path MTU discovery on the Cisco CG-OS router.

```
router# configure terminal
router(config)# ip tcp path-mtu-discovery
router(config)# copy running-config startup-config
```

Configuring IP Directed Broadcasts

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet but which originates from a device that is not itself part of that destination subnet.

A device that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way that it forwards unicast IP packets destined to a host on that subnet.

When you enable directed broadcast on an interface, the Cisco CG-OS router broadcasts those incoming IP packets identified as directed broadcast to the subnet on which that interface is attached. Then, the destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

To enable IP directed broadcasts, use the appropriate command in the interface configuration mode.

:

Command	Purpose
ip directed-broadcast	Enables the translation of a directed broadcast to physical broadcasts for an interface. To disable directed broadcasts, enter the **no ip directed-broadcast** command.

Verifying the IPv4 Configuration

To display IPv4 configuration information, enter any or all of the following commands:

Note The Cisco CG-OS router does not support the optional parameter, [**vrf** *vrf-name*], when present in any of the **show** commands listed below.

Command	Purpose
show ip adjacency	Displays the adjacency table.
show ip adjacency summary	Displays the summary of number of throttle adjacencies.
show ip arp	Displays the ARP table.
show ip arp summary	Displays the summary of the number of throttle adjacencies.
show ip adjacency throttle statistics	Displays only the throttled adjacencies.
show ip interface	Displays IP-related interface information.
show ip arp statistics	Displays the ARP statistics.

Configuration Example for IPv4

This example shows how to configure an IPv4 address:

```
configure terminal
 interface e 2/1
  ip address 192.2.1.1/16
```