



## Configuring CSS Network Protocols

---

This chapter describes how to configure Domain Name Service (DNS), Address Resolution Protocol (ARP), Routing Information Protocol (RIP), Internet Protocol (IP) routing, spanning-tree bridging, and Dynamic Host Configuration Protocol (DHCP). Information in this chapter applies to all CSS models, except where noted.

This chapter includes the following major sections:

- [Configuring the Domain Name Service](#)
- [Configuring the Address Resolution Protocol](#)
- [Configuring Routing Information Protocol](#)
- [Configuring the Internet Protocol](#)
- [Configuring the Cisco Discovery Protocol](#)
- [Configuring Spanning-Tree Bridging for the CSS](#)
- [Configuring the DHCP Relay Agent](#)

# Configuring the Domain Name Service

Use the **dns** command to enter commands that control Domain Name Service (DNS), the facility that translates host names such as myhost.mydomain.com to IP addresses such as 192.168.11.1.

This section includes the following topics:

- [Specifying a Primary DNS Server](#)
- [Using DNS Resolve](#)
- [Specifying a Secondary DNS Server](#)
- [Specifying a DNS Suffix](#)
- [Specifying UDP Traffic on the DNS Server Port](#)

Use the **show running-config global** command to display DNS configurations (refer to [Chapter 3, Managing the CSS Software](#)).

## Specifying a Primary DNS Server

Use the **dns primary** command to specify the primary DNS server. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) of the DNS server you want to specify as the primary DNS server.

For example:

```
(config)# dns primary 192.168.11.1
```

To remove the primary DNS server, enter:

```
(config)# no dns primary
```

## Using DNS Resolve

Use the **dns resolve** command to resolve a host name by querying the DNS server. Enter the host name you want to resolve in mnemonic host-name format (for example, myhost.mydomain.com).

For example:

```
(config)# dns resolve fred.arrowpoint.com
```

## Specifying a Secondary DNS Server

When a primary DNS server fails, the CSS uses the secondary DNS server to resolve host names to IP addresses. Use the **dns secondary** command to specify a secondary DNS server. Enter the IP address of the secondary DNS server in dotted-decimal notation (for example, 192.168.11.1).

```
(config)# dns secondary 192.168.3.6
```

You can specify a maximum of two secondary servers. To specify each additional server, repeat the **dns secondary** command. The order in which you enter the IP addresses is the order in which they are used when the primary DNS server fails.

To remove a secondary DNS server, specify the **no** version of the command followed by the IP address of the DNS server you wish to remove. For example:

```
(config)# no dns secondary 192.168.3.6
```

## Specifying a DNS Suffix

Use the **dns suffix** command to specify the default suffix to use when querying the DNS facility. Enter the default suffix as an unquoted text string with no spaces and a maximum of 64 characters.

For example:

```
(config)# dns suffix arrowpoint.com
```

To remove the default DNS suffix, enter:

```
(config)# no dns suffix
```

## Specifying UDP Traffic on the DNS Server Port

For DNS UDP traffic on port 53, use the **dnsflow** command to determine whether the CSS uses flow control blocks (FCBs) for DNS requests and responses. This command provides the following options:

- **enable** (default) - Causes the CSS to set up flows using FCBs for DNS requests and responses. Because UDP traffic is connectionless, the DNS flows remain active until the flow manager reclaims the flow resources.
- **disable** - Causes the CSS to not use FCBs for the DNS requests and responses. Use this setting for sites with heavy DNS traffic or sites where the DNS clients use a source and destination port of 53.

For example:

```
(config)# dnsflow disable
```

# Configuring the Address Resolution Protocol

Use the **arp** command to statically configure the IP to Media Access Control (MAC) translations necessary for the CSS to send data to network nodes. You can configure static ARP mapping for any of the CSS Ethernet interface ports.

This section includes the following topics:

- [Configuring ARP](#)
- [Configuring ARP Timeout](#)
- [Configuring ARP Wait](#)
- [Updating ARP Parameters](#)
- [Clearing ARP Parameters](#)
- [Showing ARP Information](#)

## Configuring ARP

Use the **arp** command to define a static ARP mapping. The syntax for this global configuration mode command is:

```
arp ip_or_host mac_address interface {vlan}
```

The variables and options are as follows:

- *ip\_or\_host* - The IP address of the system for static mapping. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com).
- *mac\_address* - The MAC address of the system mapped to the IP address. Enter the MAC address in hyphenated-hexadecimal notation (for example, 00-60-97-d5-26-ab).
- *interface* - The CSS Ethernet interface port that you want to configure. For a CSS 11501, enter the interface name in *interface port* format (for example, e2). For a CSS 11503 or CSS 11506, the interface format is *slot/port* (for example, 3/1).
- *vlan* - The number of the VLAN configured in a trunked interface on which the ARP address is configured (assuming trunking is enabled for the CSS Gigabit Interface port). Enter an integer from 1 to 4094 as the VLAN number.

For example:

```
(config)# arp 192.168.11.1 00-60-97-d5-26-ab e2
```

To remove a static mapping address, use the **no arp** command. For example:

```
(config)# no arp 192.168.11.1
```

**Note**

The CSS discards ARP requests from hosts that are not on the same network as the CSS circuit IP address. Thus, if a CSS and a host are within the same VLAN but configured for different IP networks, the CSS does not respond to ARP requests from the host.

## Configuring ARP Timeout

Use the **arp timeout** command to set the time, in seconds, to hold an ARP resolution result. When you change the timeout value, this value affects only new ARP entries. All previous ARP entries retain the old timeout value. To remove all entries with the old timeout value, enter the **clear arp cache** command.

The timeout value is the number of seconds the CSS holds an ARP resolution result. To set a timeout value, enter an integer from 60 to 86400 (24 hours) seconds. The default is 14400 seconds (4 hours). If you do not want the ARP entries to time out, enter **none** or **86401**.

For example:

```
(config)# arp timeout 120
```

To restore the default timeout value of 14400 seconds, enter:

```
(config)# no arp timeout
```

## Configuring ARP Wait

Use the **arp wait** command to set the time, in seconds, to wait for an ARP resolution. The wait time is the number of seconds the CSS waits for an ARP resolution in response to an ARP request to the network. Enter an integer from 5 to 30 seconds. The default is 5.

For example:

```
(config)# arp wait 15
```

To restore the default wait time of 5 seconds, enter:

```
(config)# no arp wait
```

## Updating ARP Parameters

Use the **update arp** command to update the file containing hosts reachable through ARP. This command is available only in SuperUser mode. For example:

```
# update arp file
```

## Clearing ARP Parameters

The CSS enables you to clear ARP parameters for the ARP file or ARP cache. To clear the file that contains known hosts reachable through ARP, use the **clear arp file** command. For example:

```
# clear arp file
```

Use the **clear arp cache** command to delete dynamic entries from the ARP cache. To specify an address for the single ARP entry you want to remove from the ARP cache, use the **clear arp cache ip\_or\_host** command. Enter the address in either dotted-decimal IP notation (for example, 192.168.11.1) or mnemonic host-name format (for example, myhost.mydomain.com).

For example:

```
# clear arp cache 192.168.11.1
```

## Showing ARP Information

Use the **show arp** command to display ARP information. To show static ARP mapping when you use the **show arp** command, the IP route must exist in the routing table.

The syntax for this global configuration mode command is:

```
show arp {config|file|management-port|summary|ip_or_host}
```

The syntax and options for the command are as follows:

- **show arp** - Displays the complete ARP resolution table with IP addresses, MAC addresses, and resolution type, excluding entries from the CSS Ethernet management port.
- **config** - Displays ARP global configuration parameters. The screen displays the response timeout and the flush timeout, in seconds.
- **file** - Displays the hosts that are reachable using ARP. The screen displays the IP addresses of the host systems.
- **management-port** - Displays the ARP entries from the CSS Ethernet management port. The ARP resolution table displayed through the **show arp** command displays these entries.



---

**Note** The CSS Ethernet management port IP address appears as an entry in the Management Port ARP cache. This is normal CSS behavior.

---

- **summary** - Displays the total number of static entries, total number of dynamic entries, and total number of entries in the ARP resolution table, excluding the entries from the CSS management port.
- *ip\_or host* - The IP address for the system to display its resolution. Enter the address in dotted-decimal format (for example, 192.168.11.1) or mnemonic host-name format (for example, myname.mydomain.com). You cannot enter an ARP entry derived from the CSS Ethernet management port.

For example, to display the complete ARP resolution table, enter:

```
# show arp
```

Table 6-1 describes the fields in the **show arp** command output.

**Table 6-1 Field Descriptions for the show arp Command**

Field	Description
IP Address	The IP address of the system for ARP mapping.
MAC Address	The MAC address of the system mapped to the IP address.
Type	The resolution type for the entry: Dynamic or Static. The Dynamic resolution type indicates that the entry was discovered through the ARP protocol. The Static resolution type indicates that the entry is from a static configuration.
Port	The CSS interface configured as the egress logical port.

To display a summary of entries in the ARP resolution table, enter:

```
# show arp summary
```

Table 6-2 describes the fields in the **show arp summary** command output.

**Table 6-2 Field Descriptions for the show arp summary Command**

Field	Description
Static Entry	The total number of static map entries in the ARP resolution table (from a static configuration).
Dynamic Entry	The total number of dynamic map entries in the ARP resolution table (entries discovered through the ARP protocol).
Total Entry	The total number of static and dynamic entries in the ARP resolution table.

To display the global ARP configuration, enter:

```
# show arp config
```

Table 6-3 describes the fields in the **show arp config** command output.

**Table 6-3 Field Descriptions for the show arp config Command**

Field	Description
ARP Response Timeout	The time, in seconds, to wait for an ARP resolution response before discarding the packet waiting to be forwarded to an address. The time can be from 5 to 30 seconds. The default is 5 seconds.
ARP Flush Timeout	The time, in seconds, to hold an ARP resolution result in the ARP cache. The timeout period can be from 60 to 86400 seconds (24 hours). The default is 14400 seconds (4 hours). An entry of none or 86401 indicates the ARP entries will not timeout.

To display the host IP addresses entered at initialization or boot time through ARP, enter:

```
# show arp file
```

To display the ARP entries from the CSS management port, enter:

```
# show arp management-port
```

Table 6-4 describes the fields in the **show arp management-port** command output.

**Table 6-4 Field Descriptions for the show arp management-port Command**

Field	Description
IP Address	The IP address of the system for ARP mapping.
MAC Address	The MAC address of the system mapped to the IP address.
Port	The CSS Ethernet management port.

To display the resolution for a host IP address, enter:

```
# show arp 192.50.1.6
```

To display the host IP addresses entered at initialization or boot time through ARP, enter:

```
# show arp file
```

## Configuring Routing Information Protocol

The CSS enables you to configure global Routing Information Protocol (RIP) attributes used to advertise routes on the CSS. By default, RIP advertises RIP routes and local routes for interfaces running RIP. The **rip** command advertises other routes.

The timers used by RIP in the CSS include the following default values. These RIP timer values are not user-configurable in the CSS.

- Transmit (Tx) time that is a random value between 15 and 45 seconds (it avoids router synchronization problems)
- Route expiration time of 180 seconds (if the CSS loses the link to the next hop router, the route is immediately removed).
- Hold-down time (the amount of time the CSS transmits with an infinite metric) of 120 seconds.

This section includes the following topics:

- [Configuring RIP Advertise](#)
- [Configuring RIP Redistribute](#)
- [Configuring Equal-Cost RIP Routes](#)
- [Showing RIP Configurations](#)



### Note

If you prefer OSPF instead of RIP on the CSS, refer to [Chapter 7, Configuring Open Shortest Path First \(OSPF\)](#) for information on configuring OSPF.

## Configuring RIP Advertise

Use the **rip advertise** command to advertise a route through RIP on the CSS. The syntax for this command is:

```
rip advertise ip_address subnet_mask {metric}
```

The variables for this command are as follows:

- *ip\_address* - The IP address for the route prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.1.0).
- *subnet\_mask* - The IP prefix length in CIDR bitcount notation (for example, /24) or in dotted-decimal notation (for example, 255.255.255.0).
- *metric* - (Optional) Metric to use when advertising this route. Enter a number from 1 to 15. The default is 1.

For example:

```
(config)# rip advertise 192.168.1.0/24 9
```



### Note

The network does not have to be present in the routing table to be advertised. The **SNTP ip advertise** command is intended for advertising VIP addresses.

To stop advertising a route through RIP on the CSS, enter:

```
(config)# no rip advertise 192.168.1.0/24
```

## Configuring RIP Redistribute

Use the **rip redistribute** command to advertise routes from other protocols through RIP. By default, RIP advertises RIP routes and local routes for interfaces running RIP. This command instructs RIP to advertise other routes, such as firewall routes, OSPF routes, and so on.

The syntax for this command is

```
rip redistribute [firewall|local|ospf|static] {metric}
```

The options and variables for this command are as follows:

- **firewall** - Advertises firewall routes through RIP.
- **local** - Advertises local routes (interfaces *not* running RIP).
- **static** - Advertises static routes configured for the Ethernet interface ports.
- **ospf** - Advertises OSPF routes through RIP.
- **metric** - (Optional) Metric to use when advertising this route. Enter a number from 1 to 15. The default is 1.

For example:

```
(config)# rip redistribute static 3
```

To stop advertising routes from other protocols through RIP, use either the **local**, **static**, or **firewall** option.

The following commands stop advertising static routes:

```
(config)# no rip redistribute firewall  
(config)# no rip redistribute local  
(config)# no rip redistribute static  
(config)# no rip redistribute ospf
```

## Configuring Equal-Cost RIP Routes

Use the **rip equal-cost** command to set the maximum number of routes that RIP can insert into the routing table. Enter a number from 1 to 15. The default is 1. For example:

```
(config)# rip equal-cost 4
```

To reset the number of routes to the default value of 1, enter:

```
(config)# no rip equal-cost
```

## Showing RIP Configurations

Use the **show rip** command to show a RIP configuration for one IP address or all IP addresses configured in the CSS. This command provides the following options and variables:

- **show rip** - Displays RIP configurations for all interfaces
- **show rip ip\_address** - Displays a single RIP interface entry
- **show rip globals** - Displays RIP global statistics
- **show rip statistics** - Displays RIP interface statistics for all interfaces
- **show rip statistics ip\_address** - Displays RIP interface statistics for a specific interface

Table 6-5 describes the fields in the **show rip** command output.

**Table 6-5** Field Descriptions for the show rip Command

Field	Description
IP Address	The advertised RIP interface address.
State	The operational state of the RIP interface.
RIP Send	The RIP version that the interface sends. The possible field values are as follows: <ul style="list-style-type: none"> <li>• <b>none</b> - Do not send RIP packets</li> <li>• <b>RIPv1</b> - Send RIP version 1 packets only</li> <li>• <b>RIPv2</b> - Send RIP version 2 packets only (default)</li> </ul>
RIP Recv	The RIP version that the interface receives. The possible values are as follows: <ul style="list-style-type: none"> <li>• <b>both</b> - Receive both version 1 and version 2 (default)</li> <li>• <b>none</b> - Receive no RIP packets</li> <li>• <b>Ripv1</b> - Receive RIP version 1 packets only</li> <li>• <b>Ripv2</b> - Receive RIP version 2 packets only</li> </ul>
Default Metric	The default metric used for advertising the RIP interface.

**Table 6-5** *Field Descriptions for the show rip Command (continued)*

Field	Description
Tx Log	The setting for logging RIP packet transmissions (enabled or disabled). The default setting is disabled.
Rx Log	The setting for logging RIP packets received (enabled or disabled). The default setting is disabled.

To display global RIP statistics, enter:

```
# show rip globals
```

Table 6-6 describes the fields in the **show rip globals** command output.

**Table 6-6** *Field Descriptions for the show rip globals Command*

Field	Description
RIP Route Changes	The global number of route changes made to the IP route database by RIP
RIP Query Responses	The global number of query responses sent to RIP query from other systems

To display the RIP interface statistics for all RIP interface entries, enter:

```
# show rip statistics
```

Table 6-7 describes the fields in the **show rip statistics** command output.

**Table 6-7 Field Descriptions for the show rip statistics Command**

<b>Field</b>	<b>Description</b>
System Route Changes	The global number of route changes made to the IP route database by RIP
System Global Query Responses	The global number of query responses sent to RIP query from other systems
IP Address	The RIP interface IP address
Triggered Updates Sent	The number of triggered RIP updates sent by the interface
Bad Packets Received	The number of bad RIP response packets received by the interface
Bad Routes Received	The number of bad routes in valid RIP packets received by the interface

# Configuring the Internet Protocol

Use the **ip** command to specify Internet Protocol (IP) configuration commands for the CSS. This command is available in global configuration mode.

This section includes the following topics:

- [Configuring an IP Route](#)
- [Disabling an Implicit Service for the Static Route Next Hop](#)
- [Configuring an IP Source Route](#)
- [Configuring the IP Record Route](#)
- [Configuring Box-to-Box Redundancy](#)
- [Configuring IP Equal-Cost Multipath](#)
- [Forwarding IP Subnet Broadcast Addressed Frames](#)
- [Configuring IP Unconditional Bridging](#)
- [Configuring IP Opportunistic Layer 3 Forwarding](#)
- [Showing IP Configuration Information](#)

## Configuring an IP Route

A static route consists of a destination network address and mask, as well as the next hop to reach the destination. You can also specify a default static route (using 0.0.0.0 as the destination network address and a valid next hop address) to direct frames for which no other destination is listed in the routing table. Default static routes are useful for forwarding otherwise unrouteable packets by the CSS.

When you configure a static route, the CSS creates an internal service that periodically polls the configured next hop address with an ICMP echo (or ping) keepalive. The internal service is called an implicit service. If the router fails, the CSS removes any entries from the routing table that point to the failed router and stops sending network traffic to the failed router. When the router recovers, the CSS:

- Becomes aware of the router
- Reenters applicable routes into the routing table

The implicit service does not determine if the default or static route appears in the routing table. This decision is based on the CSS having a viable ARP entry for the next hop router IP address so the CSS can forward traffic to that destination. The CSS uses the ICMP keepalive as a means to ensure the next hop router MAC address is available and current. However, in certain situations, the next hop router may block ICMP message transmitted by the CSS, which results in a failed ICMP keepalive (the ICMP keepalive is in the Down state). As long as the CSS has the ARP entry of the next hop router the static route is still placed in the routing table.


**Note**

The CSS allows you to disable the internal ICMP keepalive through the **ip-no-implicit service** command. In this case, if the MAC address for the next hop is not known to the CSS the address will not appear in the routing table.

Use the **ip route** command to configure an IP route. You can configure a static route, a default static IP route, a blackhole route (where the CSS drops any packets addressed to the route), or a firewall IP route. Each **ip route** command requires one of the following:

- An IP address and a subnet mask prefix; for example, 192.168.1.0 /24
- An IP address and a subnet mask; for example, 192.168.1.0 255.255.255.0

The syntax for this global configuration command is:

```
ip route ip_address subnet_mask[blackholeip_address2{distance |
originated-packets}|firewall index {distance}]
```

The syntax and options for the command are as follows:

- *ip\_address* - The destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *subnet\_mask* - The IP subnet mask. Enter the mask in either:
  - CIDR bitcount notation (for example, /24).
  - Dotted-decimal notation (for example, 255.255.255.0).
- **blackhole** - Instructs the CSS to drop any packets addressed to the destination.
- *ip\_address2* - The next hop address for the route. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

- *distance* - (Optional) The administrative distance. Enter an integer from 1 to 254. A smaller number is preferable. The default value is 1.
- **originated-packets** - Specifies that the route is used only by packets created using flows or sessions going to and from the CSS (for example, a Telnet session to the CSS). The route is not used by flows or sessions that go through the CSS (for example, between an attached server and a remote client).



---

**Note** A ping response and an SNMP responses do not use the originated-packets route. A ping *request* sent from the CSS uses the originated-packets route. A ping *response* sent from the CSS does not use the originated-packets route.

---

- **firewall** - Configures a firewall route. The **firewall** option instructs the CSS to use firewall load balancing for this route. You can optionally set the administrative distance.



---

**Note** The CLI prevents you from configuring IP static routes with identical destinations *and* identical administrative costs, for IP static routes that are firewall routes and IP static routes that are not firewall routes.

---

- *index* - An existing index number for the firewall route. For information on configuring a firewall index, see the **ip firewall** command (refer to the *Cisco Content Services Switch Advanced Configuration Guide*).

For example, to configure a static IP route to destination network address *192.168.0.0 /16* and a next hop address of *192.167.1.1*, enter:

```
(config)# ip route 192.168.0.0 /16 192.167.1.1
```

For example, to configure a default IP route using a destination address of *0.0.0.0 /0* and a next hop address of *192.167.1.1*, enter:

```
(config)# ip route 0.0.0.0 /0 192.167.1.1
```

For example, to configure a blackhole route, enter:

```
(config)# ip route 192.168.1.0 /24 blackhole
```

For example, to configure a firewall IP route with an index number of *3* and an administrative distance of *2*, enter:

```
(config)# ip route 192.168.1.0 /24 firewall 3 2
```

To remove a static route, enter:

```
(config)# no ip route 0.0.0.0 /0 10.0.1.1
```

To disable the dropping of packets to a blackhole route, enter:

```
(config)# no ip route 192.168.1.0 /24 blackhole
```

To remove a firewall route, enter:

```
(config)# no ip route 192.168.1.0 /24 firewall 3
```

## Disabling an Implicit Service for the Static Route Next Hop

Use the **ip no-implicit-service** command when you do not want the CSS to start an implicit service for the next hop of a static route. By default, the CSS establishes an implicit (or internal) service for the gateway address when a static route is defined. The **ip no-implicit-service** command specifies that no implicit service is established to the next hop of the static route, which disables the internal service ICMP keepalive. In this case, if the ARP address for the next hop is not known to the CSS, the address will not appear in the routing table.

The purpose of the implicit service to the next hop of a static route is to monitor the availability of the next hop to forward data traffic. When the **ip no-implicit-service** command is in effect, traffic is forwarded to the next hop even when the next hop is unavailable. Because of the possibility of data being lost if the next hop becomes unavailable, use of the **ip no-implicit-service** command is strongly discouraged.



### Note

---

Static routes can sometimes appear in the CSS routing table even when you have an implicit service for the next hop address (the default setting) and the internal keepalive is down. When the CSS detects the ARP mapping for the next hop in the static route, the CSS continues to list that route in the routing table regardless of the state of the ICMP service keepalive (Down or Up).

---

When you implement the **ip no-implicit-service** global configuration command, this action does not affect previously configured static routes. The **ip no-implicit-service** command affects only those static routes added after you enable the command. We recommend you reboot the CSS after you modify the configuration to ensure all static routes are the same, which is useful for network monitoring and troubleshooting. If you wish to stop the implicit service for a previously configured static route, then you must delete and reconfigure the static route.

For example:

```
(config)# ip no-implicit-service
```

To reset the default setting, enter:

```
(config)# no ip no-implicit-service
```

## Configuring an IP Source Route

Use the **ip source-route** command to enable the CSS to process frames with information that overrides the default routing. For example:

```
(config)# ip source-route
```



### Caution

---

Enabling the **ip source-route** command may pose a major security risk to your network. The IP source route specifies information that overrides the default routing a packet would normally take. The packet could then bypass a firewall. If this poses a problem, avoid using the **ip source-route** command.

---

The CSS does not load balance TCP or UDP packets with IP options that are destined to a VIP address. These packet types are dropped and the CSS returns an ICMP destination/port unreachable error. This behavior exists regardless of the state (enabled or disabled) of the **ip source-route** and **ip record-route** commands.

The CSS, however, does respond to ICMP packets that are destined to a VIP address. The CSS also responds to TCP or UDP packets that include IP options that are destined to a local circuit address, or require that a routing decision be made.

To disable the processing of frames with the IP source-route option (the default behavior), enter:

```
(config)# no ip source-route
```

## Configuring the IP Record Route

Use the **ip record-route** command to enable the CSS to process frames with the IP address of each router along a path. For example:

```
(config)# ip record-route
```



### Caution

Enabling the **ip record-route** command could pose security risks to your network. The **ip record-route** command inserts the IP address of each router along a path into the IP header.

The CSS does not load balance TCP or UDP packets with IP options that are destined to a VIP address. These packet types are dropped and the CSS returns an ICMP destination/port unreachable error. This behavior exists regardless of the state (enabled or disabled) of the **ip record-route** and **ip source-route** commands.

The CSS, however, does respond to ICMP packets that are destined to a VIP address. The CSS also responds to TCP or UDP packets that include IP options that are destined to a local circuit address, or require that a routing decision be made.

To disable the processing of frames with the record-route option (the default behavior), enter:

```
(config)# no ip record-route
```

## Configuring Box-to-Box Redundancy

Use the **ip redundancy** command to enable box-to-box redundancy. Box-to-box redundancy provides chassis-level redundancy between two identically configured CSSs. Refer to the *Cisco Content Services Switch Advanced Configuration Guide* for information about configuring box-to-box redundancy.

The CSS does not support simultaneous box-to-box redundancy and VIP or interface redundancy configurations.

For example:

```
(config)# ip redundancy
```

To disable box-to-box redundancy, enter:

```
(config)# no ip redundancy
```

## Configuring IP Equal-Cost Multipath

Use the **ip ecmp** command to set the equal-cost multipath (ECMP) selection algorithm and the preferred reverse egress path. The CSS supports a maximum of 15 ECMP paths.

The syntax for this global configuration command is:

```
ip ecmp [address|no-prefer-ingress|roundrobin]
```

The options for this global configuration mode command are as follows:

- **address** - Choose among alternate paths based on IP addresses. For example:

```
(config)# ip ecmp address
```

- **no-prefer-ingress** - Do not prefer the ingress path of a flow for its reverse egress path. By default, the ingress path for a flow is the preferred egress path. This means that the preferred interface over which to reply to a client is the interface on which the CSS originally received the request from the client. For example:

```
(config)# ip ecmp no-prefer-ingress
```

To reset the ingress path of a flow for its preferred reverse egress path, enter:

```
(config)# no ip ecmp no-prefer-ingress
```

- **roundrobin** - Alternate between equal paths in roundrobin fashion. For example:

```
(config)# ip ecmp roundrobin
```



### Note

The CSS applies the ECMP selection algorithm for non-TCP/UDP packets (for example, ICMP) on a packet-by-packet basis. Multipath selection for TCP and UDP is performed on a per-flow basis, and all packets for a particular flow take the same path.

## Forwarding IP Subnet Broadcast Addressed Frames

Use the **ip subnet-broadcast** command to enable the CSS to forward subnet broadcast addressed frames.

For example:

```
(config)# ip subnet-broadcast
```

To disable forwarding of subnet broadcast addressed frames (the default behavior), enter:

```
(config)# no ip subnet-broadcast
```



### Caution

Enabling the CSS to forward the subnet broadcast can make the subnet susceptible to “smurf” attacks; an attacker sends an ICMP echo request frame using a subnet broadcast address as a destination and a forged address as the source.

If a “smurf” attack is successful, all the destination subnet hosts reply to the echo and flood the path back to the source. By disabling subnet broadcast forwarding, the original echo never reaches the hosts.

## Configuring IP Unconditional Bridging

By default, the routing table lookup of a destination path by the CSS on received packets overrides bridging decisions to be made for those packets. If the routing table specifies that the CSS use a different physical Ethernet port than what is specified for port bridging, the CSS ignores the bridging decision. If you have a network that you want to bridge through the CSS to an upstream router, you may want to force the CSS to make a bridging decision on the received packets instead of making a routing table decision.

Use the **ip uncond-bridging** global configuration command to always make a bridging decision on the received packets. With this command, the bridging decision always takes precedence over a routing table decision.

For example:

```
(config)# ip uncond-bridging
```

To restore the default behavior of the CSS, enter:

```
(config)# no ip uncond-bridging
```

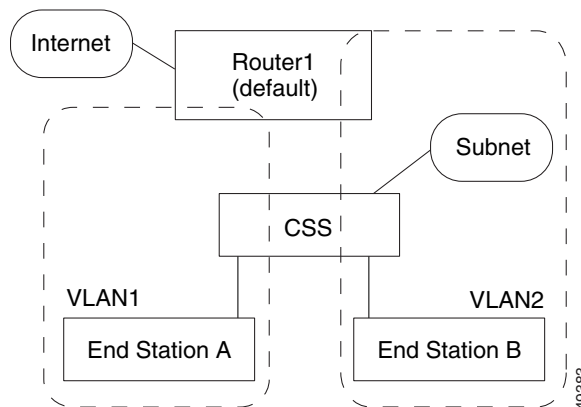
## Configuring IP Opportunistic Layer 3 Forwarding

The CSS opportunistic Layer 3 forwarding feature allows the CSS to reduce the number of network device hops for certain packets or flows. The CSS forwards packets at Layer 3 if the destination MAC address in the Ethernet header is the CSS MAC address. Use the **ip opportunistic** command to enable opportunistic Layer 3 forwarding and allow the CSS to make Layer 3 forwarding decisions even if the Layer 2 packet destination MAC address does not belong to the CSS.

For example, [Figure 6-1](#) shows a CSS connected to VLAN1 and VLAN2. Each VLAN has an end station and an uplink to Router1. End stations A and B both point to Router1 as their default router. When End Station A transmits a packet to End Station B, it uses its default route to Router1. The packet contains Router1's destination MAC address. A traditional Layer 2 device forwards the packet to Router1, and Router1 forwards the packet to End Station B on VLAN2.

Using opportunistic Layer 3 forwarding, the CSS inspects the IP packet header to determine the destination IP address. Instead of forwarding the packet to Router1, the CSS forwards the packet directly to End Station B. Because the CSS handles the packet only once, the router and uplink are not used and network resources are conserved.

**Figure 6-1** Example of Opportunistic Layer 3 Forwarding



The options for this global configuration mode command are as follows:

- **local (default)** - Applies opportunistic Layer 3 forwarding if the destination IP address belongs to a node that resides on one of the subnets directly attached to the CSS *and* the CSS is aware of an ARP resolution for that node. Because the local option is the default, use the **no ip opportunistic** command to reconfigure IP opportunistic Layer 3 forwarding to the local setting.
- **all** - Applies opportunistic Layer 3 forwarding if the destination IP address matches any entry in the CSS routing table. We do not recommend this option if the topology includes multiple routers and the CSS does not know all of the routes the routers are aware of.
- **disabled** - The CSS does not perform opportunistic Layer 3 forwarding. Regular Layer 3 forwarding is performed only for packets that contain the CSS destination MAC address.

For example, to configure IP opportunistic Layer 3 forwarding to **all**, enter:

```
(config)# ip opportunistic all
```

To reconfigure IP opportunistic Layer 3 forwarding to the default of **local** enter:

```
(config)# no ip opportunistic
```

When you configure **ip opportunistic all**, you can use the **ip route originated-packets** command (see the “[Configuring an IP Route](#)” section) to configure routes that the CSS uses to reach devices, but does not use as opportunistic routes for forwarding traffic. Routes created using the **ip route originated-packets** command apply only to packets that originate on the CSS. Packets and flows forwarded by the CSS do not use these routes.

For example:

```
(config)# ip route 0.0.0.0 /0 192.168.1.7 originated-packets
```

## Showing IP Configuration Information

Use the **show ip** command to display IP information for the CSS. This section includes the following topics:

- [Showing IP Global Configuration Parameters](#)
- [Showing IP Interface Information](#)
- [Showing IP Routing Information](#)
- [Showing IP Statistics](#)
- [Showing a Summary of IP Global Statistics](#)

### Showing IP Global Configuration Parameters

Use the **show ip config** command to display IP global configuration parameters. These parameters show the state (enabled or disabled) of the source route option, forward IP broadcasts, record-route option, and IP route change logging. The **show ip config** command also shows the value for the orphaned route timer.

[Table 6-8](#) describes the fields in the **show ip config** output.

**Table 6-8** *Field Descriptions for the show ip config Command*

Field	Description
Source Route Option	Indicates whether processing of source-routed frames is enabled or disabled.
Forward IP Broadcasts	Indicates whether forwarding IP broadcasts is enabled or disabled.
Orphaned Route Timer	The setting for the orphaned route timer.
Record Route Option	Indicates whether processing with the record-route option is enabled or disabled.

**Table 6-8** Field Descriptions for the `show ip config` Command (continued)

Field	Description
Multiple Equal Cost Path Algorithm	The setting for the equal-cost multipath selection algorithm. The possible settings are as follows: <ul style="list-style-type: none"> <li>• <b>Address</b> - Choose among alternate paths based on IP addresses</li> <li>• <b>Roundrobin</b> - Alternate between equal paths in roundrobin fashion</li> </ul>
IP Route Change Logging	Indicates whether logging IP route changes is enabled or disabled.

## Showing IP Interface Information

Use the `show ip interfaces` command to display configured IP interfaces on the CSS. The display includes the circuit state, IP address, broadcast address, Internet Control Message Protocol (ICMP) settings, and Router Discovery Program (RDP) settings.

[Table 6-9](#) describes the fields in the `show ip interfaces` command output.

**Table 6-9** Field Descriptions for the `show ip interfaces` Command

Field	Description
Circuit Name	The name of the circuit associated with the IP interface.
State	The state of the IP interface. The possible states are as follows: <ul style="list-style-type: none"> <li>• <b>Active (1)</b> - Interface is up</li> <li>• <b>Disabled (2)</b> - Interface is disabled</li> <li>• <b>NoCircuit (3)</b> - Interface is waiting for an underlying circuit</li> </ul>
IP Address	The IP address assigned to the circuit.
Network Mask	The network mask of the circuit.

**Table 6-9** Field Descriptions for the `show ip interfaces` Command (continued)

Field	Description
Broadcast Address	The broadcast IP address associated with the IP interface. If left at zero, the all-ones host is used for numbered interfaces. 255.255.255.255 is always used for unnumbered interfaces.
Redundancy	Indicates whether the redundancy protocol is running on the interface. The default state is Disabled.
ICMP Redirect	Whether the transmission of Internet Control Message Protocol (ICMP) redirect messages is enabled or disabled. The default state is Enabled.
ICMP Unreachable	Whether the transmission of ICMP Destination Unreachable messages is enabled or disabled. The default state is enabled.
RIP	Whether RIP is enabled or disabled.

## Showing IP Routing Information

Use the `show ip routes` command to display IP routing information. The syntax and options for this command are as follows:

- `show ip routes` - Displays the entire routing table, including host IP address, next hop, interface, route type, protocol, age (in seconds), and metric.
- `show ip routes firewall` - Displays all firewall routes.
- `show ip routes local` - Displays all local routes.
- `show ip routes ospf` - Displays all OSPF routes.
- `show ip routes rip` - Displays all RIP routes.
- `show ip routes static` - Displays all static routes.
- `show ip routes summary` - Displays the total number of OSPF routes (including a breakdown of Intra, Inter, and Ext routes), RIP routes, local routes, static routes, and firewall routes.
- `show ip routes ip_or_host {to ip_or_host | mask_or_prefix}` - Displays information about a route to a destination, a specific route, or routes in a range.

The variables are as follows:

- *ip\_or\_host* - The IP address of the host or network prefix. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1). The IP address after the **to** keyword is the final IP address in a range.
- *mask\_or\_prefix* - Subnet address of the specific network. Enter the subnet address in mask or prefix notation (for example, /24).

To show all IP routes in the CSS, enter:

```
# show ip routes
```

Table 6-10 describes the fields in the **show ip routes** command output.

**Table 6-10 Field Descriptions for the show ip routes Command**

Field	Description
Prefix/length	The IP address and prefix length for the route.
Next hop	The IP address for the next hop.
If	The Index value that identifies the local interface through which the next hop of this route should be reached.
Type	The type of the route entry. The possible types are as follows: <ul style="list-style-type: none"> <li>• local - Local interface</li> <li>• remote - Remote destination</li> <li>• mgmt - Management interface</li> </ul>
Proto	The protocol for the route.
Age	The maximum age of the route.
Metric	The metric cost of the route.

## Showing IP Statistics

Use the **show ip statistics** command to display aggregate TCP statistics for the unit. [Table 6-11](#) describes the fields in the **show ip statistics** output.

**Table 6-11 Field Descriptions for the show ip statistics Command**

Field	Description
<b>UDP Statistics</b>	
Input Datagrams	The total number of flow-related UDP datagrams delivered to UDP users.
No Port Errors	The total number of received UDP datagrams for which there was no application at the destination port.
Output Datagrams	The total number of flow-related UDP datagrams sent from the CSS.
Input Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
<b>TCP Statistics</b>	
Retransmit Algorithm	The algorithm used to determine the timeout value for retransmitting unacknowledged octets.
Max Retransmit Time	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the Closed state.
Failed Attempts	The number of times TCP connections have made a direct transition to the Closed state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the Listen state from the SYN-RCVD state.
Established Conns	The number of TCP connections for which the current state is either Established or Close-Wait.

**Table 6-11 Field Descriptions for the show ip statistics Command (continued)**

<b>Field</b>	<b>Description</b>
Output Segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Input Errors	The total number of segments received in error (for example, bad TCP checksums).
Min Retransmit Time	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
Max TCP Connections	The total number of TCP connections that the CSS supports.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Resets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Input Segments	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Retransmit Segments	The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Output Resets	The number of TCP segments sent containing the RST flag.
<b>ICMP Statistics</b>	
Echo Requests In	The number of received ICMP Echo request messages. Typically, when the CSS receives the ICMP request, both the Echo Requests In and the Echo Replies Out counters increment as a pair for the ICMP request in and ICMP reply out packets.

**Table 6-11** Field Descriptions for the `show ip statistics` Command (continued)

Field	Description
Echo Replies In	The number of received ICMP Echo reply messages. Typically, when the CSS receives an ICMP reply, both the Echo Requests Out and the Echo Replies In counters increment as a pair for the ICMP reply in and ICMP request out packets.
Unreachable	The number of received ICMP Destination Unreachable messages.
Redirect	The number of received ICMP Redirect messages.
Router Solicit	The number of received ICMP router solicitation packets.
Param Problem	The number of received ICMP Parameter Problem messages.
Timestamp Reply	The number of sent ICMP Timestamp Reply messages.
Information Reply	The number of received ICMP information reply packets.
Mask Reply	The number of received ICMP Address Mask Reply messages.
Echo Requests Out	The number of transmitted ICMP Echo request messages. Typically, when the CSS transmits an ICMP request, both the Echo Requests Out and the Echo Replies In counters increment as a pair for the ICMP request out and ICMP reply in packets.
Echo Replies Out	The number of transmitted ICMP Echo reply messages. Typically, when the CSS transmits an ICMP reply, both the Echo Requests In and the Echo Replies Out counters increment as a pair for the ICMP reply out and ICMP request in packets.
Source Quench	The number of received ICMP Source Quench messages.
Router Adv	The number of received ICMP router advertisement packets.

**Table 6-11** Field Descriptions for the `show ip statistics` Command (continued)

<b>Field</b>	<b>Description</b>
Time Exceeded	The number of received ICMP Time Exceeded messages.
Timestamp	The number of sent ICMP Timestamp (request) messages.
Information Request	The number of received ICMP information request packets.
Mask Request	The number of sent ICMP Address Mask Request messages.
Invalid	The number of received bad ICMP type packets.
<b>ARP Statistics</b>	
Requests In	The number of received ARP request packets.
Requests Out	The number of sending ARP request packets.
Duplicate Addr	The number of received ARP packets with a detected duplicate IP address. The duplicate IP address can be the local IP address, VIP, or virtual interface.
Invalid	The number of invalid or bad ARP packets.
Replies In	The number of received ARP reply packets.
Replies Out	The sending ARP reply packet count.
In Off Subnet	The number of received ARP packets with sender or target addresses outside of the subnet range of the receiving interface.
Unresolved	The number of processed IP frames with unresolved next hop MAC addresses.

## Showing a Summary of IP Global Statistics

Use the **show ip summary** command to display a summary of IP global statistics. The statistics include data on reachable and total routes, reachable and total hosts, memory in use for each, and total IP routing memory in use.

[Table 6-12](#) describes the fields in the **show ip summary** command output.

**Table 6-12** *Field Descriptions for the show ip summary Command*

Field	Description
Reachable Routes	The current number of reachable routes.
Total Routes	The current number of routes maintained, both reachable and unreachable.
Reachable Hosts	The current number of reachable host entries.
Total Hosts	The current number of host entries, both reachable and unreachable.
Total Memory in use - IP Routing Memory Pool	The total amount of memory in bytes allocated for the IP routing table. When there are no additional free entries in the memory pool, more memory is allocated to the pool.

# Configuring the Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a medium-independent protocol that runs over Layer 2 (the data link layer) on the CSS and other Cisco manufactured equipment, such as routers, switches, bridges, and access servers. Use the **cdp** global configuration command to allow the CSS to advertise itself to all other neighboring Cisco CDP-compatible devices on a network. The CSS transmits CDP advertisements to other CDP-compatible devices on the network; the CSS does not listen for CDP messages from the other CDP-compatible devices.

Any Cisco device with CDP support can learn about the CSS by listening to the periodic messages transmitted by the CSS and determining when the CSS is active. Network operators and analysts can use this information for configuration monitoring, topology discovery, and fault diagnosis.

CDP messages contain specific information about the CSS, such as:

- Device ID (CSS base MAC address)
- IP address (CSS management port IP address)
- Ethernet port ID name
- CSS functional capability flag (Router, Transparent Bridge, or Switch)
- CSS software version
- CSS platform

CDP advertisements also include hold time information, which defines the length of time the receiving device is to hold CDP information before discarding it.

This section includes the following topics:

- [Enabling CDP](#)
- [Setting the CDP Hold Time](#)
- [Setting the CDP Transmission Rate](#)
- [Showing CDP Information](#)

## Enabling CDP

Use the **cdp run** global configuration command to enable CDP transmissions from the CSS to other neighboring Cisco CDP-compatible devices on the network. By default, CDP is disabled for the CSS.

For example:

```
(config)# cdp run
```

To disable CDP transmissions on the CSS, enter:

```
(config)# no cdp run
```

## Setting the CDP Hold Time

Use the **cdp holdTime** global configuration command to specify the amount of time a receiving device retains the CDP information sent by the CSS (time-to-live information) before discarding this information. If a neighboring device does not receive a CDP message before the hold time expires, the neighboring device drops the CSS as a neighbor. Valid entries are 10 to 255 seconds. The default is 180 seconds.

To specify a CDP hold time of 255 seconds for the receiving device, enter:

```
(config)# cdp holdTime 255
```

To reset the CDP hold time back to the default value of 180 seconds, enter:

```
(config)# no cdp holdTime
```

## Setting the CDP Transmission Rate

Use the **cdp timer** global configuration command to specify the frequency at which the CSS transmits CDP packets to all receiving CDP-compatible devices. Valid entries are 5 to 254 seconds. The default is 60 seconds.

To change the CDP transmission rate for the CSS to 120 seconds, enter:

```
(config)# cdp timer 120
```

To reset the CDP timer to the default rate of 60 seconds, enter:

```
(config)# no cdp timer
```

## Showing CDP Information

Use the **show cdp** command to display and verify CDP information for the CSS, such as frequency of transmissions and the hold time for transmitted CSS CDP information.

For example:

```
(config)# show cdp

Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 16 seconds
  TimeLastCdpSent: 0 days 00:00:30
```

The following example illustrates the CDP output on a Cisco Catalyst 8540 router using the Cisco IOS **show cdp neighbors** command.

```
24-8540-1>show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S -
Switch, H - Host, I - IGMP, r - Repeater

Device ID           Local Intrfce  Holdtme  Capability  Platform  Port ID
00-10-58-01-4d-e3   Eth 0          178      R T S       CSS 11501  Eth-Mgmt
SCA043801A5         Eth 0          144      T S         WS-C6009  3/1
25-8540-1           Fas 0/0/7      142      R T         C8540CSR  Fas 0/0/4
25-8540-1           Eth 0          142      R T         C8540CSR  Eth 0
SCA043801HU(bxb11  Eth 0          151      T S         WS-C6009  2/48
00-07-85-43-14-1d  Eth 0          170      R T S       CSS11503  Eth-Mgmt
```

# Configuring Spanning-Tree Bridging for the CSS

The CSS supports configuration of Spanning-Tree Protocol (STP) bridging. Spanning-tree bridging detects, and then prevents, loops in the network. Use the **bridge** command to configure global spanning-tree bridging options for the CSS, such as bridge aging time, forward delay time, hello time interval, and maximum age. Make sure you configure the spanning-tree bridging parameters the same on all switches running STP in the network.



## Note

When connecting a Cisco Catalyst switch to a CSS using an 802.1Q trunk and the STP, the Catalyst runs a spanning-tree instance for each VLAN. When you configure an 802.1Q trunk on an Ethernet interface for the Catalyst switch, the bridge protocol data units (BPDUs) are tagged with the corresponding VLAN ID and the destination MAC address changes from the standard 01-80-C2-00-00-00 to the proprietary 01-00-0c-cc-cc-cd. This modification allows Cisco switches operating in a non-Cisco (a mix of other vendors) 802.1Q trunk environment to maintain spanning-tree states for all VLANs. Although the CSS maintains a spanning-tree instance for each VLAN as well, the CSS uses the standard 01-80-C2-00-00-00 destination MAC address for all BPDUs (tagged or untagged). When you connect a Cisco Catalyst switch to a CSS over an 802.1Q trunk, the result is that neither switch recognizes the other's BPDUs, and both assume root status. If a spanning-tree loop is detected, the Catalyst switch goes into blocking mode on one of its looped ports.

This section includes the following topics:

- [Configuring Spanning-Tree Bridge Aging-Time](#)
- [Configuring Spanning-Tree Bridge Forward-Time](#)
- [Configuring Spanning-Tree Bridge Hello-Time](#)
- [Configuring Spanning-Tree Bridge Max-Age](#)
- [Configuring Spanning-Tree Bridge Priority](#)
- [Disabling Bridge Spanning-Tree](#)
- [Showing Bridge Configurations](#)

For details about configuring spanning-tree bridging parameter for an Ethernet interface or for a trunked Ethernet interface and VLAN pair, refer to [Chapter 5, Configuring Interfaces and Circuits](#).

## Configuring Spanning-Tree Bridge Aging-Time

Use the **bridge aging-time** command to set the bridge filtering database aging time for the CSS. The aging time is the timeout period, in seconds, for aging out dynamically learned forwarding information. Enter an integer from 10 to 1000000. The default is 300.

To set the bridge aging time to 600, enter:

```
(config)# bridge aging-time 600
```

To restore the default aging time of 300, enter:

```
(config)# no bridge aging-time
```

## Configuring Spanning-Tree Bridge Forward-Time

Use the **bridge forward-time** command to set the bridge forward delay time. The forward time is the delay time, in seconds, that all bridges use for forward delay when this bridge is acting as the root. Enter an integer from 4 to 30. The default is 4.

To set the bridge forward time to 9, enter:

```
(config)# bridge forward-time 9
```

To restore the default delay time of 4, enter:

```
(config)# no bridge forward-time
```

## Configuring Spanning-Tree Bridge Hello-Time

Use the **bridge hello-time** command to set the bridge hello time interval. The hello time is the time, in seconds, that all bridges wait before sending a hello packet (when the bridge acts as the root). Enter an integer from 1 to 10. The default is 1.

To set the bridge hello time to 9, enter:

```
(config)# bridge hello-time 9
```

To restore the default hello time interval of 1, enter:

```
(config)# no bridge hello-time
```

## Configuring Spanning-Tree Bridge Max-Age

Use the **bridge max-age** command to set the bridge spanning-tree maximum age. The maximum age is the time, in seconds, that protocol information received on a port is stored by the CSS (when a bridge acts as the root). Enter an integer from 6 to 40. The default is 6.

**Note**

Ensure the bridge maximum age is greater than or equal to 2 times (bridge hello-time + 1 second) and less than or equal to 2 times (bridge forward-time - 1 second).

To set the bridge maximum age to 21, enter:

```
(config)# bridge max-age 21
```

To restore the default maximum age of 6, enter:

```
(config)# no bridge max-age
```

## Configuring Spanning-Tree Bridge Priority

To set the priority that spanning tree uses to choose the root bridge in the network, use the global **bridge priority** command. In spanning tree, the 2-octet field is prepended to the 6-octet MAC address to form an 8-octet bridge identifier. The device with the lowest bridge identifier is considered the highest priority bridge and becomes the root bridge. The range for bridge priority is 0 to 65535. The default is 32768.

For example:

```
(config)# bridge priority 1700
```

To restore the bridge priority to the default of 32768, enter:

```
(config)# no bridge priority
```

## Disabling Bridge Spanning-Tree

Spanning-tree bridging is enabled by default. When you disable spanning-tree bridging, the CSS forwards all multicast traffic, including bridge protocol data units (BPDUs) for the bridge multicast group and for trunked VLANs. The CSS can still operate in an 802.1Q spanning-tree environment as long as you do not require that the CSS put any of its ports into a blocking state.

To disable spanning-tree bridging, enter:

```
(config)# bridge spanning-tree disable
```



### Caution

Disabling spanning-tree bridging may make your network susceptible to packet storms.

To reenable spanning-tree bridging, enter:

```
(config)# bridge spanning-tree enable
```

## Showing Bridge Configurations

Use the **show bridge forwarding** command to display bridge forwarding information. [Table 6-13](#) describes the fields in the **show bridge forwarding** command output.

**Table 6-13** Field Descriptions for the *show bridge forwarding* Command

Field	Description
VLAN	The bridge interface virtual LAN number
MAC Address	The MAC address for the entries
Port Number	The port number used for bridge forwarding

Use the **show bridge status** command to display bridge status information. [Table 6-14](#) describes the fields in the **show bridge status** output.

**Table 6-14 Field Descriptions for the show bridge status Command**

Field	Description
STP State	The state of the Spanning-Tree Protocol: Enabled or Disabled.
Root Max Age	The timeout period, in seconds, during which the host times out root information.
Root Hello Time	The interval, in seconds, during which the root bridge broadcasts its hello message to other devices.
Root Fwd Delay	The delay time, in seconds, that the root bridge uses for forward delay.
Designated Root	The bridge ID for the designated root.
Bridge ID	The bridge ID of the bridge.
Port	The port ID.
State	<p>The state of the port. The possible states are as follows:</p> <ul style="list-style-type: none"> <li>• Block - The blocking state. A port enters the blocking state after CSS initialization. The port does not participate in frame forwarding.</li> <li>• Listen - The listening state. This state is the first transitional state a port enters after the blocking state. The port enters this state when STP determines that the port should participate in frame forwarding.</li> <li>• Learn - The learning state. The port enters the learning state from the listening state. The port in the learning state prepares to participate in frame forwarding.</li> <li>• Forward - The forwarding state. The port enters the forwarding state from the learning state. A port in the forwarding state forwards frames.</li> <li>• Disabled - The disabled state. A port in the disabled state does not participate in frame forwarding or the Spanning-Tree Protocol. A port in the disabled state is non operational.</li> </ul>

**Table 6-14** Field Descriptions for the `show bridge status` Command (continued)

Field	Description
Designated Bridge	The bridge ID for the designated bridge.
Designated Root	The bridge ID for the designated root.
Root Cost	The cost of the root.
Port Cost	The cost of the port.
Desg Port	Designated port.

## Configuring the DHCP Relay Agent

The Dynamic Host Configuration Protocol (DHCP) servers provide configuration parameters to DHCP clients. When DHCP clients and associated servers do not reside on the same IP network or subnet, a DHCP relay agent can transfer DHCP messages between them. To configure a DHCP relay agent on a CSS, define DHCP server destinations on a circuit and enable the DHCP relay agent on the circuit.

You must first assign an IP address on the circuit to be able to configure the DHCP relay agent for the circuit. Use the **ip address** command in the specific circuit mode to assign the IP address and a subnet mask. For example:

```
(config-circuit[VLAN2])# ip address 178.3.6.53/8
```

This section includes the following topics:

- [Adding a DHCP Destination on a Circuit](#)
- [Enabling and Disabling DHCP on the Circuit](#)
- [Defining the Hops Field Value for Forwarding DHCP Messages](#)
- [Displaying the DHCP Relay Configuration](#)

## Adding a DHCP Destination on a Circuit

A CSS circuit acts as the DHCP relay agent. For each circuit on the CSS, you can configure a maximum of five DHCP destinations. The initial DHCP broadcast request is sent to all of the configured destinations.

Do not configure a relay destination on a circuit when the relay destination is directly connected to or reachable from one of the ports on the same circuit. In this case, the DHCP packets reach the relay destination through normal broadcast and a relay agent is not required.

Use the **dhcp relay-to** command to specify the DHCP relay destination address. This command is available in circuit configuration mode. Enter an IP address in dotted-decimal notation.

For example, to add a destination address of 192.168.22.25 to a DHCP server, enter:

```
(config-circuit[VLAN2])# dhcp relay-to 192.168.22.25
```

To remove the relay destination address, enter:

```
(config-circuit[VLAN2])# no dhcp relay-to 192.168.22.25
```

## Enabling and Disabling DHCP on the Circuit

After you enable the DHCP relay agent on the CSS circuit, the CSS transfers DHCP messages between DHCP clients and servers. Use the **dhcp-relay-agent** command to enable the agent on the circuit. This command is available in circuit configuration mode.

For example:

```
(config-circuit[VLAN2])# dhcp-relay-agent
```

To disable the DHCP relay agent on the circuit, enter:

```
(config-circuit[VLAN2])# no dhcp-relay-agent
```

## Defining the Hops Field Value for Forwarding DHCP Messages

The CSS forwards or discards a DHCP message based on the hops field value in the BOOTP header. When messages have values in the hops fields that exceed the maximum value set on the CSS, the CSS discards the message. Use the **dhcp-agent max-hops** global configuration command to set the maximum allowable number in the hops field. By default, the maximum allowable number is 4. You can set a number from 1 to 15.

For example, to set the maximum allowable value of 10, enter:

```
(config)# dhcp-agent max-hops 10
```

To reset the maximum allowable number in the hops field to the default of 4, enter:

```
(config)# no dhcp-agent max-hops
```

## Displaying the DHCP Relay Configuration

Use the **show dhcp-relay-agent global** command to display the DHCP configuration information on a CSS. This command is available in all modes. For example:

```
# show dhcp-relay-agent global
```

[Table 6-15](#) describes the fields in the **show dhcp-relay-agent global** command output.

**Table 6-15** Field Descriptions for the show dhcp-relay-agent global Command

Field	Description
Max Hops	The maximum allowable number in the hops field of the BOOTP header. The CSS does not forward packets with headers that contain a larger number.
Number of circuits configured for DHCP	The number of CSS circuits configured for DHCP.
Circuit	The circuit configured for DHCP.
IfAddress	The interface address for the circuit.

**Table 6-15** Field Descriptions for the *show dhcp-relay-agent global* Command

Field	Description
DHCP State	The DHCP relay agent state on the circuit (Enabled or Disabled).
Relay destination	The DHCP relay destination address for the server. Each circuit can have five destination addresses.

## Where to Go Next

[Chapter 7, Configuring Open Shortest Path First \(OSPF\)](#) describes how to configure and view information for the OSPF protocol.

■ Where to Go Next