



CHAPTER 2

Configuring Routes on the ACE

This chapter describes how the ACE is considered a router hop in the network when it is in routed mode. In the Admin or user contexts, the ACE supports static routes only. The ACE supports up to eight equal cost routes for load balancing.

This chapter describes how to configure a default or static route on the ACE and contains the following major sections:

- [Assigning an IP Address to Interfaces for a Routing Traffic](#)
- [Configuring a Default or Static Route](#)
- [Removing a Default or Static Route](#)
- [Advertising a VLAN for RHI](#)
- [Verifying Connectivity of a Remote Host or Server](#)
- [Displaying IP Route Information](#)
- [Displaying FIB Table Information](#)

Assigning an IP Address to Interfaces for a Routing Traffic

When you assign an IP address on an interface, its mode automatically becomes routed. To assign an IP address to a VLAN interface, use the **ip address** command in interface configuration mode. The syntax of this command is as follows:

```
ip address ip_address mask
```

The *ip_address mask* arguments specify the IP address and mask for the VLAN interface.

For detailed information on configuring an IP address on an interface, see [Chapter 1, “Configuring VLAN Interfaces.”](#)

For example, to set the IP address of 192.168.1.1 255.255.255.0 for VLAN interface 200, enter:

```
host1/Admin(config)# interface vlan 200  
host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
```

If you make a mistake while entering this command, you can reenter the command with the correct information.

Configuring a Default or Static Route

Admin and user contexts do not support dynamic routing. You must use static routes for any networks to which the ACE is not directly connected; for example, you must use a static route when there is a router between a network and the ACE.

For traffic that originates on or is routed through the ACE and is destined for a nondirectly connected network, configure either a default route or static routes so that the ACE knows where to send the traffic. Traffic that originates on the ACE might include communications to a syslog server, Websense or N2H2 server, or AAA server.

The simplest option is to configure a default route to send all traffic to an upstream router. The default route identifies the router IP address where the ACE sends all IP packets for which it does not have a route.

**Note**

Routes that identify a specific destination address take precedence over the default route.

To set a default or static route, use the **ip route** command in configuration mode. The syntax of this command is as follows:

```
ip route dest_ip_prefix netmask gateway_ip_address
```

The keywords, arguments, and options are as follows:

- *dest_ip_prefix*—IP address for the route. Enter the address in dotted-decimal IP notation (for example, 192.168.20.1).
- *netmask*—Subnet mask for the route. Enter the subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- *gateway_ip_address*—IP address of the gateway router (the next-hop address for this route). The gateway address must be in the same network as specified in the **ip address** command for a VLAN interface. For information on configuring the address, see the [“Assigning an IP Address to Interfaces for a Routing Traffic”](#) section.

**Note**

When you configure a default gateway, the MAC address of the gateway must not constantly change. We recommend to use a Hot Standby Router Protocol (HSRP) IP address or other virtual IP address which maintains a single MAC address for multiple interfaces.

**Note**

Management traffic coming into the ACE is not affected by the **no normalization** command, which does not support asymmetric routes. For information about normalization, see the *Cisco Application Control Engine Module Security Configuration Guide*.

For example, to configure a static route to send all traffic destined for 10.1.1.0/24 to the router (10.1.2.45), enter:

```
host1/Admin(config)# ip route 10.1.1.0 255.255.255.0 10.1.2.45
```

To configure a default route, set the IP address and the subnet mask for the route to 0.0.0.0. For example, if the ACE receives traffic that does not have a route and you want the ACE to send the traffic out the interface to the router at 192.168.4.8, enter:

```
host1/Admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.4.8
```

Removing a Default or Static Route

You can remove a default or static IP route from the configuration by using the **no** form of the **ip route** command. For example, enter:

```
host1/Admin(config)# no ip route 192.168.42.0 255.255.255.0  
192.168.1.5 1
```

Advertising a VLAN for RHI

To advertise a VLAN for route health injection (RHI) that is different from the VIP interface VLAN, use the **ip route inject vlan** command in interface configuration mode. By default, the ACE advertises the VLAN of the VIP interface for RHI.

Use this command when there is no directly shared VLAN between the ACE and the Catalyst 6500 series supervisor engine. This topology can occur when there is an intervening device, for example, a Cisco Firewall Services Module (FWSM), configured between the ACE and the supervisor engine.

**Note**

Be sure to configure this command on the VIP interface of the ACE.

The syntax of this command is as follows:

```
ip route inject vlan vlan_id
```

The *vlan_id* is the interface shared between the supervisor engine and the intervening device. Enter it as an integer from 2 to 4090.

For example, to advertise route 200 for RHI, enter:

```
host1/Admin(config-if) # ip route inject vlan 200
```

To restore the ACE default behavior of advertising the VIP interface VLAN for RHI, enter:

```
host1/Admin(config-if) # no ip route inject vlan 200
```

Verifying Connectivity of a Remote Host or Server

You can verify the connectivity of a remote host or server by using the **ping** command in Exec mode to send echo messages from the ACE.

The syntax of this command is as follows:

```
ping system_address [count count [size size [timeout time]]]
```

The arguments and options are as follows:

- *system_address*—IP address of a remote host or server to ping. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10). If you do not specify the IP address of the remote host, the CLI prompts you for the information. For information on additional prompts, see [Table 2-1](#).
- **count** *count*—(Optional) Specifies the repeat count. Enter the repeat count as an integer from 1 to 65000. The default is 5.
- **size** *size*—(Optional) Specifies the datagram size. Enter the datagram size as an integer from 36 to 1440. The default is 100.
- **timeout** *time*—(Optional) Specifies the timeout in seconds. Enter the timeout value as an integer from 0 to 3600. The default is 2.

The following example shows how to send a ping to a server located at IP address 192.168.219.140:

```
host1/Admin# ping 192.168.173.140
PING 192.168.173.140 with timeout = 2, count = 5, size = 100
Response from 192.168.173.140 : seq 1 time 1.213 ms
Response from 192.168.173.140 : seq 2 time 0.175 ms
Response from 192.168.173.140 : seq 3 time 0.210 ms
Response from 192.168.173.140 : seq 4 time 0.162 ms
Response from 11.1.11.4 : seq 5 time 0.214 ms
5 packet sent, 5 responses received, 0% packet loss
```

To abnormally terminate a ping session, press **Ctrl-C**.


Note

The first ping may fail because the ARP table is not populated with the MAC address for the remote host or server.

The **ping** command provides additional options to verify the connectivity of a remote host or server. To specify these additional parameters, type **ping** at the CLI ACE prompt and press enter.

[Table 2-1](#) summarizes the options and the defaults for the **ping** command.

Table 2-1 Options and Defaults for the ping Command

Option	Description	Default
Target IP address	IP address or hostname of the destination node to ping.	Not applicable
Repeat count	Number of ping packets to be sent to the destination address.	5 packets
Datagram size	Size of each ping packet in bytes.	100 bytes
Timeout in seconds	Timeout interval after which a ping request is considered a failure. The ping is not aborted and sends the next ping packet, if any.	2 seconds
Extended commands	Specifies whether a series of additional commands appear.	No

Table 2-1 Options and Defaults for the ping Command (continued)

Option	Description	Default
Source address or interface	Numeric IP address or the name of the source interface.	Not applicable
Set DF bit in IP header	Path MTU Discovery strategy.	No
Time to Live	Value of the TTL field in the IP header that determines how long the ping packet exists before being discarded. The TTL value is reduced by one unit at each hop.	128

To trace the routes taken for a specified IP address, use the **tracert** command in Exec mode.

The syntax of this command is as follows:

```
tracert [ip_address [size packet]]
```

The arguments and option are as follows:

- *ip_address*—IP address for the route. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10). This argument is optional if you do not include it with the command. You are prompted for an IP address.
- *size packet*—(Optional) Specifies the packet size. Enter a number from 40 to 452. The default is 40.

For example, to trace the IP address 192.168.173.140, enter:

```
host1/Admin# tracert 192.168.173.140
tracert to 192.168.173.140 (192.168.173.140), 30 hops max, 40 byte
packets
 1 192.86.215.2 (192.86.215.2) 0.558 ms 0.325 ms 0.297 ms
 2 * * *
 3 * * *
```

To terminate a tracert session, press **Ctrl-C**.

Using Traceroute on the ACE-Configured IP Addresses

You can use traceroute on ACE-configured IP addresses, however there are certain restrictions. When you use traceroute to a configured ACE IP interface:

- ICMP traceroute works when you configure a management policy to permit ICMP traffic, similar to the following example:

```
class-map type management match-any remote-access
  description remote-access-traffic-match
  match protocol icmp any
```



Note Most traceroutes use the default protocol of UDP. Use a command line option to change traceroute to ICMP. For example, in Linux, use the `-I` option.

- UDP or TCP-based traceroute does not work. There is no method to permit UDP or TCP traffic to ephemeral ports going to the ACE.

When you use UDP, TCP, or ICMP-based traceroute to a host behind the ACE, it works as expected. However, the ACE does not appear in the traceroute as a hop. The ACE does not decrement the TTL of IP packets that it forwards.

When you use traceroute to a VIP address configured on the ACE, the ACE does not intercept traceroute packets sent to the configured VIP address. The ACE attempts to match the packet to the load-balance policies. If a protocol match occurs, the ACE sends the packet to the real server that responds to the traceroute accordingly.

Displaying IP Route Information

To display IP routes on the ACE, use the **show ip route** command in Exec mode. For example, enter:

```
host1/Admin# show ip route
```

[Table 2-2](#) describes the fields in the **show ip route** command output.

Table 2-2 *Field Description for the show ip route Command*

Field	Description
Destination	Destination address for the route.
Gateway	Gateway address for the route.
Interface	VLAN interface number for this entry.
Flag	Flag to identify the route type and state, as identified by one of the following codes displayed above the output information: <ul style="list-style-type: none"> • H indicates a host route. • I indicates an interface route. • S indicates a static route. • N indicates a NAT route. • A indicates that the route needs an ARP resolve. • E indicates an ECMP route.

To display the route summary for the current context, use the **show ip route summary** command. For example, enter:

```
host1/Admin# show ip route summary
```

[Table 2-3](#) describes the fields in the **show ip route summary** command output.

Table 2-3 *Field Description for the show ip route summary Command*

Field	Description
Route Source	Source of the route. The possible value are as follows: <ul style="list-style-type: none"> • Connected for a route to hosts that are connected to the same network. • Static for a configured route.
Count	Number of routes that are connected or static.
Memory (bytes)	Memory consumed by the route entries.

To display IP traffic information, use the **show ip traffic** command in Exec mode. The syntax of this command is as follows:

show ip traffic

For example, enter:

```
host1/Admin# show ip traffic
```

Table 2-4 describes the fields in the **show ip traffic** command output.

Table 2-4 *Field Descriptions for the show ip traffic Command Output*

Field	Description
IP Statistics	
Rcvd	Total number of packets received by the ACE, number of bytes received by the ACE, number of input errors, number of packets received by the ACE with no route, and number of packets received by the ACE that had an unknown protocol.
Frag	Number of fragments that the ACE reassembled, number of fragments that the ACE could not reassemble, number of packets that the ACE fragmented, and number of packets that the ACE could not fragment.
Bcast	Number of broadcast packets received and sent.
Mcast	Number of multicast packets received and sent.
Sent	Total packets sent, number of bytes sent, and number of packets sent with no route.
Drop	Number of packets discarded because they had no route and number of packets discarded.
ICMP Statistics	

Table 2-4 *Field Descriptions for the show ip traffic Command Output (continued)*

Field	Description
Rcvd	<p>Reports statistics for the following ICMP messages received by the ACE:</p> <ul style="list-style-type: none"> • Redirects • ICMP Unreachable • ICMP Echo • ICMP Echo Reply • Mask Requests • Mask Replies • Quench • Parameter • Timestamp
Sent	<p>Reports statistics for the following ICMP messages sent by the ACE:</p> <ul style="list-style-type: none"> • Redirects • ICMP Unreachable • ICMP Echo • ICMP Echo Reply • Mask Requests • Mask Replies • Quench • Timestamp • Parameter • Time Exceeded
TCP Statistics	
Rcvd	Total number of TCP segments and errors received by the ACE.

Table 2-4 *Field Descriptions for the show ip traffic Command Output (continued)*

Field	Description
Sent	Total number of TCP segments sent by the ACE.
UDP Statistics	
Rcvd	Total number of UDP segments, UDP errors, and segments with no port number received by the ACE.
Sent	Total number of UDP segments sent by the ACE
ARP Statistics	
Rcvd	Number of ARP packets, errors, requests, and responses received by the ACE.
Sent	Number of ARP packets, errors, requests, and responses sent by the ACE.

The **show ip route internal** command is used for debugging purposes. The output of this command is for use by trained Cisco personnel as an aid in debugging and troubleshooting the ACE. For information on the command syntax, see the *Cisco Application Control Engine Module Command Reference*.

Displaying FIB Table Information

The forwarding information base (FIB) table contains information that the forwarding processors require to make IP forwarding decisions. This table is derived from the route and ARP tables. To display the FIB table for the context, use the **show ip fib** command. For example, enter:

```
host1/Admin# show ip fib
```

[Table 2-5](#) describes the fields in the **show ip fib** command output.

Table 2-5 *Field Description for the show ip fib Command*

Field	Description
Destination	Destination address for the route.
Interface	VLAN interface number for this entry.

Table 2-5 *Field Description for the show ip fib Command (continued)*

Field	Description
EncapID	Encapsulation identifier.
Flag	Flag to identify the route type and state, as identified by one of the following codes displayed above the output information: <ul style="list-style-type: none"> • H indicates a host route. • I indicates interface route. • S indicates a static route. • N indicates a NAT route. • A indicates that the route needs an ARP resolve. • E indicates an ECMP route. • V indicates that the route destination matches a class map-defined virtual server.

To display a summary of the FIB table for the context, use the **show ip fib summary** command. For example, enter:

```
host1/Admin# show ip fib summary
```

[Table 2-6](#) describes the fields in the **show ip fib summary** command output.

Table 2-6 *Field Description for the show ip fib summary Command*

Field	Description
Resolved routes	Number of prefixes programmed in mtrie.
Leaves, bytes	Number of mtrie leaf nodes allocated and memory consumed in bytes.
Nodes, bytes	Number of mtrie internal nodes allocated and memory consumed in bytes.
ecmps, bytes	Number of ECMP nodes allocated and memory consumed in bytes.

The **show ip fib** command is used for debugging purposes. The output of this command is for use by trained Cisco personnel as an aid in debugging and troubleshooting the ACE. For information on the command syntax, see the *Cisco Application Control Engine Module Command Reference*.