



Configuring Static and Default Routes

This chapter describes how to configure static and default routes on the ASA and includes the following sections:

- [Information About Static and Default Routes, page 25-1](#)
- [Licensing Requirements for Static and Default Routes, page 25-2](#)
- [Guidelines and Limitations, page 25-2](#)
- [Configuring Static and Default Routes, page 25-2](#)
- [Monitoring a Static or Default Route, page 25-9](#)
- [Configuration Examples for Static or Default Routes, page 25-11](#)
- [Feature History for Static and Default Routes, page 25-13](#)

Information About Static and Default Routes

To route traffic to a nonconnected host or network, you must define a static route to the host or network or, at a minimum, a default route for any networks to which the ASA is not directly connected; for example, when there is a router between a network and the ASA.

Without a static or default route defined, traffic to nonconnected hosts or networks generates the following syslog message:

```
%ASA-6-110001: No route to dest_address from source_address
```

You might want to use static routes in single context mode in the following cases:

- Your networks use a different router discovery protocol from EIGRP, RIP, or OSPF.
- Your network is small and you can easily manage static routes.
- You do not want the traffic or CPU overhead associated with routing protocols.

The simplest option is to configure a default route to send all traffic to an upstream router, relying on the router to route the traffic for you. However, in some cases the default gateway might not be able to reach the destination network, so you must also configure more specific static routes. For example, if the default gateway is outside, then the default route cannot direct traffic to any inside networks that are not directly connected to the ASA.

In transparent firewall mode, for traffic that originates on the ASA and is destined for a nondirectly connected network, you need to configure either a default route or static routes so the ASA knows out of which interface to send traffic. Traffic that originates on the ASA might include communications to a

syslog server, Websense or N2H2 server, or AAA server. If you have servers that cannot all be reached through a single default route, then you must configure static routes. Additionally, the ASA supports up to three equal cost routes on the same interface for load balancing.

Licensing Requirements for Static and Default Routes

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6.

Failover Guidelines

Supports Stateful Failover of dynamic routing protocols.

Additional Guidelines

- IPv6 static routes are not supported in transparent mode in ASDM.
- In clustering, static route monitoring is only supported on the master unit. For information about clustering, see [Chapter 10, “Configuring a Cluster of ASAs.”](#)

Configuring Static and Default Routes

This section explains how to configure a static route and a static default route and includes the following topics:

- [Configuring a Static Route, page 25-3](#)
- [Configuring a Default Static Route, page 25-7](#)
- [Configuring IPv6 Default and Static Routes, page 25-8](#)

Configuring a Static Route

Static routing algorithms are basically table mappings established by the network administrator before the beginning of routing. These mappings do not change unless the network administrator alters them. Algorithms that use static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple. Because of this fact, static routing systems cannot react to network changes.

Static routes remain in the routing table even if the specified gateway becomes unavailable. If the specified gateway becomes unavailable, you need to remove the static route from the routing table manually. However, static routes are removed from the routing table if the specified interface goes down, and are reinstated when the interface comes back up.



Note

If you create a static route with an administrative distance greater than the administrative distance of the routing protocol running on the ASA, then a route to the specified destination discovered by the routing protocol takes precedence over the static route. The static route is used only if the dynamically discovered route is removed from the routing table.

You can define up to three equal cost routes to the same destination per interface. Equal-cost multi-path (ECMP) is not supported across multiple interfaces. With ECMP, the traffic is not necessarily divided evenly between the routes; traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

To configure a static route, [see the following section](#) [choose one of the following](#):

- [Adding or Editing a Static Route, page 25-3](#)
- [Configuring Static Route Tracking, page 25-6](#)
- [Deleting Static Routes, page 25-6](#)

Adding or Editing a Static Route

To add or edit a static route, enter the following command:

Command	Purpose
<pre>route if_name dest_ip mask gateway_ip [distance]</pre> <p>Example:</p> <pre>hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 [1]</pre>	<p>Enables you to add a static route.</p> <p>The <i>dest_ip</i> and <i>mask</i> arguments indicate the IP address for the destination network and the <i>gateway_ip</i> argument is the address of the next-hop router. The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.</p> <p>The <i>distance</i> argument is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connected routes.</p> <p>The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static route takes precedence. Connected routes always take precedence over static or dynamically discovered routes.</p>

To add or edit a static route in ASDM, perform the following steps:

Step 1 In the main ASDM window, choose **Configuration > Device Setup > Routing > Static Routes**.

Step 2 Choose which route to filter by clicking one of the following radio buttons:

- **Both** (filters both IPv4 and IPv6)
- **IPv4 only**
- **IPv6 only**

By default, the Both radio button is selected, and both IPv4 and IPv6 addresses appear in the pane. To limit your viewed choices to routes configured with IPv4 addresses, click the **IPv4** radio button. To limit your viewed choices to routes configured with IPv6 addresses, click the **IPv6** radio button.

Step 3 Click **Add** or **Edit**.

The Add or Edit Static Route dialog box appears.

Step 4 From the Interface drop-down list, choose the internal or external network interface name enabled in the Interface field:

- **management** (internal interface)
- **outside** (external interface)

Step 5 In the IP Address field, type an internal or external network IP address for the destination network.

For IPv4 addresses, enter **0.0.0.0** to specify a default route. The 0.0.0.0 IP address can be abbreviated as 0. Optionally, click the ellipsis to browse for an address.

For IPv6 addresses, enter two colons (::) to specify a default route. Optionally, click the ellipsis to browse for an address.

Step 6 In the Gateway IP field, enter the IP address of the gateway router, which is the next hop address for this route.

To enter a default route, set the IP address and mask to **0.0.0.0**, or the shortened form of **0**.

Optionally, click the ellipsis to browse for an address.



Note If an IP address from one ASA interface is used as the gateway IP address, the ASA will ARP the designated IP address in the packet instead of ARPing the gateway IP address.

The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.

Step 7 Choose the netmask from the drop-down list for the destination network. Depending upon which route you chose to filter (IPv4, IPv6, or both), do one of the following:

- For IPv4 static routes (or for both IPv4 and IPv6 static routes), enter the network mask address that applies to the IP address. Enter **0.0.0.0** to specify a default route. The **0.0.0.0** netmask can be abbreviated as **0**.
- For IPv6 static routes only, enter a prefix length.

Step 8 In the Metric field, type the metric, or administrative distance.

The metric or distance is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols, but not directly connected routes.

The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

Step 9 (Optional) In the Options area, choose one of the following options for a static route:

- **None** to have no options specified for the static route. This setting is the default.
- **Tunneled** to specify the route as the default tunnel gateway for VPN traffic. This setting is used for the default route only. You can configure only one tunneled route per device. The tunneled option is not supported in transparent mode.
- **Tracked** to specify that the route is tracked. The tracking object ID and the address of the tracking target also appear. The tracked option is supported in single, routed mode only. Specify the following settings for the tracked option:
 - In the Track ID field, enter a unique identifier for the route tracking process.
 - In the Track IP Address/DNS Name field, enter the IP address or hostname of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available from that interface.
 - In the SLA ID field, enter a unique identifier for the SLA monitoring process.



Note The Tracked option is not supported for IPv6.

Step 10 (Optional) Click **Monitoring Options**.

The Route Monitoring Options dialog box appears. From here, you change the following tracking object monitoring properties:

- **Frequency**, which allows you to modify how often, in seconds, the ASA should test for the presence of the tracking target. Valid values range from 1 to 604800 seconds. The default value is 60 seconds.
- **Threshold**, which allows you to enter the amount of time, in milliseconds, that indicates an over-threshold event. This value cannot be more than the timeout value.
- **Timeout**, which allows you to modify the amount of time, in milliseconds, that the route monitoring operation should wait for a response from the request packets. Valid values range from 0 to 604800000 milliseconds. The default value is 5000 milliseconds.
- **Data Size**, which allows you to modify the size of data payload to use in the echo request packets. The default value is 28. Valid values range from 0 to 16384.



Note This setting specifies the size of the payload only; it does not specify the size of the entire packet.

- **ToS**, which allows you to choose a value for the type of service byte in the IP header of the echo request. Valid values are from 0 to 255. The default value is 0.
- **Number of Packets**, which allows you to choose the number of echo requests to send for each test. Valid values range from 1 to 100. The default value is 1.

Step 11 Click **OK**.

Step 12 Click **Apply** to save the configuration.

The added or edited route information appears in the Static Routes pane. The monitoring process begins as soon as you save the newly configured route.

Configuring Static Route Tracking

To configure tracking for a static route, perform the following steps:



Note

Static route tracking is available for IPv4 routes only.

- Step 1** Choose a target of interest. Make sure that the target responds to echo requests.
 - Step 2** Open the Static Routes pane by choosing **Configuration > Device Setup > Routing > Static Routes**.
 - Step 3** Click **Add** to configure a static route that is to be used based on the availability of your selected target of interest. You must enter the Interface, IP Address, Mask, Gateway, and Metric settings for this route.
 - Step 4** Click the **Tracked** radio button in the Options area for this route.
 - Step 5** Configure the tracking properties. You must enter a unique Track ID, a unique SLA ID, and the IP address of your target of interest.
 - Step 6** (Optional) To configure the monitoring properties, click **Monitoring Options** in the Add Static Route dialog box.
 - Step 7** Click **OK** to save your changes.
The monitoring process begins as soon as you save the tracked route.
 - Step 8** Create a secondary route by repeating Steps 1 through 7.
The secondary route is a static route to the same destination as the tracked route, but through a different interface or gateway. You must assign this route a higher administrative distance (metric) than your tracked route.
 - Step 9** Click **OK** to save your changes.
-

Deleting Static Routes

To delete a static route, perform the following steps:

- Step 1** Choose **Configuration > Device Setup > Routing > Static Routes**.
- Step 2** On the Static Routes pane, choose which route to delete.
By default, the Both radio button is checked, and both IPv4 and IPv6 addresses appear in the pane.
 - To limit your viewed choices to routes configured with IPv4 addresses, click the **IPv4** radio button.
 - To limit your viewed choices to routes configured with IPv6 addresses, click the **IPv6** radio button.
- Step 3** Click **Delete**.
The deleted route is removed from list of routes on in the main Static Routes pane.

Step 4 Click **Apply** to save the changes to your configuration.

Examples

The following example shows static routes that are equal cost routes that direct traffic to three different gateways on the outside interface. The ASA distributes the traffic among the specified gateways.

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.3
```

Configuring a Default Static Route

A default route identifies the gateway IP address to which the ASA sends all IP packets for which it does not have a learned or static route. A default static route is simply a static route with 0.0.0.0/0 as the destination IP address. Routes that identify a specific destination take precedence over the default route.



Note

In Versions 7.0(1) and later, if you have two default routes configured on different interfaces that have different metrics, the connection to the ASA that is made from the higher metric interface fails, but connections to the ASA from the lower metric interface succeed as expected.

You can define up to three equal cost default route entries per device. Defining more than one equal cost default route entry causes the traffic sent to the default route to be distributed among the specified gateways. When defining more than one default route, you must specify the same interface for each entry.

If you attempt to define more than three equal cost default routes or a default route with a different interface than a previously defined default route, you receive the following message:

"ERROR: Cannot add route entry, possible conflict with existing routes."

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the tunneled option, all traffic from a tunnel terminating on the ASA that cannot be routed using learned or static routes is sent to this route. For traffic emerging from a tunnel, this route overrides any other configured or learned default routes.

Limitations on Configuring a Default Static Route

The following restrictions apply to default routes with the tunneled option:

- Do not enable unicast RPF (**ip verify reverse-path** command) on the egress interface of a tunneled route, because this setting causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route, because this setting causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes, because these inspection engines ignore the tunneled route.
- You cannot define more than one default route with the tunneled option.
- ECMP for tunneled traffic is not supported.

To add or edit a tunneled default static route, enter the following command:

Command	Purpose
<pre>route if_name 0.0.0.0 0.0.0.0 gateway_ip [distance tunneled]</pre> <p>Example:</p> <pre>hostname(config)# route outside 0 0 192.168.2.4 tunneled</pre>	<p>Enables you to add a static route.</p> <p>The <i>dest_ip</i> and <i>mask</i> arguments indicate the IP address for the destination network and the <i>gateway_ip</i> argument is the address of the next hop router. The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.</p> <p>The <i>distance</i> argument is the administrative distance for the route. The default is 1 if you do not specify a value. Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connect routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamic route, the static routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.</p>



Tip

You can enter 0 0 instead of 0.0.0.0 0.0.0.0 for the destination network address and mask, as shown in the following example:

```
hostname(config)# route outside 0 0 192.168.1 1
```

To add or edit a tunneled default static route in ASDM, perform the following steps:

- Step 1

On the main ASDM window, choose **Configuration > Device Setup > Routing > Static Routes**.
- Step 2

Click **Add** or **Edit**.
- Step 3

In the Options area, choose **Tunneled**.
- Step 4

Click **OK**.

Configuring IPv6 Default and Static Routes

The ASA automatically routes IPv6 traffic between directly connected hosts if the interfaces to which the hosts are attached are enabled for IPv6 and the IPv6 ACLs allow the traffic.

To configure an IPv6 default route and static routes, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	ipv6 route <i>if_name</i> ::/0 <i>next_hop_ipv6_addr</i> Example: <pre>hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1</pre>	Adds a default IPv6 route. The example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 The address ::/0 is the IPv6 equivalent of any.
Step 2	ipv6 route <i>if_name</i> <i>destination</i> <i>next_hop_ipv6_addr</i> [<i>admin_distance</i>] Example: <pre>hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 [110]</pre>	Adds an IPv6 static route to the IPv6 routing table. The example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1, and with an administrative distance of 110.



Note

The **ipv6 route** command works the same way as the **route** command does, which is used to define IPv4 static routes.

To add or edit a default static route in ASDM, perform the following steps:

- | | |
|---------------|--|
| Step 1 | In the main ASDM window, choose Configuration > Device Setup > Routing > Static Routes . |
| Step 2 | Click the IPv6 only radio button. |
| Step 3 | Click Add or Edit . |
| Step 4 | Click OK . |

Monitoring a Static or Default Route

One of the problems with static routes is that there is no inherent mechanism for determining if the route is up or down. They remain in the routing table even if the next hop gateway becomes unavailable. Static routes are only removed from the routing table if the associated interface on the ASA goes down.

The static route tracking feature provides a method for tracking the availability of a static route and installing a backup route if the primary route should fail. For example, you can define a default route to an ISP gateway and a backup default route to a secondary ISP in case the primary ISP becomes unavailable.

The ASA implements this feature by associating a static route with a monitoring target that you define, and monitors the target using ICMP echo requests. If an echo reply is not received within a specified time period, the object is considered down and the associated route is removed from the routing table. A previously configured backup route is used in place of the removed route.

When selecting a monitoring target, you need to make sure that it can respond to ICMP echo requests. The target can be any network object that you choose, but you should consider using the following:

- The ISP gateway (for dual ISP support) address

- The next hop gateway address (if you are concerned about the availability of the gateway)
- A server on the target network, such as a AAA server, that the ASA needs to communicate with
- A persistent network object on the destination network

**Note**

A desktop or notebook computer that may be shut down at night is not a good choice.

You can configure static route tracking for statically defined routes or default routes obtained through DHCP or PPPoE. You can only enable PPPoE clients on multiple interfaces with route tracking configured.

To configure static route tracking, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	sla monitor <i>sla_id</i> Example: hostname(config)# sla monitor sla_id	Configures the tracked object monitoring parameters by defining the monitoring process. If you are configuring a new monitoring process, you enter sla monitor configuration mode. If you are changing the monitoring parameters for an unscheduled monitoring process that already has a type defined, you automatically enter sla protocol configuration mode.
Step 2	type echo protocol ipIcmpEcho <i>target_ip</i> interface <i>if_name</i> Example: hostname(config-sla-monitor)# type echo protocol ipIcmpEcho target_ip interface if_name	Specifies the monitoring protocol. If you are changing the monitoring parameters for an unscheduled monitoring process that already has a type defined, you automatically enter sla protocol configuration mode and cannot change this setting. The <i>target_ip</i> argument is the IP address of the network object whose availability the tracking process monitors. While this object is available, the tracking process route is installed in the routing table. When this object becomes unavailable, the tracking process removes the route and the backup route is used in its place.
Step 3	sla monitor schedule <i>sla_id</i> [life { forever <i>seconds</i> }] [start-time { <i>hh:mm[:ss]</i> <i>month day</i> <i>day month</i> } pending now after <i>hh:mm:ss</i>] [ageout <i>seconds</i>] [recurring] Example: hostname(config)# sla monitor schedule sla_id [life {forever seconds}] [start-time {hh:mm[:ss] month day day month} pending now after hh:mm:ss] [ageout seconds] [recurring]	Schedules the monitoring process. Typically, you will use the sla monitor schedule sla_id life forever start-time now command for the monitoring schedule, and allow the monitoring configuration to determine how often the testing occurs. However, you can schedule this monitoring process to begin in the future and to only occur at specified times.

	Command	Purpose
Step 4	track <i>track_id</i> rtr <i>sla_id</i> reachability	Associates a tracked static route with the SLA monitoring process.
	Example: hostname(config)# track <i>track_id</i> rtr <i>sla_id</i> reachability	The <i>track_id</i> argument is a tracking number you assign with this command. The <i>sla_id</i> argument is the ID number of the SLA process.
Step 5	Do one of the following to define the static route to be installed in the routing table while the tracked object is reachable. These options allow you to track a static route or a default route obtained through DHCP or PPPOE.	
	route <i>if_name</i> <i>dest_ip</i> <i>mask</i> <i>gateway_ip</i> [<i>admin_distance</i>] track <i>track_id</i>	Tracks a static route. You cannot use the tunneled option with the route command in static route tracking.
	Example: hostname(config)# route <i>if_name</i> <i>dest_ip</i> <i>mask</i> <i>gateway_ip</i> [<i>admin_distance</i>] track <i>track_id</i>	
	Example: hostname(config)# interface <i>phy_if</i> hostname(config-if)# dhcp client route track <i>track_id</i> hostname(config-if)# ip address dhcp setroute hostname(config-if)# exit	Tracks a default route obtained through DHCP, Remember that you must use the setroute keyword with the ip address dhcp command to obtain the default route using DHCP.
	Example: hostname(config)# interface <i>phy_if</i> hostname(config-if)# pppoe client route track <i>track_id</i> hostname(config-if)# ip address pppoe setroute hostname(config-if)# exit	Tracks a default route obtained through PPPoE. You must use the setroute keyword with the ip address pppoe command to obtain the default route using PPPoE.

To monitor the state of a route in ASDM, in the main ASDM window, perform the following steps:

Step 1 Choose **Monitoring > Routing > Routes**.

In the Routes pane, each row represents one route. You can filter by IPv4 connections, IPv6 connections, or both. The routing information includes the protocol, the route type, the destination IP address, the netmask or prefix length, the gateway IP address, the interface through which the route is connected, and the administrative distance.

Step 2 To update the current list, click **Refresh**.

Configuration Examples for Static or Default Routes

The following example shows how to create a static route that sends all traffic destined for 10.1.1.0/24 to the router 10.1.2.45, which is connected to the inside interface, defines three equal cost static routes that direct traffic to three different gateways on the outside interface, and adds a default route for tunneled traffic. The ASA then distributes the traffic among the specified gateways:

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.1
```

```
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.2
hostname(config)# route outside 10.10.10.0 255.255.255.0 192.168.2.3
hostname(config)# route outside 0 0 192.168.2.4 tunneled
```

Unencrypted traffic received by the ASA for which there is no static or learned route is distributed among the gateways with the IP addresses 192.168.2.1, 192.168.2.2, and 192.168.2.3. Encrypted traffic received by the ASA for which there is no static or learned route is passed to the gateway with the IP address 192.168.2.4.

The following example creates a static route that sends all traffic destined for 10.1.1.0/24 to the router (10.1.2.45) connected to the inside interface:

```
hostname(config)# route inside 10.1.1.0 255.255.255.0 10.1.2.45 1
```

- Step 1** In the main ASDM window, choose **Configuration > Device Setup > Routing > Static Routes**.
 - Step 2** Choose **Management** from the Interfaces drop-down list.
 - Step 3** Enter **10.1.1.0** in the IP Address field.
 - Step 4** Choose **255.255.255.0** from the Mask drop-down list.
 - Step 5** Enter **10.1.2.45 1** in the Gateway IP field.
A static route is created that sends all traffic destined for 10.1.1.0/24 to the router 10.1.2.45, which is connected to the inside interface.
 - Step 6** Click **OK**.
 - Step 7** Choose **Configuration > Device Setup > Routing > Static Routes**.
 - Step 8** Click **Add**.
 - Step 9** Enter the IP Address in the IP Address field for the destination network.
In this case, the route IP addresses are: 192.168.2.1, 192.168.2.2, 192.168.2.3, and 192.168.2.4. When adding 192.168.2.4, click the **Tunneled** radio button in the Options area.
 - Step 10** Enter the Gateway IP Address in the Gateway IP Address field for the address of the next hop router.
The addresses you specify for the static route are the addresses that are in the packet before entering the ASA and performing NAT.
 - Step 11** Choose the netmask for the destination network from the NetMask drop-down list.
 - Step 12** Click **OK**.
-

Feature History for Static and Default Routes

Table 25-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 25-1 Feature History for Static and Default Routes

Feature Name	Platform Releases	Feature Information
Routing	7.0(1)	Static and default routing were introduced. We introduced the route command. We introduced the following screen: Configuration > Device Setup > Routing.
Clustering	9.0(1)	Supports static route monitoring on the master unit only.

