


Configure Virtual Routers

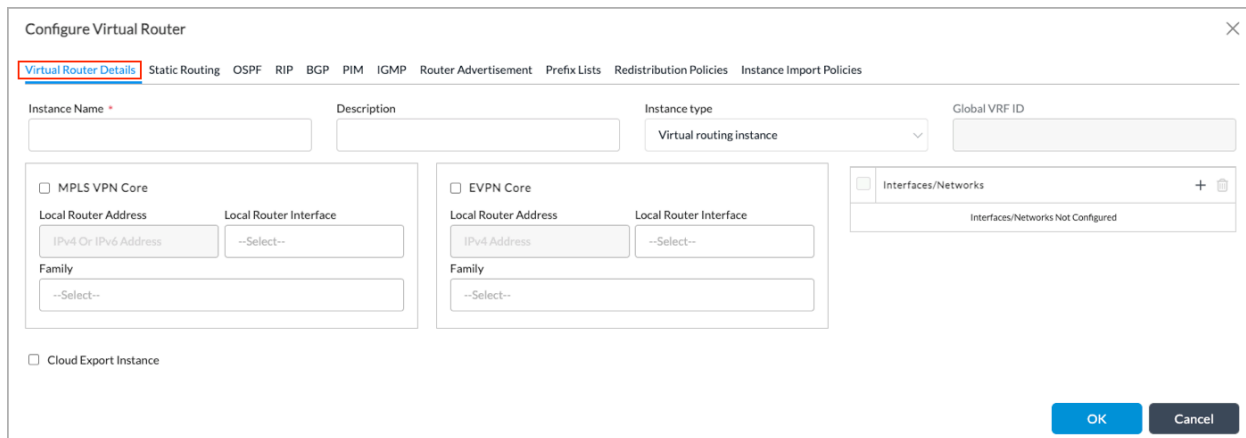
 For supported software information, click [here](#).

A virtual router is a software object that functions like a hardware-based Layer 3 Internet Protocol (IP) router. A virtual router enables a computer to perform the functions of a physical router. Just as with a physical router, on a virtual router you configure static and dynamic routing protocols, including unicast and multicast protocols, router advertisements, and redistribution and import policies.

You configure all properties of a virtual router in the Configure Virtual Router popup window.

Set Up a Virtual Router

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > Virtual Routers in the left menu bar
4. Click the  Add icon. The Configure Virtual Router popup window displays.




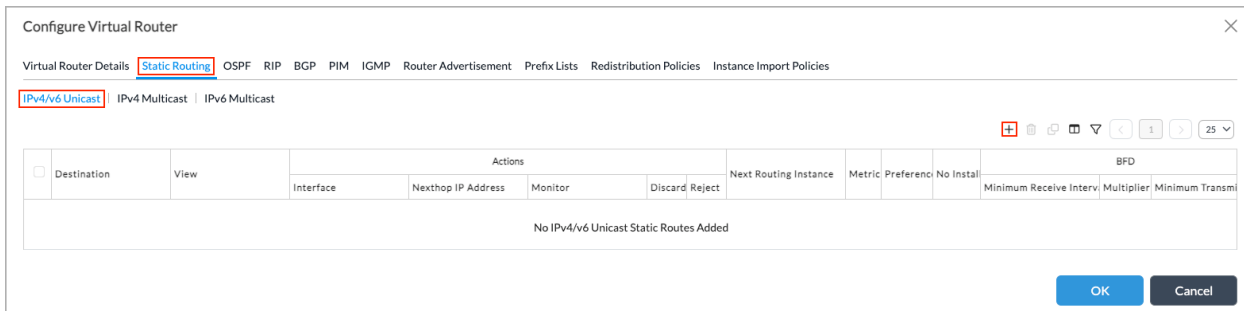
5. Select the Virtual Router Details tab. Enter information for the following fields.

Field	Description
Instance Name	Enter a unique name for the virtual router.
Description	Enter a text description for the interface.
Instance Type	<p>Select the virtual router instance type:</p> <ul style="list-style-type: none"> Virtual Routing Instance—Configure a simple VPN. This is the basic instance type. Virtual Routing Forwarding Instance—Configure a router for Layer 3 VPN.
Global VRF ID	Enter an ID for the global VRF.
MPLS VPN Core (Group of Fields)	For a virtual routing instance and for MPLS, click to configure the virtual router as the core router.
<ul style="list-style-type: none"> MPLS Local Router Address 	For a virtual routing instance and for MPLS, enter the local router's IPv4 or IPv6 address.
<ul style="list-style-type: none"> MPLS Local Router Interface 	Select the local router interface to use for MPLS.
<ul style="list-style-type: none"> Family 	Select the family to use for the virtual router.
EVPN Core (Group of Fields)	Ethernet VPN (EVPN) enables you to connect two or more Layer 2 domains over IP or MPLS Layer 3 underlay networks.
<ul style="list-style-type: none"> EVPN Local Router Address 	Enter the IP address of the local EVPN router.
<ul style="list-style-type: none"> EVPN Local Router Interface 	Select a local router interface for the EVPN core.
<ul style="list-style-type: none"> Family 	Select a family for the virtual router.
Create Dynamic GRE Tunnels	Click to create dynamic GRE tunnels.
Interfaces/Networks	Select one or more interfaces to assign to the routing instance.

6. Click OK.

Configure Static Routes

1. If you are continuing from the previous section, skip to Step 6.
2. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar.
5. Click the  Add icon. The Configure Virtual Router popup window displays.
6. Select Static Routing in the horizontal menu bar in the Configure Virtual Router window.




Configure Virtual Router

Virtual Router Details **Static Routing** OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

IPv4/v6 Unicast IPv4 Multicast IPv6 Multicast

Destination	View	Actions				Next Routing Instance	Metric	Preference	No Install	BFD			
		Interface	Nexthop IP Address	Monitor	Discard/Reject					Minimum Receive Interv	Multiplier	Minimum Transm	
No IPv4/v6 Unicast Static Routes Added													

OK Cancel

7. To add an IPv4 or IPv6 unicast static route, select the IPv4/IPv6 Unicast tab and then click the  Add icon. Enter information for the following fields.

Add IPv4/v6 Unicast
✕

Destination *

IPv4 or IPv6 Address/Mask

Monitor

--Select--

Monitor Group

--Select--

Metric

Allowed Range is 1 - 4294967295

Preference

1

Tag

Action

Interface

--Select--

☒ Nexthop IP Address
☐ Next Routing Instance
☐ Discard
☐ Reject

IPv4 Or IPv6 Address

--Select--

☐ No Install

☐ Enable ICMP

Interval

Allowed Range is 1 - 60

Threshold

Allowed Range is 1 - 60

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)

Allowed Range is 1 - 255000

Minimum Transmit Interval (msec)

Allowed Range is 1 - 255000

Multiplier

Allowed Range is 1 - 255

OK

Cancel


Field	Description								
Destination	Enter the destination IP address or network.								
Action (Group of Fields)									
◦ Next-Hop Interface	Select the next-hop interface towards the destination network.								
◦ Next-Hop IP Address	Click to specify the IP address to use to reach the destination network.								
◦ Next Routing Instance	Click to select the routing instance to use to reach the destination network.								
◦ Discard	<p>Install the route in both the control plane and the data plane. In the data plane, the traffic is installed with the Discard option.</p> <p>For example, if there is a static route to 172.16.0.0/16 for which the Discard option is selected, a more specific route to 172.16.1.0/24 for which the Forward action is selected, and a default route (0.0.0.0/0), the data plane actions are as follows:</p> <table border="1"> <thead> <tr> <th>Route</th><th>Data Plane Action</th></tr> </thead> <tbody> <tr> <td>0.0.0.0/0 (default forwarding)</td><td>Forward</td></tr> <tr> <td>172.16.0.0/16</td><td>Discard</td></tr> <tr> <td>172.16.1.0/24</td><td>Forward</td></tr> </tbody> </table> <p>The following examples illustrate how packets are handled:</p> <ul style="list-style-type: none"> ◦ A packet to 172.16.1.10 is forwarded to the next hop. ◦ A packet to 172.16.5.10 is silently dropped. ◦ A packet to 8.8.8.8 is forwarded through the default gateway next hop. 	Route	Data Plane Action	0.0.0.0/0 (default forwarding)	Forward	172.16.0.0/16	Discard	172.16.1.0/24	Forward
Route	Data Plane Action								
0.0.0.0/0 (default forwarding)	Forward								
172.16.0.0/16	Discard								
172.16.1.0/24	Forward								
◦ Reject	Install the route in both the control plane and the data plane. In the data plane, the traffic is installed with the								

	<p>Reject option.</p> <p>For example, if there is a static route to 172.16.0.0/16 for which the Reject option selected, a more specific route to 172.16.1.0/24 for which the Forward action selected, and a default route (0.0.0.0/0), the data plane actions are as follows:</p> <table border="1"> <thead> <tr> <th>Route</th><th>Data Plane Action</th></tr> </thead> <tbody> <tr> <td>0.0.0.0/0 (default forwarding)</td><td>Forward</td></tr> <tr> <td>172.16.0.0/16</td><td>Reject</td></tr> <tr> <td>172.16.1.0/24</td><td>Forward</td></tr> </tbody> </table> <p>The following examples illustrate how packets are handled:</p> <ul style="list-style-type: none"> ◦ A packet to 172.16.1.10 is forwarded to the next hop. ◦ A packet to 172.16.5.10 is dropped, and an ICMP message is sent to the sender reporting that the destination is unreachable. ◦ A packet to 8.8.8.8 is forwarded through the default gateway next hop. 	Route	Data Plane Action	0.0.0.0/0 (default forwarding)	Forward	172.16.0.0/16	Reject	172.16.1.0/24	Forward
Route	Data Plane Action								
0.0.0.0/0 (default forwarding)	Forward								
172.16.0.0/16	Reject								
172.16.1.0/24	Forward								
<ul style="list-style-type: none"> ◦ No Install 	<p>Install the route in the control plane only, and do not install the route in the data plane.</p> <p>For example, if there is a static route to 172.16.0.0/16 for which the No Install option selected and a default route (0.0.0.0/0), a packet destined to 172.16.0.10 is sent using the default route if the data plane has no matching routes that are longer.</p>								
Enable ICMP (Group of Fields)	<p>Click to enable ICMP monitoring of the next hop configured for the static route. If the ICMP monitoring fails, the route is withdrawn from the routing table. Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously,</p>								

	and if any one of the monitors fails, the static route is withdrawn from the routing table.
◦ Interval	Enter the time interval between ICMP packets. <i>Range: 1 through 60 seconds</i>
◦ Threshold	Enter the the number of ICMP probes to be missed before setting the state of the ICMP monitor as down and withdrawing the static route. <i>Range: 1 through 60</i>
Metric	Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol. <i>Range: 1 through 4294967295</i>
Preference	Enter the administrative distance (AD) or route preference value of the static route. You can assign a preference for each route. The preference is used to choose between multiple paths learned from different routing protocols. <i>Range: 1 through 255</i>
Tag	Enter a tag for the static route.
Monitor	Select the name of a liveness detection monitor that must be up for the static route to become active. To configure a monitor, see Configure IP SLA Monitor Objects . Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously, and if any one of the monitors fails, the static route is withdrawn from the routing table.
Enable BFD (Group of Fields)	Click to enable Bidirectional Forwarding Detection monitoring of the next hop configured for the static route. If the BFD monitoring fails, the route is withdrawn from the routing table. Note that if you configure one or more of the Enable ICMP, Monitor, and Enable BFD fields simultaneously, and if any one

	of the monitors fails, the static route is withdrawn from the routing table.
◦ Minimum Receive Interval	Enter the minimum time interval to receive routes, in milliseconds. <i>Range:</i> 1 through 255000 milliseconds
◦ Multiplier	Enter the multiplier value to use to calculate the final minimum receive interval and minimum transmit interval. <i>Range:</i> 1 through 255
◦ Minimum Transmit Interval	Enter the time after which routes can be retransmitted, in milliseconds. <i>Range:</i> 1 through 255000 milliseconds

8. Click OK

9. To add an IPv4 multicast static route, select the IPv4 Multicast tab and then click the  Add icon. Enter information for the following fields.

Add IPv4 Multicast

Destination *

IPv4 Address/Mask

Metric

Allowed Range is 1 - 4294967295

Preference

1

Tag

Action

Interface

--Select--

☒ Nexthop IP Address

☐ Next Routing Instance

IPv4 Or IPv6 Address

--Select--

☐ Enable ICMP

Interval

Allowed Range is 1 - 60

Threshold


Allowed Range is 1 - 60

OK

Cancel

Field	Description
Destination	Enter the destination IP address or network.
Action (Group of Fields)	
◦ Interface	Select the interface towards the destination network.
◦ Next-Hop IP Address	Click to specify the IP address to use to reach the destination network.
◦ Next Routing Instance	Click to select the routing instance to use to reach the destination network.
Metric	Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol. <i>Range: 1 through 4294967295</i>
Preference	Enter the preference value of the IPv4 route. <i>Range: 1 through 255</i>
Tag	Enter a tag for the IPv4 route.

10. Click OK.

11. To add an IPv6 multicast static route, select the IPv6 Multicast tab and then click the  Add icon. Enter information for the following fields.

Add IPv6 Multicast

Destination *

IPv6 Address/Mask

Metric

Allowed Range is 1 - 4294967295

Preference

1

Tag

Action

Interface

--Select--

☒ Nexthop IP Address

☐ Next Routing Instance

IPv6 Address

--Select--

☐ Enable ICMP

Interval

Allowed Range is 1 - 60

Threshold

Allowed Range is 1 - 60

OK

Cancel

Field	Description
Destination	Enter the destination IP address or network.
Action (Group of Fields)	
◦ Interface	Select the interface towards the destination network.
◦ Next-Hop IP Address	Click to specify the IP address to use to reach the destination network.
◦ Next Routing Instance	Click to select the routing instance to use to reach the destination network.
Metric	Enter the cost to reach the destination network. The metric is used to choose between multiple paths learned with the same routing protocol. <i>Range: 1 through 4294967295</i>
Preference	Enter the preference value of the IPv6 route. <i>Range: 1 through 255</i>
Tag	Enter a tag for the IPv6 route.


12. Click OK. The static route displays in the Configure Virtual Router popup window.

Configure OSPF and OSPFv3

The open shortest path first (OSPF) is an interior gateway routing protocol (IGP) that uses a link-state routing algorithm. OSPFv2 for IPv4 is defined in RFC 2328. OSPF is widely used as the IGP for IPv4, IPv6, and dual-stack (IPv4/IPv6) environments.

To configure OSPF and OSPFv3 for IPv4, IPv6, and dual-stack (IPv4/IPv6) environments:

1. If you are continuing from the previous section, skip to Step 6.
2. In Director view:

- a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar.
5. Click the  Add icon. The Configure Virtual Router popup window displays.
6. Select OSPF in the horizontal menu bar in the Configure Virtual Router window.

Configure Virtual Router

Virtual Router DetailsStatic RoutingOSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies Instance Import Policies

OSPF InstanceOSPFv3 Instance

Instance ID


View

Router ID

No OSPF Instance Added

OK

Cancel

7. Click the  Add icon. The Add OSPF Instance popup window displays. Enter information for the following fields.

Add OSPF Instance

Instance ID *

Allowed Range is 1 - 65535

Router ID *

IPv4 Address

Domain VPN Tag

Allowed Range is 1 - 4294967295

Internal Admin Distance

Allowed Range is 1 - 255

External Admin Distance

Allowed Range is 1 - 255

Reference Bandwidth (Mbps)

Enable Alarms

Disable DN Bit

AreasDebugDefault Information

Area ID

Type

Networks

Virtual Links


No Area Record Added

OK

Cancel

Field	Description
Instance ID	Enter the instance ID to assign to OSPF. Range: 1 through 65535

Field	Description
Router ID	Enter the router IP address to use for OSPF.
Domain VPN Tag	Enter the MPLS VPN tag attached to OSPF routes in this domain. Use this to enabled the OSPF PE-CE protocol on a PE router for external learned routes. <i>Range: 1 through 4294967295</i>
Internal Admin Distance	Enter the administrative distance for internal routes (routes learned within the routing domain). <i>Range: 1 through 255</i>
External Admin Distance	Enter the administrative distance for external routes (routes learned from another routing domain). <i>Range: 1 through 255</i>
Reference Bandwidth	Enter the reference bandwidth value to use when calculating the interface cost, in Mbps.
Enable Alarms	Click to enable the generation of alarms.
Disable DN Bit	Click to reset the DN it When redistributing routes. The DN bit is used for loop prevention, so it is always enabled or set.
Areas Tab	Select the Areas tab to configure the OSPF area.

8. Click the  Add icon to configure an OSPF area. An area is a collection of OSPF networks, routers, and links. Each area is assigned an ID. An area with zero as its ID is a backbone or normal area. Areas with non-zero IDs are non-backbone areas. Each area must be connected to the backbone area known as area 0. Areas communicate with other areas through the backbone area. Enter information for the following fields.

Add OSPF Instance Add Area

Area ID *

Type
Network
Virtual Link
Sham Link

Type
Standard
Default Metric
Allowed Range is 1 - 16777215
No Summaries

OK
Cancel

Field	Description
Area ID	Enter an ID for the area. A backbone area has an area ID of 0.0.0.0. Areas with non-zero IDs are non-backbone areas.
Type (Tab)	Select the Type tab to configure the OSPF area type.
<ul style="list-style-type: none"> Type 	Select the area type: <ul style="list-style-type: none"> Backbone—Backbone area is normal area. Normal—For non-backbone area. NSSA—Not-so-stubby areas can import external routes into the OSPF routing domain and that can provide transit services to routing domains that are not part of the OSPF routing domain. Stub—External routes are not advertised.
Default Metric	For a stub or an NSSA area, enter the metric for the default route. <i>Range: 1 through 16777215</i>
<ul style="list-style-type: none"> No Summaries 	For all area types except Normal, click to have a border router not advertise routes from the area.

- Select the Network tab to configure the network interface or IP address of the OSPF network. The list of configured networks displays.

Add OSPF Instance Add Area

Area ID *

Type
Network
Virtual Link
Sham Link

+

<


1

>

25

	Network IP / Network Name	Network Type	Priority	Passive	Timers				Authentication Type
					Dead Interval (sec)	Hello Interval (sec)	Re-transmit Interval (sec)	Transit Delay (sec)	
No Network Added									

OK
Cancel

10. Click the  Add icon, and enter information for the following fields.

Add OSPF Instance Add Area Add Network

☒ Network IP
☐ Network Name

Network IP *

IPv4 Address

Network Name

--Select--

Network Type

Broadcast Type

Priority

1

Helper Mode Policy

All

Maximum Grace Period

140

Metric

1

☐ Passive

Timers

Hello Interval (seconds)

10

Dead Interval (seconds)

40

Re-transmit Interval (seconds)

5

Transit Delay (seconds)

1

Authentication

Type

--Select--

Key ID

0

MD5 Auth Key

Auth Key

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)

Allowed Range is 1 - 255000

Multiplier

Allowed Range is 1 - 255

Minimum Transmit Interval (msec)

Allowed Range is 1 - 255000

OK

Cancel

Field	Description
Network IP	Click and enter the IP address of the network. If you select Network IP, the Network Name field is grayed out.
Network Name	Click and enter the name of the network. If you select Network Name, the Network IP field is grayed out.
Network Type	Select the network type: <ul style="list-style-type: none"> Broadcast Type Loopback Type

Field	Description
	<ul style="list-style-type: none"> ◦ Point-to-Point Type
Priority	Enter a priority value to use in the election of the designated router (DR) and the backup designated router (BDR). On a multiaccess network, the OSPF router with the highest priority becomes the designated router, and the OSPF router with the second-highest priority becomes the backup router. If you set the priority to 0, the device does not participate in designated router and backup designated router election process
Helper Mode Policy	<p>Select in which peer OSPF restart situation the local router should act as a helper:</p> <ul style="list-style-type: none"> ◦ All—All OSPF restart situations ◦ Policy Reload—Software upgrade or reload of the peer router ◦ Policy Software—Crash of the OSPF process on the peer router ◦ Policy Switch—Control plane switchover on the peer router ◦ Policy Unknown—OSPF issues a restart reason not signaled in the graceful restart (type 9) link-state advertisement (LSA)
Maximum Grace Period	Enter a value to signal how long, in seconds, a helper should help a router. When this period expires, the helper brings down the adjacency with the restarting router, flushes its LSAs from the database, and floods new LSAs to the rest of the network to inform the other routers that it has lost its adjacency to the neighbor.
Metric	<p>Enter a value for the OSPF interface cost, which is used to calculate the total cost to reach a destination.</p> <p><i>Range:</i> 1 through 65535</p> <p><i>Default:</i> 1</p>
Passive	Click to indicate that the router is a passive listener. A passive router does not advertise itself. If you do not click, the router actively propagates messages.

Field	Description
Timers (Group of Fields)	
<ul style="list-style-type: none"> Hello Interval 	<p>Enter the time, in seconds, between the transmission of hello packets that this interface sends to neighbor routers.</p> <p><i>Range:</i> 1 through 255 seconds</p> <p><i>Default:</i> 10 seconds</p>
<ul style="list-style-type: none"> Dead Interval 	<p>Enter the time period, in seconds, during which at least one hello packet must be received from a neighbor before the router declares that neighbor to be down.</p> <p><i>Range:</i> 1 through 65535 seconds</p> <p><i>Default:</i> 40 seconds</p>
<ul style="list-style-type: none"> Retransmit Interval 	<p>Enter the time, in seconds, between the retransmission of LSAs to adjacent routers for a given interface.</p> <p><i>Range:</i> 1 through 3600 seconds</p> <p><i>Default:</i> 5 seconds</p>
<ul style="list-style-type: none"> Transit Delay 	<p>Enter the delay in retransmitting a message, in seconds</p> <p>Enter the time, in seconds, for how often to transmit a link-state update (LSU) on the interface.</p> <p><i>Range:</i> 1 through 3600 seconds</p> <p><i>Default:</i> 1 second</p>
Authentication (Group of Fields)	
<ul style="list-style-type: none"> Type 	<p>Select how to authenticate OSPF router traffic:</p> <ul style="list-style-type: none"> MD5—Use encrypted authentication Simple Password—Use simple password-based authentication.
<ul style="list-style-type: none"> Key ID 	For MD5, enter the key ID.
<ul style="list-style-type: none"> MD5 Auth Key 	For MD5, enter the authorization key.

Field	Description
◦ Auth Key	For password-based authentication, enter the password.
Enable BFD (Group of Fields)	<p>Click to enable BFD for OSPF. When BFD is enabled, when OSPF goes down, the router is marked as being down.</p> <p>When a BFD session that supports OSPF goes down, the OSPF neighborship also goes down without waiting for the dead timer interval to expire.</p>
◦ Minimum Receive Interval	<p>Enter the time interval, in milliseconds, at which the BFD peer can receive control packets.</p> <p><i>Range:</i> 1 through 255000 milliseconds</p> <p><i>Default:</i> 150 milliseconds</p>
◦ Multiplier	Enter the number of times that a BFD control packet can be missed before BFD declares the neighbor to be down.
◦ Minimum Transmit Interval	<p>Enter the time interval, in milliseconds, at which this device can send BFD control packets.</p> <p><i>Range:</i> 1 through 255000 milliseconds</p> <p><i>Default:</i> 150 milliseconds</p>

11. Click OK.

12. Select the Virtual Link tab to configure an OSPF virtual link. When you merge networks, non-backbone areas communicate with each other through a virtual link. The list of configured virtual links displays.

Add OSPF Instance Add Area

Area ID *

Type Network **Virtual Link** Sham Link

+

Neighbour ID

Transit Area

Admin Up

Timers

Hello (seconds)

Dead (seconds)

Rx (seconds)

Tx Delay (seconds)

Authentication Type

No Virtual Link Added

OK Cancel

13. Click the  Add icon, and enter information for the following fields.

Add OSPF Instance
Add Area
Add Virtual Link
✕

Neighbour ID *

Transit Area *

☐ Admin Up

Timers

Hello Interval (seconds)

Dead Interval (seconds)

Re-transmit Interval (seconds)

Transit Delay (seconds)

Authentication

Type

--Select--

Key ID

MD5 Auth Key

Auth Key

OK

Cancel

Field	Description
Neighbor ID	Enter the IP address of the neighboring area.
Transit Area	Enter the ID or IP address of the backbone area.
Passive	(For Releases 21.2 and earlier.) Click to mark the router as a passive listener. A passive router sends no advertisement messages.
Admin Up	Click to indicate that the administrative status of the link is up.
Timers (Group of Fields)	
◦ Hello Interval	Enter the interval, in seconds after which router sends advertisement messages.
◦ Dead Interval	Enter the time to wait, in seconds, before the router declares a neighbor to be dead because it has

Field	Description
	received no advertisements within that amount of time.
◦ Retransmit Interval	Enter the retransmit interval, in seconds, after which the router can retransmit a message.
◦ Transmit Delay	Enter the delay, in seconds, for retransmitting a message.
Authentication (Group of Fields)	
◦ Type	Select how to authenticate router traffic: <ul style="list-style-type: none"> ◦ MD5—Use encrypted authentication ◦ Simple Password—Use password-based authentication
◦ Key ID	For MD5 authentication, enter the key ID.
◦ MD5 Auth key	For MD5 authentication, enter the authorization key.
◦ Auth Key	For password-based authentication, enter the password.

14. Click OK.
15. (For Releases 22.1.1 and later.) Select the Sham Link tab to configure a sham link. An OSPF sham link is a logical intra-area link carried by the backbone network. Routes exchanged over the backbone must appear as if being exchanged over an intra-area link for them to be classified as intra-area, and thus preferred, routes. Note that you can configure OSPF sham links only for OSPF Version 2 and only for area 0. You can configure only one sham link per OSPF instance.

Add OSPF Instance Add Area

Area ID *

0

Type
Network
Virtual Link
Sham Link

+

1

25

<input type="checkbox"/>	Local Endpoint Address	Remote Endpoint Address	Timers				Authentication Type
			Hello Interval (seco	Dead Interval (seco	Re-transmit Interval (secc	Transit Delay (seco	
No Sham Link Added							

OK
Cancel

16. Click the  Add icon, and enter information for the following fields.

Add OSPF Instance Add Area Add Sham Link

Local Endpoint Address *
Remote Endpoint Address *
Metric

IPv4 Address

IPv4 Address

0

Timers

Dead Interval (seconds)
Hello Interval (seconds)
Re-transmit Interval (seconds)

40

10

5

Transit Delay (seconds)

1

Authentication

Authentication Type
Authentication Key


--Select--

OK
Cancel

Field	Description
Local Endpoint Address (Required)	Enter the IPv4 address of the local endpoint (local loopback interface).

Field	Description
Remote Endpoint Address (Required)	Enter the IPv4 address of the remote endpoint (loopback interface on the provider edge (PE) interface).
Metric	Enter a value for the OSPF interface cost, which is used to calculate the total cost to reach a destination. <i>Range:</i> 1 through 65535
Timers (Group of Fields)	
◦ Hello Interval	Enter the interval, in seconds, after which router sends advertisement messages.
◦ Dead Interval	Enter the time to wait, in seconds, before the router declares a neighbor to be dead because it has received no advertisements within that amount of time.
◦ Retransmit Interval	Enter the retransmit interval, in seconds, after which the router can retransmit a message.
◦ Transmit Delay	Enter the delay, in seconds, for retransmitting a message.
Authentication (Group of Fields)	
◦ Authentication Type	<p>Select an authentication type:</p> <ul style="list-style-type: none"> ◦ MD5—Use encrypted authentication. Then, enter an ID in the Key ID field and a key in the MD5 Authentication Key field. ◦ None—Use no authentication. ◦ Simple Password—Use simple password-based authentication. Then, enter a password in the Authentication Key field.

17. Click OK three times to return to the OSPF tab of the Configure Virtual Router popup window.

19. Click the  Add icon to configure an OSPFv3 area. An area is a collection of OSPF networks, routers, and links. Each area is assigned an ID. An area with zero as its ID is a backbone or normal area. Areas with non-zero IDs are non-backbone areas. Each area must be connected to the backbone area known as area 0. Areas communicate with other areas through the backbone area. Enter information for the following fields.

Add OSPFv3 InstanceAdd Area

Area ID *

Type

NetworkVirtual Link

Type

Standard

No Summaries

OK

Cancel

Field	Description
Area ID	Enter an ID for the area. A backbone area has an area ID of 0.0.0.0. Areas with non-zero IDs are non-backbone areas.
Type (Tab)	Select the Type tab to configure the OSPFv3 area type.
<div>Type</div>	<div>Select the area type:<div><div>Backbone</div>—Backbone area is normal area.</div><div><div>NSSA</div>—Not-so-stubby areas can import external routes into the OSPF routing domain and that can provide transit services to routing domains that are not part of the OSPF routing domain.</div><div><div>Stub</div>—External routes are not advertised.</div></div>
<div>No Summaries</div>	For all area types except Normal, click to have a

Field	Description
	border router not advertise routes from the area.

20. Select the Network tab to configure the network interface or IP address of the network running OSPFv3. The list of configured networks displays.

Add OSPFv3 Instance Add Area

Area ID *

Type **Network** Virtual Link

+

<

1

>

25

<input type="checkbox"/>	Interface / Network Name	Network Type	Priority	Passive	Dead Interval (sec Hello)
No Network Added					

OK
Cancel

21. Click the **+** Add icon, and enter information for the following fields.

Add OSPFv3 Instance Add Area Add Network

☒ Interfaces
☐ Network Name

Interfaces *

--Select--

Network Name

--Select--

Network Type

Broadcast Type

Instance ID *

0

Priority

1

Metric

1

☐ Passive

Timers

Hello Interval (seconds)

10

Dead Interval (seconds)

40

Re-transmit Interval (seconds)

5

Transit Delay (seconds)

1

OK

Cancel

Field	Description
Interfaces	Select an interface in the OSPFv3 area. If you select Interfaces, the Network Name field is grayed out.
Network Name	Select the name of the network for the OSPFv3 area. If you select Network Name, the Interfaces field is grayed out.
Interfaces	Select an interface for the OSPFv3 area.
Network Name	Select the name of the network for the OSPFv3 area.
Network Type	Select the network type: <ul style="list-style-type: none"> Broadcast Type Loopback Type Point-to-Point Type
Instance ID	Enter the ID for the OSPFv3 instance.

Field	Description
Priority	Enter a value for the priority. A router with a higher priority propagates routes before other routers.
Metric	Enter a metric value to use to determine how to choose a route to advertise. The route can be chosen based on path length, bandwidth, hop count, load, path cost, MTU, and communication cost.
Passive	Click to indicate that the router is a passive listener. A passive router does not advertise itself. If you do not click, the router actively propagates messages.
Timers (Group of Fields)	
◦ Hello Interval	Enter the interval, in seconds, after which router advertises itself.
◦ Dead Interval	Enter the time to wait, in seconds, before declaring a router dead, in seconds, because the router does not advertise itself.
◦ Retransmit Interval	Enter the time after which the router can transmit a message, in seconds.
◦ Transit Delay	Enter the delay in retransmitting a message, in seconds.

22. Select the Virtual Link tab to configure an OSPFv3 virtual link. When you merge networks, non-backbone areas communicate with each other through a virtual link. The list of configured virtual links displays.

Add OSPF V3 Instance > Add Area


Area ID*
0.0.0.0

Type
Network
Virtual Link

+
-
|||
▼
1
25

	Neighbour ID	Transit Area	Timers	
			Hello (sec)	Dead (sec)
NO VIRTUAL LINK ADDED				

OK
Cancel

23. Click the  Add icon, and add information for the following fields.

Add OSPF V3 Instance > Add Area > Add Virtual Link

Neighbour ID*
Transit Area*
Instance ID
0

Timers

Hello Interval (sec)
Dead Interval (sec)
10
60

OK
Cancel

Field	Description
Neighbor ID	Enter the IP address of the neighboring area.
Transit Area	Enter the ID or IP address of the backbone area.
Instance ID	Enter the ID of the OSPFv3 instance.


Field	Description
Timers (Group of Fields)	
◦ Hello Interval	Enter the interval, in seconds after which router sends advertisement messages.
◦ Dead Interval	Enter the time to wait, in seconds, before the router declares a neighbor to be dead because it has received no advertisements within that amount of time.

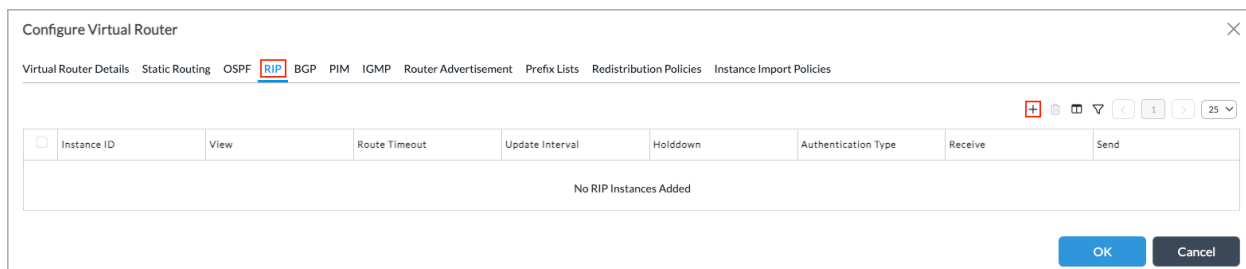
24. Click OK. The Configure Virtual Router popup window displays the OSPF instance.

Configure RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol. RIP uses hop counts as routing metrics and prevents routing loops by implementing a limit on the number of hops allowed in the source-to-destination path. The largest number of hops allowed is 15. This number limits the size of networks supported by RIP.

To configure RIP:

1. If you are continuing from the previous section, skip to Step 6.
2. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar
5. Click the  Add icon. The Configure Virtual Router popup window displays.
6. Select RIP in the horizontal menu bar in the Configure Virtual Router window.



7. Click the  Add icon. The Add RIP Instance popup window displays.

Add RIP Instance

General

Groups

Instance ID *

Allowed Range is 1 - 65535

Preference

Allowed Range is 1 - 255

Route Timeout

Allowed Range is 1 - 255

Update Interval

Allowed Range is 1 - 2147483

Holddown

Allowed Range is 1 - 255

Authentication Type

--Select--

Authentication Key

Receive

Multicast

Send

Version 2

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)

Allowed Range is 1 - 255000

Multiplier

Allowed Range is 1 - 255

Minimum Transmit Interval (msec)

Allowed Range is 1 - 255000

OK


Cancel

8. In the General tab, enter information for the following fields.

Field	Description
General Tab	Select the General tab to enter the details.
Instance ID	Enter the RIP instance ID number. <i>Range:</i> 1 through 65535
Preference	Enter a preference value for the instance. <i>Range:</i> 1 through 255
Route Timeout	Enter the time value for routes, in milliseconds. <i>Range:</i> 1 through 255 milliseconds
Update Interval	Enter the interval between gratuitous response messages, in seconds. Response messages are broadcast to all interfaces on which RIP is enabled. <i>Range:</i> 1 through 2147483 seconds <i>Default:</i> 30 seconds

Field	Description
Hold Down	<p>Enter a value for the hold-down timer. The hold-down timer is started for each route entry when the hop count changes from a lower value to higher value. During this time, no update can be made to the routing entry.</p> <p><i>Range:</i> 1 through 255</p>
Authentication Type	<p>Select the type of authentication:</p> <ul style="list-style-type: none"> ◦ MD5 ◦ None ◦ Simple password
Authentication Key	<p>For simple password authentication, enter the password.</p>
Receive	<p>Select how to receive response message from neighboring routers:</p> <ul style="list-style-type: none"> ◦ Multicast ◦ None
Send	<p>Selection how to send request messages:</p> <ul style="list-style-type: none"> ◦ None ◦ Version 2
Enable BFD (Group of Fields)	<p>Click to enable BFD on the interface, to allow BFD to report when RIP becomes unavailable.</p>
◦ Minimum Receive Interval	<p>Enter the minimum time interval to receive routes, in milliseconds.</p> <p><i>Range:</i> 1 through 255000 milliseconds</p>
◦ Multiplier	<p>Enter the multiplier value used to calculate the final minimum receive interval and minimum transmit</p>

Field	Description
	interval. <i>Range: 1 through 255</i>
<ul style="list-style-type: none"> Minimum Transmit Interval 	Enter the time after which routes can be retransmitted, in milliseconds. <i>Range: 1 through 255000 milliseconds</i>

- Select the Groups tab to configure information for a RIP group. The Add Group popup window displays. Click the  Add icon to add a RIP group.
- Select the General tab, and enter information for the following fields.

Add RIP Instance Add Group

General Interfaces Networks

Name *

Name

Authentication Type

--Select--

Authentication Key

Receive

Multicast

Send

Version 2

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)

Allowed Range is 1 - 255000

Multiplier

Allowed Range is 1 - 255

Minimum Transmit Interval (msec)


Allowed Range is 1 - 255000

OK Cancel

Field	Description
Name	Enter a name for the RIP group.
Authentication Type	Select the type of authentication: <ul style="list-style-type: none"> MD5 None Simple Password

Field	Description
Authentication Key	For simple password authentication, enter the password. It can be up to 64 characters long.
Receive	<p>Select how to receive response message from neighboring routers:</p> <ul style="list-style-type: none"> ◦ Multicast ◦ None
Send	<p>Select how to send request messages:</p> <ul style="list-style-type: none"> ◦ None ◦ Version 2
Enable BFD (Group of Fields)	Click to enable BFD on the interface, to allow BFD to report when RIP becomes unavailable.
◦ Minimum Receive Interval	<p>Enter the minimum time interval to receive routes, in milliseconds.</p> <p><i>Range:</i> 1 through 255000 milliseconds</p>
◦ Multiplier	<p>Enter the multiplier value used to calculate the final minimum receive interval and minimum transmit interval.</p> <p><i>Range:</i> 1 through 255</p>
◦ Minimum Transmit Interval	<p>Enter the time after which routes can be retransmitted, in milliseconds.</p> <p><i>Range:</i> 1 through 255000 milliseconds</p>

11. Click OK.

12. Select the Interfaces tab, click the  Add icon to configure interfaces in the RIP group, and enter information for the following fields. Note that you can configure either interfaces in the RIP group (in the Interfaces tab) or networks in the RIP group (in the Networks) tab, but not both.

Add RIP InstanceAdd GroupAdd Interface

Interface *

--Select--

Authentication Type

--Select--

Authentication Key

Receive

Multicast

Send

Version 2

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)

Allowed Range is 1 - 255000

Multiplier

Allowed Range is 1 - 255

Minimum Transmit Interval (msec)


Allowed Range is 1 - 255000

OK

Cancel

Field	Description
Interface	Select the interface to add to the RIP group.
Authentication Type	Type of authentication: <ul style="list-style-type: none"> ◦ MD5 ◦ None ◦ Simple Password
Authentication Key	For Simple Password authentication, enter the password. It can be up to 64 characters long.
Receive	Select how to receive response message from neighboring routers: <ul style="list-style-type: none"> ◦ Multicast ◦ None
Send	Selection how to send request messages: <ul style="list-style-type: none"> ◦ None ◦ Version 2
Enable BFD (Group of Fields)	Click to enable BFD on the interface, to allow BFD to report when RIP becomes unavailable.
◦ Minimum Receive Interval	Enter the minimum time interval to receive routes, in milliseconds. <i>Range:</i> 1 through 255000 milliseconds
◦ Multiplier	Enter the multiplier value used to calculate the final minimum receive interval and minimum transmit interval. <i>Range:</i> 1 through 255
◦ Minimum Transmit Interval	Enter the time after which routes can be retransmitted, in milliseconds.

	Range: 1 through 255000 milliseconds
--	--------------------------------------

13. Click OK. The Edit Group window displays the interface.
14. Select the Network tab to configure networks in the RIP group, then click the  Add icon. In the Add RIP Instance Add Group Add Network screen, enter information for the following fields. Note that you can configure either interfaces in the RIP group (in the Interfaces tab) or networks in the RIP group (in the Networks) tab, but not both.

Add RIP Instance Add Group Add Network

Network Name *
--Select--

Authentication Type
--Select--

Authentication Key

Receive
Multicast

Send
Version 2

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)
Allowed Range is 1 - 255000

Multiplier
Allowed Range is 1 - 255

Minimum Transmit Interval (msec)
Allowed Range is 1 - 255000

OK Cancel

Field	Description
Network Name	Select the network to add to the RIP group.
Authentication Type	Type of authentication: <ul style="list-style-type: none"> MD5 None Simple Password
Authentication Key	For Simple Password authentication, enter the password. It can be up to 64 characters long.
Receive	Select how to receive response message from neighboring routers: <ul style="list-style-type: none"> Multicast None

Field	Description
Send	Selection how to send request messages: <ul style="list-style-type: none"> ◦ None ◦ Version 2
Enable BFD (Group of Fields)	Click to enable BFD on the interface, to allow BFD to report when RIP becomes unavailable.
<ul style="list-style-type: none"> ◦ Minimum Receive Interval 	Enter the minimum time interval to receive routes, in milliseconds. <i>Range: 1 through 255000 milliseconds</i>
<ul style="list-style-type: none"> ◦ Multiplier 	Enter the multiplier value used to calculate the final minimum receive interval and minimum transmit interval. <i>Range: 1 through 255</i>
<ul style="list-style-type: none"> ◦ Minimum Transmit Interval 	Enter the time after which routes can be retransmitted, in milliseconds. <i>Range: 1 through 255000 milliseconds</i>

15. Click OK. The list of configured networks displays.
16. Click OK. The Configure Virtual Router popup window displays the RIP instance.

Configure BGP

For information about configuring the Border Gateway Protocol (BGP), see [Configure BGP](#).

Configure PIM

For Releases 20.2 and later.



For information about configuring Protocol-Independent Multicast (PIM), see [Configure PIM](#) in the [Configure IP Multicast](#) article.

Configure IGMP

For Release 20.2 and later.

For information about configuring the Internet Group Management Protocol (IGMP), see [Configure IGMP](#) in the [Configure IP Multicast](#) article.

Configure Router Advertisements

1. If you are continuing from the previous section, skip to Step 6.
2. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar.
5. Click the  Add icon. The Configure Virtual Router popup window displays.
6. Select the Router Advertisement tab in the horizontal menu bar.
7. Click the  Add icon. In the Add Router Advertisement popup window, enter information for the following fields.

Add Router Advertisement

Interface Name *

--Select--

Life Time (seconds)

1800

Link MTU

Exclude

Max Advertisement Interval (seconds)

600

Min Advertisement Interval (seconds)

200

Reachable Time (milliseconds)

0

Retransmit Timer (milliseconds)

0

Managed Address Configuration

Reset

Other Stateful Configuration

Reset

Router Preference

Medium

Prefix List

 Delegated Prefix Pool

+

<

1

>

25


<input type="checkbox"/>	Prefix	Autonomous Flag	Preferred Lifetime (seconds)	Valid Lifetime (seconds)	On Link Flag
No Prefix List Added					

OK

Cancel

Field	Description
Interface Name	Select the interface to use.

Field	Description
Lifetime	Enter the default router lifetime, in seconds.
Link MTU	Include/Exclude link MTU in the router advertisement.
Maximum Advertisement Interval	Enter the maximum interval between each router advertisement message, in seconds.
Minimum Advertisement Interval	Enter the minimum interval between each router advertisement message, in seconds.
Reachable Time	Enter how long the host or router considers a neighbor as reachable until another reachability confirmation is received from that neighbor, in milliseconds.
Retransmit Timer	Enter how often to retransmit neighbor solicitation messages, in milliseconds.
Managed Address Configuration	Select whether to have the host to use a stateful autoconfiguration protocol for address autoconfiguration, in addition to any already configured stateless autoconfiguration.
Other Stateful Configuration	Select whether to enable autoconfiguration of other non-address-related information: <ul style="list-style-type: none"> ◦ Reset ◦ Set
Router Preference	Select the advertise router preference in the router advertisement: <ul style="list-style-type: none"> ◦ High ◦ Low ◦ Medium <p>When an IPv6 host receives a router advertisement message, it can use the router preference setting to select a default router.</p>

8. Select the Prefix List tab, then click the  Add icon. In the Add Router Advertisement Add Prefix List popup window, enter information for the following fields.

Add Router Advertisement Add Prefix List

Prefix

Autonomous Flag

Set

Preferred Lifetime (seconds)

Valid Lifetime (seconds)


On Link Flag

Set

OK

Cancel

Field	Description
Prefix	Enter the IP prefix.
Autonomous Flag	Select whether prefixes in the router advertisement messages are used for stateless address autoconfiguration: <ul style="list-style-type: none"> Reset Set
Preferred Lifetime	Enter how long to prefer the autoconfigured prefix, in seconds.
Valid Lifetime	Enter how long the prefix remains valid, in seconds.
On-Link Flag	Select whether the prefix advertised in a router-advertisement message is an on-link prefix: <ul style="list-style-type: none"> Reset Set

- Click OK.
- In the Add Router Advertisement screen, select the Delegated Prefix Pool tab, and then click the  Add icon.
- In the Add Router Advertisement Add Prefix List popup window, enter information for the following fields.

Add Router Advertisement Add Prefix List

Delegated Prefix Pool *

Autonomous Flag

Set

Preferred Lifetime (seconds)

Valid Lifetime (seconds)

On Link Flag

Set

OK

Cancel

Field	Description
Delegated Prefix Pool	Enter the number of delegated prefixes to include in router advertisement messages.
Autonomous Flag	Select whether prefixes in the router advertisement messages are used for stateless address autoconfiguration: <ul style="list-style-type: none"> Reset Set
Preferred Lifetime (seconds)	Enter how long to prefer the autoconfigured prefix, in seconds.
Valid Lifetime (seconds)	Enter how long the prefix remains valid, in seconds.
On Link Flag	Select whether the prefix advertised in a router-advertisement message is an on-link prefix: <ul style="list-style-type: none"> Set Reset

12. Click OK. The Add Router Advertisement popup window displays the configured router advertisements.


Configure Prefix Lists

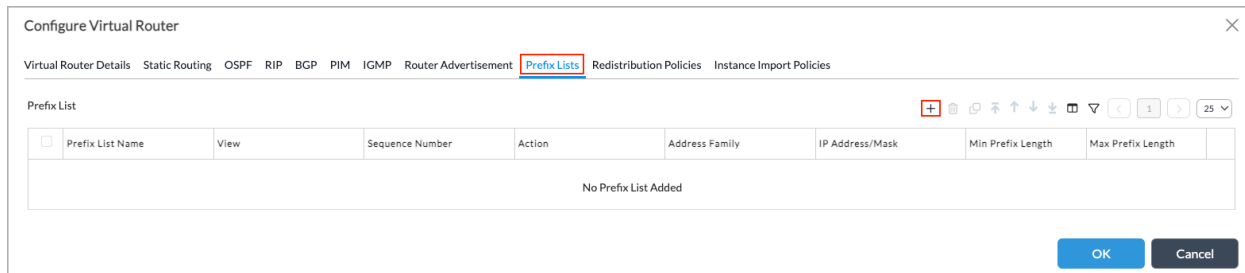
- If you are continuing from the previous section, skip to Step 6.
- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select an appliance in the main pane. The view changes to Appliance view.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Virtua...

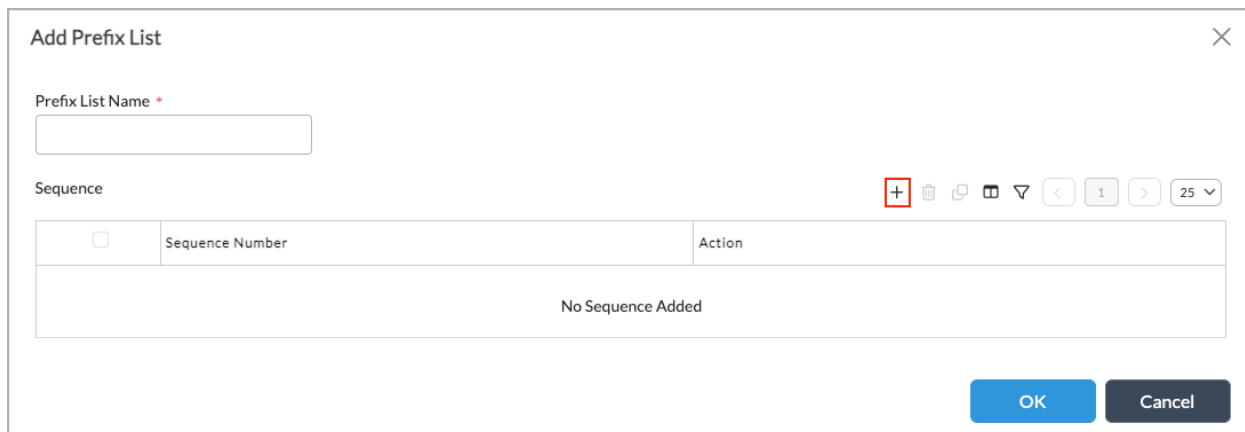
Updated: Wed, 23 Oct 2024 08:23:31 GMT


Copyright © 2024, Versa Networks, Inc.

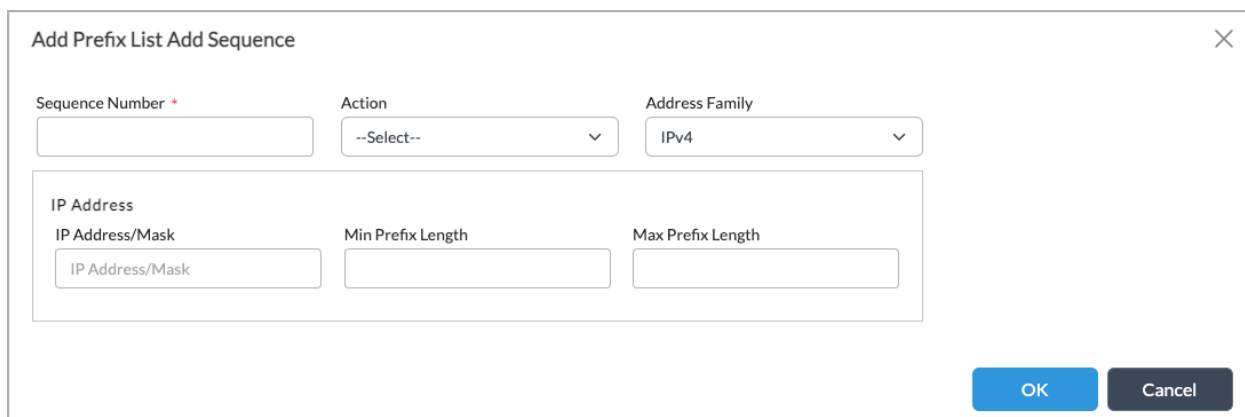
3. Select Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar.
5. Click  Add icon. The Configure Virtual Router popup window displays.
6. Select Prefix Lists tab in the horizontal menu bar.



7. Click  Add icon. The Add Prefix List window displays.



8. In the Prefix List Name field, enter a name for the prefix list.
9. In the Sequence field, click  Add icon to add a sequence. Enter information for the following fields.




Field	Description
Sequence Number	Enter a sequence number for the prefix list.
Action	Select the action to take on the routes: <ul style="list-style-type: none"> ◦ Deny—Select to deny routes on this prefix list. ◦ Permit—Select to allow routes on this prefix list.
Address Family	Select the broadcast address family protocol of the route: <ul style="list-style-type: none"> ◦ IPv4 ◦ IPv6
IP Address (Group of Fields)	
◦ IP Address/Mask	Enter the IPv4 or IPv6 prefix of the routes grouped in this prefix list.
◦ Minimum Prefix Length	Enter the minimum number of prefix length to match. For IPv4 prefix: <i>Range:</i> 0 through 32 For IPv6 prefix: <i>Range:</i> 0 through 128
◦ Maximum Prefix Length	Enter the maximum number of prefix length to match. For IPv4 prefix: <i>Range:</i> 0 through 32 For IPv6 prefix: <i>Range:</i> 0 through 128

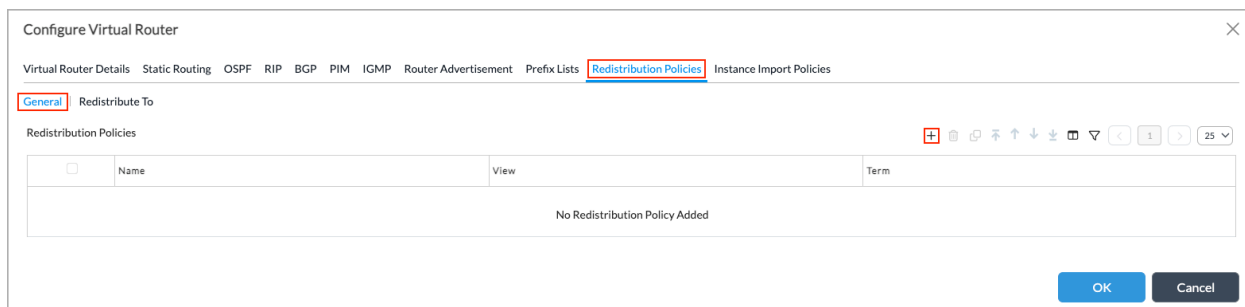
10. Click OK. The Add Prefix List popup window displays the configured sequence.
11. Click OK. The Configure Virtual Router popup window displays the configured prefix lists.

Configure Redistribution Policies


You configure redistribution policies to forward routes from one routing protocol to another protocol. You can redistribute routes among static, OSPF, and BGP. For example, to send static routes to an OSPF route, you need a redistribution policy.

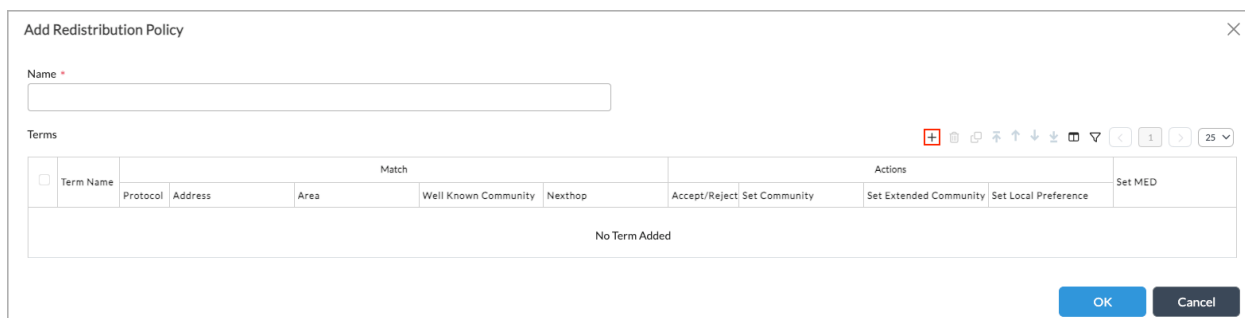
To configure redistribution policies:

1. If you are continuing from the previous section, skip to Step 6.
2. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select an appliance in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar
5. Click the  Add icon. The Configure Virtual Router popup window displays.
6. Select the Redistribution Policies tab in the horizontal menu bar.



The screenshot shows the 'Configure Virtual Router' window with the 'Redistribution Policies' tab selected. The 'General' sub-tab is active, showing a 'Redistribute To' section. Below this is a table for 'Redistribution Policies' with columns for Name, View, and Term. The table is currently empty, displaying 'No Redistribution Policy Added'. At the bottom right are 'OK' and 'Cancel' buttons.

7. Click the  Add icon.
8. In the Add Redistribution Policy popup window, enter the name of the policy in the Name field.



The screenshot shows the 'Add Redistribution Policy' window. It has a 'Name' field at the top. Below it is a 'Terms' section with a table. The table has columns for Term Name, Match (Protocol, Address, Area, Well Known Community, Nexthop), and Actions (Accept/Reject, Set Community, Set Extended Community, Set Local Preference, Set MED). The table is currently empty, displaying 'No Term Added'. At the bottom right are 'OK' and 'Cancel' buttons.

9. Click the  Add icon. In the Add Redistribution Policy Add Term window, enter information for the following fields.

Add Redistribution Policy Add Term

Term Name *

Match

Action

Protocol

--Select--

Route Type

--Select--

Address

IPv4 Or IPv6 Address/Prefix

Area

OSPF Tag

Static Tag

Well Known Community

--Select--

Community

Extended Community

Prefix Filter

--Select--

Nexthop Filter

--Select--

Nexthop

IPv4 Or IPv6 Address/Prefix

☒ Monitor
☐ Monitor Group

Monitor

--Select--

Monitor Group

--Select--

State

--Select--

OK

Cancel

Field	Description
Term Name	Enter a name for the term in the redistribution policy. The first instance created is evaluated first by the policy rule, and the remaining terms are evaluated in the order they are listed in the term name table.

10. Select the Match tab to define redistribution policy match conditions. Enter information for the following fields.

Field	Description
Protocol	Select the protocol to match for redistribution: <ul style="list-style-type: none"> ◦ BGP ◦ DHCP ◦ Direct ◦ OSPF ◦ RIP ◦ SD-WAN ◦ Static
Route Type	Select the route type for the protocol.
Address	Enter the IPv4 or IPv6 address of the route to match.
Area	Enter the OSPF area to match.

Field	Description
OSPF Tag	Enter the OSPF tag to match.
Static Tag	Enter the OSPF static tag to match.
Well-Known Community	<p>(For Releases 21.2.1 and later.) Select a well-known community:</p> <ul style="list-style-type: none"> ◦ no_advertise—A BGP speaker that receives a route containing this community value must not advertise the route to any external or internal peer. ◦ no_export—A BGP speaker that receives a route containing this community value must not advertise the route to its external BGP peers. However, the BGP speaker can advertise the route to its IBGP peers and to confederation peers in other member ASs within its local confederation. ◦ no_export_subconfed—A BGP speaker that receives a route containing this community value must not advertise the route to any external peer including peers in other member ASs within its confederation. <p>If you select a well-known community, you cannot also configure a string in the Community field.</p>
Community	<p>Enter the BGP community string to match.</p> <p>A BGP community is a group of destinations with a common property. This path attribute in BGP update messages identifies community members and performs actions at a group level instead of to an individual level. BGP communities help identify and segregate BGP routes, enabling a smooth traffic flow.</p> <p>If you configure a community string, you cannot also select a community in the Well-Known Community field.</p>
Extended Community	Enter the extended BGP community identifier.
Prefix Filter	Name of the prefix list that defines the terms for the route prefixes to be advertised.

Field	Description
Next-Hop Filter	Name of the prefix list that defines the terms for matching the next hop of the route.
Next Hop	Enter the next-hop address for the route.
Monitor	Name of the monitor used for liveness detection, the state of which should be matched.
Monitor Group	Name of the monitor-group used for liveness detection, the state of which should be matched.
State	State of the monitor or monitor group to match.

11. Select the Action tab to define redistribution policy action conditions. Enter information for the following fields.

Add Redistribution Policy Add Term

Term Name *

Match
Action

Accept/Reject
Accept

Set

Well Known Community
--Select--

Community

Extended Community

Local Preference

MED

Origin
Remote IGP

OSPF Tag

☐ OSPF Metric to BGP MED
☐ OSPF Metric to BGP Local Preference

Metric

Metric Conversion
--Select--

OSPF External Type
--Select--

Route Preference

Standby

Metric

Metric Conversion
--Select--

Local Preference

VRRP

Standby Local Preference

Standby Metric


OK
Cancel

Field	Description
Accept/Reject	<p>Select the action to take for the route:</p> <ul style="list-style-type: none"> ◦ Accept—Accept all the traffic for the route. ◦ Reject—Rejects all the traffic for the route.
Set (Group of Fields)	
<ul style="list-style-type: none"> ◦ Well-Known Community 	<p>(For Releases 21.2.1 and later.) Select a well-known community:</p> <ul style="list-style-type: none"> ◦ no_advertise—A BGP speaker that receives a route containing this community value must not advertise the route to any external or internal peer. ◦ no_export—A BGP speaker that receives a route containing this community value must not advertise the route to its external BGP peers. However, the BGP speaker can advertise the route to its IBGP peers and to confederation peers in other member ASs within its local confederation. ◦ no_export_subconfed—A BGP speaker that receives a route containing this community value must not advertise the route to any external peer including peers in other member ASs within its confederation. <p>If you select a well-known community, you cannot also configure a string in the Community field.</p>
<ul style="list-style-type: none"> ◦ Community 	<p>Enter the BGP community string to match.</p> <p>A BGP community is a group of destinations with a common property. This path attribute in BGP update messages identifies community members and performs actions at a group level instead of to an individual level. BGP communities help identify and segregate BGP routes, enabling a smooth traffic flow.</p> <p>If you configure a community string, you cannot also select a community in the Well-Known Community field.</p>

Field	Description
◦ Extended Community	Enter the BGP extended community identifier to add to the route.
◦ Local Preference	Enter the local BGP preference to add to the route.
◦ MED	Enter the multiexit BGP discriminator to add to the route.
◦ Origin	For BGP, select the source of the BGP route: <ul style="list-style-type: none"> ◦ Local EGP ◦ Remote IGP ◦ Unknown Heritage
◦ OSPF Tag	For OSPF, enter the OSPF tag to add to the route.
◦ OSPF Metric to BGP MED	For routes being redistributed from OSPF to BGP, click to set the MED of BGP route to the same value as the OSPF metric.
◦ OSPF Metric to BGP Local Preference	For routes being redistributed from OSPF to BGP, click to set the local preference of BGP route to a mapped value from OSPF metric (4294967295 minus the OSPF metric).
Metric	Enter a value to determine how one route should be chosen over another: <ul style="list-style-type: none"> ◦ Bandwidth ◦ Communication cost ◦ Hop count ◦ Load ◦ MTU ◦ Path cost ◦ Path length
Metric Conversion	Select the conversion factor for the metric value: <ul style="list-style-type: none"> ◦ Inverse ◦ Scale Down ◦ Scale Up

Field	Description
	<ul style="list-style-type: none"> ◦ Set ◦ Truncate
OSPF External Type	<p>Select the OSPF external type to use when distributing a route to OSPF:</p> <ul style="list-style-type: none"> ◦ E1 ◦ E2
Route Preference	Enter a value for the route preference.
Standby (Group of Fields)	Configure interchassis HA standby metrics.
<ul style="list-style-type: none"> ◦ Metric 	Enter the metric value for the interchassis HA standby.
<ul style="list-style-type: none"> ◦ Metric Conversion 	<p>Select how to convert the for metric value from a route during redistribution:</p> <ul style="list-style-type: none"> ◦ Inverse ◦ Scale Down ◦ Scale Up ◦ Set ◦ Truncate
<ul style="list-style-type: none"> ◦ Local Preference 	Enter the local preference to use during the route redistribution.
VRRP (Group of Fields)	
<ul style="list-style-type: none"> ◦ Standby Preference 	Enter the standby preference to use when exporting the prefix corresponding to the subnet of the interface in VRRP backup state.
<ul style="list-style-type: none"> ◦ Standby Metric 	Enter the metric value to set while the device is in VRRP backup state.

12. Click OK. The Add Redistribution Policy popup window displays the configured policies.

13. In the Configure Virtual Router > Redistribution Policies screen, select the Redistribute To tab, and click the  Add icon. Enter information for the following fields.

Add Redistribute To
✕

From RIB *

--Select--

Destination *

--Select--

Policy Name *

--Select--

OK

Cancel

Field	Description
From RIB	Select the route table from which the redistribution occurs: <ul style="list-style-type: none"> inet-multicast-rib inet-unicast-rib inet6-multicast-rib inet6-unicast-rib
Destination	Select the destination to which the redistribution occurs: <ul style="list-style-type: none"> bgp inet-multicast-rib inet6-multicast-rib ospf rip
Policy Name	Select the name of the redistribution policy to use.

- Click OK. The Configure Virtual Router popup window displays the configured redistribution policies.

Configure Instance Import Policies

- If you are continuing from the previous section, skip to Step 6.
- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.

- c. Select an appliance in the main pane. The view changes to Appliance view.
3. Select the Configuration tab in the top menu bar.
4. Select Networking > Virtual Routers in the left menu bar.
5. Click the **+** Add icon. The Configure Virtual Router popup window displays.
6. Select the Instance Import Policies tab in the horizontal menu bar.

Configure Virtual Router

Virtual Router Details Static Routing OSPF RIP BGP PIM IGMP Router Advertisement Prefix Lists Redistribution Policies **Instance Import Policies**

+ 1 25

<input type="checkbox"/>	From Instance	View	Family	Policy Name	From SAFI	To SAFI
No Import Policies Added						

OK Cancel

7. Click the **+** Add icon and enter information for the following fields.

Add Import Policies

From Instance *

Family

Policy Name

From SAFI

To SAFI

OK Cancel

Field	Description
From Instance	Select the instance to use for the import policies.
Family	Select the address family of the routes.
Policy Name	Select the name of the redistribution policy.
From SAFI	Select the subsequent address family identifier from which to import the policy: <ul style="list-style-type: none"> ◦ Multicast ◦ Unicast
To SAFI	Select the subsequent address family identifier to which to export the policy: <ul style="list-style-type: none"> ◦ Multicast ◦ Unicast

- Click OK. The Configure Virtual Router popup window displays the configured import policies.

Default Routing Preferences

The following table lists the default values for route preferences, also referred to as administrative distances. The route with the lowest preference is the most likely to become the active route.

Route Source	Default Preference
Connected	0
Static	1
EBGP	20
OSPF internal	30
OSPF external	110
RIP	120
IBGP	200

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.2.1 adds the following BGP configuration fields: AS Path Ignore, AS Path Multipath Relax, Community 4-Byte, Relax Rirst AS Check, Soft Reconfiguration, Suppress Peer AS, Weight, and Well-Known Community.
- Release 22.1.1 adds support for OSPF sham links, SLA profiles tab for BGP, peer and peer group policy match and actions based on SLA parameters, and AS mode 5.

Additional Information

[Configure BGP](#)

[Configure Interchassis HA](#)

[Configure IP Multicast](#)

[Configure IP SLA Monitor Objects](#)

[Troubleshoot Routing Protocols](#)