

Configure BGP

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


The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that is used for exchanging routing information between gateway hosts in a network. BGP is often the protocol used between gateway hosts on the Internet.


This article describes how to configure BGP on Versa Operating System™ (VOS™) devices.

Start Configuring BGP

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a post-staging template 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 BGP tab.

Configure Basic BGP

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the General tab, and enter information for the following fields.

Add BGP Instance

General

Prefix List

SLA Profile

Peer/Group Policy

Peer Group

Route Aggregation

Damping Policy

Versa Private TLV

Advanced

Description

Router ID *

IPv4 Address

Hold Time (seconds)

Allowed Range is 3 - 65535

IBGP Preference

Allowed Range is 1 - 255

SLA Community

Passive

Site Of Origin

Instance ID *

Allowed Range is 1 - 65535

Local AS *

0 to 4294967295 Or <0.65535>.<0.65535>

TTL

Allowed Range is 1 - 255

EBGP Preference

Allowed Range is 1 - 255

Suppress Peer AS

Remove All Private AS#

Soft Reconfiguration

Peer AS

1 to 4294967295 Or <0.65535>.<0.65535>

Password

Relax First AS Check

Route Reflector Client

Local AS Mode

--Select--

Local Address

IP Address Or Interface

Local Network Name

--Select--

AS Origination Interval

Allowed Range is 1 - 65535

Community 4 byte

Enable Alarms

Prefix Limit

Maximum

Allowed Range is 1 - 2147483647

Threshold

Allowed Range is 1 - 100


Restart Interval

Allowed Range is 30 - 86400

Action

Drop

Family | Debug

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	
		Maximum	Threshold				
--Select--	Allowed Range is 1 - 255	Allowed Range is 1 - 214	Allowed Range is 1 - 100	Allowed Range is 30 - 86400	--Select--	<input type="checkbox"/> Soft Reconfiguration	
No Records to Display							

OK

Cancel

Field	Description
Description	Enter a text description for the BGP instance.
Instance ID (Required)	Enter the ID assigned of the BGP instance. A virtual router can have multiple BGP instances. <i>Range:</i> 1 through 65535
Disable	Disable all static neighbors in the BGP instance
Router ID (Required)	Enter the IP address of the router. Click the Tool icon

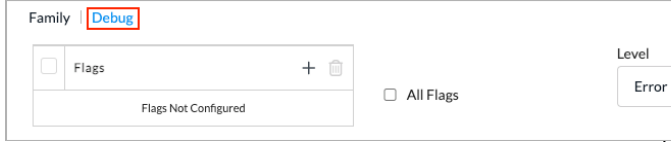
Field	Description
	to parameterize the value for this field.
Local AS (Required)	Enter the local AS number. Click the Tool icon to parameterize the value for this field. <i>Range:</i> 0 through 4294967295, or (0 through 65535.0 through 65535)
Peer AS	Enter the remote peer's AS number. Click the Tool icon to parameterize the value for this field. <i>Range:</i> 0 through 4294967295, or (0 through 65535.0 through 65535)
Local Address	Select the IP address or interface of the BGP instance. Click the Tool icon to parameterize the value for this field.
Hold Time	Enter the hold time, in seconds, to negotiate with a peer. <i>Range:</i> 3 through 65535 seconds
TTL	Enter the time-to-live value, which is the number of hops that a packet can travel in a network before the packet expires. <i>Range:</i> 1 through 255 <i>Default for EBGp:</i> 64 (Note that you do not need to enable EBGp multihop.) <i>Default for IBGP:</i> 64
Password	Enter the password to authenticate the BGP instance.
Local Network Name	Select the network to which the BGP instance belongs. The drop-down lists the names of user-defined networks.
IBGP Preference	Enter the preference value to assign to routes learned from IBGP. <i>Range:</i> 1 through 255 <i>Default:</i> 200

Field	Description
EBGP Preference	<p>Enter the preference value to assign to routes learned from EBGP.</p> <p><i>Range:</i> 1 through 255</p> <p><i>Default:</i> 20</p>
Local AS Mode	<p>Select the BGP AS mode to use on the local device:</p> <ul style="list-style-type: none"> ◦ 1—Peering session is established with the local AS configured in BGP instance or with a BGP group or neighbor. When importing routes, an AS number is not inserted in the AS path. When exporting routes, the selected local AS number is prepended to the AS path. ◦ 2—Peering session is established with local AS configured as a BGP group or neighbor. When importing routes, the local AS number of the group or neighbor is inserted in AS path. When exporting routes, the local AS number configured on the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to the AS path. This is the default. ◦ 3—Peering session is established with the local AS configured for the BGP group or neighbor. When importing routes, no AS number is inserted in the AS path. When exporting routes, the local AS configured for the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to AS path. ◦ 4—Peering session is established with the local AS number configured for the BGP group or neighbor. When importing routes, no AS number is inserted in the AS path. When exporting routes, the local AS number configured for the BGP group or neighbor is prepended to the AS path. ◦ 5—(For Releases 22.1.1 and later.) Peering session is established with the local AS number configured for the BGP group or neighbor. When importing routes, the local AS in the BGP group or neighbor is inserted in the AS path. When exporting routes, the local AS number configured in the BGP group or neighbor is prepended to the AS path. <p><i>Default:</i> 2</p>

Field	Description
AS Origination Interval	<p>Enter the minimum time that must elapse between successive advertisements of Update messages that report changes within the advertising BGP speaker's own AS.</p> <p><i>Range:</i> 1 through 65535</p>
SLA Community	Enter the extended community value to use for SLAs.
Suppress Peer AS	(For Releases 21.2.1 and later.) Click to suppress and not advertise routes received from an EBGP neighbor to another neighbor that is in the same AS as originating neighbor.
Relax First AS Check	(For Releases 21.2.1 and later.) Click to relax the check that the first (left-most) AS number in an AS path receives from an EBGP neighbor is same as neighbor's AS.
Community 4 Byte	(For Releases 21.2.1 and later.) Click to process the community using 4-byte AS numbers.
Passive	Click to have BGP only accept traffic, and not transmit routes.
Remove All Private AS Numbers	Click to remove all private AS numbers from a route's AS path of the route before sending the route to peers.
Route Reflector Client	Click to have an IBGP router function as a route reflector. A route reflector broadcasts the routes of all the other routers in the network
Enable Alarms	Click to enable alarm generation.
Site of Origin	Enter the site-of-origin community to use while redistributing routes.
Soft Reconfiguration	(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects the routes.

Field	Description
Prefix Limit (Group of Fields)	Limit the number of prefixes received from a session with a BGP neighbor.
<ul style="list-style-type: none"> Maximum 	<p>Enter the maximum number of prefixes that can be received from the BGP neighbor.</p> <p><i>Range:</i> 1 through 2147483647</p>
<ul style="list-style-type: none"> Threshold 	<p>Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reach, the VOS device sends an SNMP trap warning message.</p> <p><i>Range:</i> 1 through 100 percent</p>
<ul style="list-style-type: none"> Restart Interval 	<p>When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached.</p> <ul style="list-style-type: none"> <i>Range:</i> 30 through 86400 seconds
<ul style="list-style-type: none"> Action 	<p>Select the action to take when the maximum prefix limit is exceeded:</p> <ul style="list-style-type: none"> Drop—Drop the BGP session to the neighbor. Warn—Send a warning message.
Family (Group of Fields)	Configure the following fields, and then click the Add icon to add a BGP family.
<ul style="list-style-type: none"> Family 	<p>Select the protocol for the family:</p> <ul style="list-style-type: none"> IPv4 Layer 3 VPN Unicast—Use for Layer 3 VPN. IPv4 Multicast—Use for BGP. IPv4 Unicast—Use for BGP. IPv4 Versa Private—Use for SD-WAN. IPv4 VPN Multicast—Use for Layer 3 VPN. IPv6 Multicast—Use for BGP.

Field	Description
	<ul style="list-style-type: none"> ◦ IPv6 VPN Multicast—Use for Layer 3 VPN. ◦ IPv6 Unicast—Use for BGP. ◦ IPv6 VPN Unicast—Use for Layer 3 VPN. ◦ L2VPN EVPN—Use for Layer 2 VPN.
<ul style="list-style-type: none"> ◦ Loop Count 	<p>Enter the number of times the detection of the local device's AS in the AS PATH attribute is allowed for the BGP address family. If the count exceeds the loop count value, the system discards the route.</p> <p><i>Range:</i> 1 through 255</p>
<ul style="list-style-type: none"> ◦ Prefix Limit 	<p>Limit the number of prefixes received from a session with a BGP neighbor:</p> <ul style="list-style-type: none"> ◦ Maximum—Enter the maximum number of prefixes that can be received from the BGP neighbor. <i>Range:</i> 1 through 2147483647 ◦ Threshold—Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reach, the VOS device send an SNMP trap warning message.. <i>Range:</i> 1 through 100 percent
<ul style="list-style-type: none"> ◦ Restart Interval 	<p>When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached.</p> <p><i>Range:</i> 30 through 86400 seconds</p>
<ul style="list-style-type: none"> ◦ Action 	<p>Select the action to take when the maximum prefix limit is exceeded:</p> <ul style="list-style-type: none"> ◦ Drop—Drop the BGP session to the neighbor. ◦ Warn—Send a warning message.
<ul style="list-style-type: none"> ◦ Soft Reconfiguration 	<p>(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects</p>

Field	Description
	the routes.
Debug (Group of Fields)	
Flags Table	Click the + Add icon to select a debug flag. You can add multiple debug flags.
All Flags	Click to use all debug flags.
Level	Select a debug level.

9. Click OK.

Configure BGP Prefix Lists

Peer group policy uses prefix lists to change the attributes of routes, and to allow or deny advertising routes to the peer routers.

To configure a BGP prefix list:

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab. The main pane displays a list of the BGP instances that are already configured.
7. Click the **+** Add icon. The Add BGP Instance popup window displays.
8. Select the Prefix List tab.

Add BGP Instance ✕

General **Prefix List** SLA Profile Peer/Group Policy Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

+ 🗑️ 📄 📄 🔍 < 1 > 25 ▾

<input type="checkbox"/>	Prefix List Name	Sequence Number	Action	Address Family	SAFI	IP Address/Mask	Min Prefix Length	Max Prefix Length
No Prefix List Added								

OK
Cancel

9. Click the **+** Add icon. The Add BGP Instance Add Prefix List popup window displays.

Add BGP Instance Add Prefix List ✕

Prefix List Name *

Sequence

+ 🗑️ 📄 📄 🔍 < 1 > 25 ▾

<input type="checkbox"/>	Sequence Number	Action
No Sequence Added		

OK
Cancel

10. Click the **+** Add icon to add a prefix list. Enter information for the following fields.

Add BGP Instance Add Prefix List Add Sequence ✕

Sequence Number *

Action

--Select-- ▾

Address Family

IPv4 ▾

SAFI *

Unicast ▾

IP Address

IP Address/Mask

IP Address/Mask

Min Prefix Length

Max Prefix Length

OK
Cancel

Field	Description
Sequence Number (Required)	Enter a number for the order or sequence number of the prefix list.

Field	Description
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 family protocol of the route: <ul style="list-style-type: none"> ◦ IPv4 ◦ IPv6
SAFI (Required)	Select the subaddress family indicator.
IP Address (Group of Fields)	Configure an IP address to group the routes for this prefix list.
<ul style="list-style-type: none"> ◦ IP Address/Mask 	Enter the IPv4 or IPv6 address of the routes grouped in this prefix list.
<ul style="list-style-type: none"> ◦ 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
<ul style="list-style-type: none"> ◦ 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

11. Click OK.

Configure a BGP SLA Profile

For Releases 22.1.1 and later.

A peer group policy can use SLA parameters to change the attributes of routes, and to allow or deny the advertising of routes to the peer routers. You define SLA parameters in SLA profiles, and you can use the profiles in match lists for peer and peer group policies.

Before configuring an SLA profile, you can do the following:

- For better control plane performance, enable soft reconfiguration. You can enable it for the BGP instance, the peer group, or neighbor (peer).
- Configure an application monitor on the gateway for the application. The application monitor collect metrics, as seen from the gateway, for traffic sent towards a SaaS application. The gateway sends the application monitor metrics to directly connected SD-WAN branches. Branches receive metrics from multiple gateways, and they can use the metrics to select the best path towards the SaaS application. For more information, see [Add a SaaS Application Monitor](#) in [Configure SaaS Application Monitoring](#).

Add SaaS App Monitor

Name * Monitor Type * Monitoring Threshold Monitoring Interval(s)

Destination Port Predefined SaaS Group FQDN / Host Address * ☐ Default LEF Profile

☐ Response Codes
Response Codes Not Configured

☒ Local Organizations *
Tenant1

☒ Export Organizations
Tenant1

☒ Routing Instances *
Internet1-Transport-VR
Internet2-Transport-VR

Response Code Ranges
Low High

Export Threshold
Export Threshold Latency(ms) Export Threshold Loss(%)

Traceroute
Up Interval (min) Down Interval (min)

- Configure SD-WAN traffic engineering. Note that for end-to-end metric comparison, the path metrics that you use in the traffic-engineering configuration must be consistent with the threshold that you configure for the BGP SLA profile used for end-to-end metric comparison. For example, if you use delay for best SLA selection in the SLA profile, you must configure the delay in path metrics for traffic engineering. For more information, see [Configure SD-WAN Traffic Engineering](#).

Edit Traffic Engineering

Slam

Advertisement Interval (sec)

15

Advertise Latency Duration (sec)

20

Advertise Loss Duration (sec)

60

Forwarding Profile

---Please Select---

☒ Advertise Remote

☒ No Transit

Forwarding Class

Forwarding Class *	Include	Path Metrics	Export		Ecmp		
			Latency Change Threshold(%)	Loss Change Threshold(%)	Latency Tolerance(milliseco...	Loss Tolerance(%)	
---Please Sel	<input type="checkbox"/>	latency	10	2	10	1	+
fc_ef	true	latency,loss	40	2	10	1	✎ ✕

OK

Cancel

To configure a BGP SLA profile:

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab. The main pane displays a list of the BGP instances that are already configured.
7. Click the **+** Add icon. The Add BGP Instance popup window displays.
8. Select the SLA Profile tab.

Add BGP Instance

General

Prefix List

SLA Profile

Peer/Group Policy

Peer Group

Route Aggregation

Damping Policy

Versa Private TLV

Advanced

+

✕

📄

🔍

1

25

<input type="checkbox"/>	Profile Name	Sequence Number	Application Monitor	SLA Measurement Scope	Best Nexthop Selection	Latency (milliseconds)	Loss (%)	Forwarding Class
No SLA Profile Added								

OK

Cancel

9. Click the  Add icon. The Add BGP Instance Add SLA Profile popup window displays.

Add BGP Instance

Add SLA Profile

✕

Profile Name *

Sequence

+

🗑️

📄

📅

🔍

<

>

25

<input type="checkbox"/>	Sequence Number	Application Monitor
No Sequence Added		

OK

Cancel

10. Enter a name for the SLA profile, and then click the  Add icon. In the Add BGP Instance Add SLA Profile Add Sequence popup window, enter information for the following fields.

Add BGP Instance

Add SLA Profile

Add Sequence

Sequence Number *

Application Monitor

SLA Measurement Scope

Best Nexthop Selection Criteria

Max Threshold

Latency (milliseconds)

Loss (%)

Forwarding Class

OK

Cancel

Field	Description
Sequence Number (Required)	<p>Enter a number for the sequence.</p> <p><i>Range:</i> 0 through 4,294,967,295</p> <p><i>Default:</i> None</p>
Application Monitor	Enter the name of an SaaS application monitor.
SLA Measurement Scope	Select the SLA measurement scope to use for end-to-end path metrics:

Field	Description
	<ul style="list-style-type: none"> ◦ Gateway to Application ◦ Site to Application ◦ Site to Gateway
Best Next-Hop Selection Criteria	<p>Select the criteria to use for selecting the next hop among multiple gateways:</p> <ul style="list-style-type: none"> ◦ Best Score—Select the SLA with the best Versa link score (VLS). ◦ Least Latency—Select the SLA with the least latency. ◦ Least Packet Loss—Select the SLA with the least packet loss.
Maximum Threshold (Group of Fields)	<p>Configure the maximum threshold for end-to-end path metrics. Note that the threshold settings must be consistent with the SD-WAN traffic-engineering path metrics to ensure that the data path used for traffic is consistent with the next-hop selection for BGP that is based on SLA profiles.</p>
<ul style="list-style-type: none"> ◦ Latency 	<p>Enter the maximum latency, in milliseconds. The path metrics in the traffic-engineering configuration must be consistent with the SLA profile</p>
<ul style="list-style-type: none"> ◦ Loss 	<p>Enter the maximum loss, as a percentage.</p>
Forwarding Class	<p>Select a forwarding class to use for SLA measurement.</p> <p><i>Range: 0 through 15</i></p>

11. Click OK.

For an example of configuring SLA-based routing, see [Example of Configuring BGP SLA-Based Routing](#), below.

Configure BGP Peer and Peer Group Policy

A peer group policy filters the routes defined in the BGP prefix list. For matching routes, the policy can change route attributes. The policy allows or denies the advertising of these routes to the peers.

BGP peer and peer group policies consist of one or more terms for filtering BGP routes that are received from or

advertised to remote BGP peers. The policy executes terms in the order in which they are listed in the term name table. Each term consists of match conditions and actions to apply to matching routes. If a route matches, an Accept or Reject action is performed by an accept term or a reject term.



A Reject term results in the rejection of the route, and no further terms are evaluated.

An Accept term sets route attributes. A BGP peer and peer group policy has the following types of Accept terms :

- Generic Accept term—Terms that are configured with the Accept action and that are not part of an AND series or an OR series. For these types of terms, the policy collects the route attributes listed on the Action tab and then continues with the next term.
- AND series—A sequence of Accept terms. The policy evaluates all terms in the sequence, and if all the terms result in a match, the policy collects the route attributes listed on the Action tab of the last term. Route attributes for other terms in the series are ignored. Evaluation continues with the next term after the AND series. You create an AND series by configuring a sequence of terms using the Next-Term field, and, in all but the last term, selecting the value AND Series in the Next-Term Action field.
- OR series—A sequence of Accept terms. The policy evaluates the terms in the sequence in order, and, for the first matching term in the series, the policy collects the route attributes listed on the Action tab for that term. After a term matches, the remaining terms in the OR series are not evaluated. Evaluation continues with the next term after the OR series. You create an OR series by configuring a sequence of terms using the Next-Term field, and, in all but the last term, selecting value OR Series in the Next-Term Action field. An example OR series configuration is shown in [Configure Support for ECMP across Gateways](#), below.

If the policy evaluation completes the last term without rejecting the route, all attributes that are collected for accept terms, AND series, and OR series are applied to the route.

To configure a peer and peer group policy:

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Peer/Group Policy tab.


Add BGP Instance

General Prefix List SLA Profile Peer/Group Policy Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

☐ Peer/Group Policy Name Term Name Action

No Routing Peer Policy Added

OK Cancel

9. Click the  Add icon. The Add BGP Instance Add Peer/Group Policy popup window displays.

Add BGP Instance Add Peer/Group Policy


Name *

Terms

☐ Term Name

No Term Added

OK Cancel

10. Enter a name for the peer group policy, and then click OK.
11. Click the  Add icon. In the Add BGP Instance Add Peer/Group Policy Add Term popup window, select the Match tab and then enter information for the following fields.

Add BGP Instance Add Peer/Group Policy Add Term

Term Name *

Match

Action

Standby Action

Family
--Select--

AS Path

Metric

NLRI
--Select--

Source Address
--Select--

Nexthop
--Select--

Well Known Community
--Select--

Community

Extended Community

Origin
--Select--

SLA Profile
Name
--Select--

Nexthop Name
--Select--

Local Circuit Name
--Select--

Nexthop List
☐ Nexthop List
+

Local Circuit List
☐ Local Circuit List
+

Nexthop List Not Configured

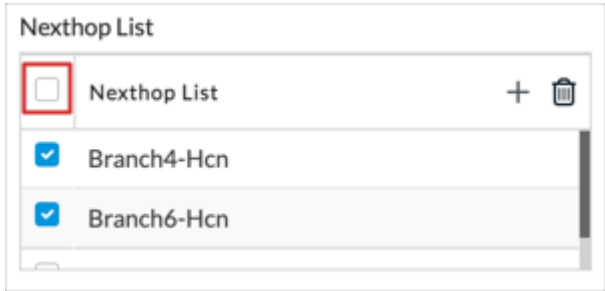
Local Circuit List Not Configured



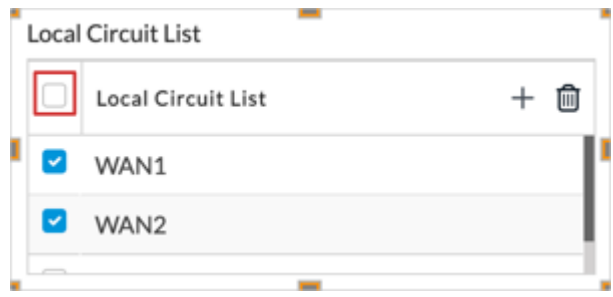

OK

Cancel

Field	Description
Term Name (Required)	Enter a name for the policy term. Note that a policy executes terms in the order in which they are listed in the Term Name table.
Family	<p>Select the protocol family to match:</p> <ul style="list-style-type: none"> IPv4 Layer 3 VPN Unicast—Use for Layer 3 VPN. IPv4 Multicast—Use for BGP. IPv4 Unicast—Use for BGP. IPv4 Versa Private—Use for SD-WAN. IPv4 VPN Multicast—Use for Layer 3 VPN. IPv6 Multicast—Use for BGP. IPv6 Unicast—Use for BGP. IPv6 VPN Multicast—Use for Layer 3 VPN. IPv6 VPN Unicast— Use for Layer 3 VPN. L2VPN EVPN—Use for Layer 2 VPN.

Field	Description
AS Path	Enter the number of the AS path to match.
Metric	Enter the BGP multiple exit discriminator (MED) value to match.
NLRI	Select the network layer reachability information (NLRI) from the user-defined prefix lists to match.
Source Address	Select the source address of the prefix list from the list of user-defined prefix lists to match.
Next Hop	Select the IP address of the prefix list to use as the next hop from the user-defined prefix lists to match.
Well-Known Community	<p>(For Releases 21.2.1 and later.) Select a well-known community to match:</p> <ul style="list-style-type: none"> ◦ no_advertise—A BGP device that receives a route containing this community value must not advertise the route to any external or internal peer. ◦ no_export—A BGP device that receives a route containing this community value must not advertise the route to its external BGP peers. However, the BGP device 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 device 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</p>

Field	Description
	<p>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 string to match. In an extended community, you can group a larger number of destinations than in a community.
Origin	<p>Select the source of the route:</p> <ul style="list-style-type: none"> ◦ Local EGP ◦ Remote IGP ◦ Unknown Heritage
SLA Profile (Group of Fields)	(For Releases 22.1 and later.)
◦ Name	Select an SLA profile.
◦ Next Hop	Select a next hop. You can select an individual next hop in this field, or you can configure a list of next hops in the Next-Hop List field.
◦ Local Circuit Name	Select a local circuit name. You can select an individual local circuit in this field, or you can configure a list or circuits in the Local Circuit List field.
◦ Next-Hop List	<p>Select the sites to include in the next-hop list by clicking the box preceding the site name in the Next-Hop List table. A <input checked="" type="checkbox"/> checked blue box indicates that a site is selected.</p> 

Field	Description
	<p>To select or deselect all the sites in the table, click Next-Hop List.</p> <p>To add sites to the table, click the  Add icon and then choose a site.</p>
<ul style="list-style-type: none"> Local Circuit List 	<p>Select local circuits to include in the local circuit list by clicking the box preceding the circuit name in the Local Circuit table. A  checked blue box indicates that a circuit is selected. The circuit names in the local circuit list are considered for best circuit selection to reach the best next hop from the next-hop list. If you do not configure a local circuit list, the local circuit with the best SLA is used.</p>  <p>To select or deselect all circuits in the table, click Local Circuit List.</p> <p>To add circuits to the table, click the  Add icon and then choose a circuit.</p>

- Select the Action tab to enter information for the action to take for routes that meet the match criteria. Enter information in the following fields.

Add BGP Instance Add Peer/Group Policy Add Term

Term Name *

Match

Action

Standby Action

Accept/Reject

Accept

Damping

☐ Enable ECMP for BGP Routes in RIB

Origin

--Select--

Nexthop

Local Preference

Allowed Range is 0 - 2147483647

AS Path

--Select--

Local AS Prepend Count

Allowed Range is 1 - 255

AS Path Prepend

Allowed Range is 1 - 4294967295

Community Action

--Select--

☐ SLA Community Action

Well Known Community

--Select--

Community

Route Preference

Extended Community Action

--Select--

Extended Community

Metric Action

--Select--

Metric

Allowed Range is 1 - 4294967295

Next Term

--Select--

Weight

Allowed Range is 1 - 2147483647

Next Term Action

--Select--

OK

Cancel

Field	Description
Accept/Reject	Select whether to either accept or reject the route.
Damping	Enter a value for BGP route-flap damping.
Enable ECMP for BGP Routes in RIB	Select to perform ECMP for BGP paths in the route table. BGP performs equal-cost multipath load balancing when two or more routes have the same administrative distance.
Origin	Select the source of the route: <ul style="list-style-type: none"> Local EGP Remote IGP Unknown Heritage
Next Hop	Enter the IP address of the next hop.

Field	Description
Local Preference	<p>Enter local preference value to use to choose the outbound external BGP path.</p> <p><i>Range:</i> 0 through 2147483647</p>
AS Path	<p>Select a regular expression to match the AS path for the route:</p> <ul style="list-style-type: none"> ◦ No AS path action. ◦ Prepend the local AS path the number of times specified in the Local AS Prepend Count (local-as-prepend-count) field. ◦ Remove all the AS numbers that match those specified in the Match AS Path (match as-path) field. ◦ Remove all the AS numbers that match those specified in the Match AS Path (match as-path) field, and prepend the local AS the number of times specified in the Local AS Prepend Count (local-as-prepend-count) field.
Local AS Prepend Count	<p>Enter the number of times to prepend the local AS number to the AS path.</p> <p><i>Range:</i> 1 through 255</p>
AS Path Prepend	<p>Enter the number of times to prepend the AS number to the AS path.</p> <p><i>Range:</i> 1 through 4294967295</p>
Community Action	<p>Select how to match the community list for a route:</p> <ul style="list-style-type: none"> ◦ Community field is ignored. ◦ Remove all communities from the route. ◦ Remove all communities with the single community specified by set-community. ◦ Remove all communities that match set-community. ◦ Append the value of a single community specified

Field	Description
	by set-community to the list of communities.
SLA Community Action	(For Releases 22.1.1 and later.) Click to enable the SLA community action, which automatically sets the community using the gateway with the best SLA.
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 device that receives a route containing this community value must not advertise the route to any external or internal peer. ◦ no_export—A BGP device that receives a route containing this community value must not advertise the route to its external BGP peers. However, the BGP device 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 device 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. 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>
Preference for this Route	Enter the preference value for the route.

Field	Description
	<i>Range:</i> 1 through 255
Extended Community Action	<p>Select how to match the extended community list for a route:</p> <ul style="list-style-type: none"> ◦ Append the value of a single community specified by set-community to the list of communities. ◦ Ignore the community field. ◦ Remove all communities from the route. ◦ Remove all communities with the single community specified by set-community. ◦ Remove all communities that match set-community.
Extended Community	Enter a value for the BGP extended community.
Metric Action	<p>Select a metric action to take:</p> <ul style="list-style-type: none"> ◦ Add—Add constant to attribute. ◦ IGP—Track the IGP metric. ◦ Set value—Absolute value of the metric to set. ◦ Subtract—Subtract a constant value from the attribute.
Metric	<p>Enter the metric value to assign to the route.</p> <p><i>Range:</i> 1 through 4294967295</p>
Next Term	Select the name of the next term to evaluate. You can use this field to create a sequence of terms, and then you use the Next-Term Action field to configure the sequence as an AND or OR series.
Weight	<p>(For Releases 21.2.1 and later.) Enter a weight value to use when receiving routes from all neighbors in the peer group. The weight value is a locally significant parameter.</p> <p><i>Range:</i> 1 through 2147483647</p>

Field	Description
	<i>Default: 0</i>
Next-Term Action	<p>(For Releases 22.1.1 and later.) When you use the Next Term field, select whether to create an AND series and an OR series:</p> <ul style="list-style-type: none"> ◦ AND Series—Add this term to an AND series. ◦ OR Series—Add this term to an OR series.

13. Select the Standby Action tab to enter information for the action to take when the VOS device is an interchassis high availability (HA) standby device. Enter information for the following fields.

Add BGP Instance Add Peer/Group Policy Add Term

Term Name *

Match Action **Standby Action**

Standby AS Path
--Select--

Standby Local AS Prepend Count
Allowed Range is 1 - 255

Standby AS Path Prepend
Allowed Range is 1 - 4294967295

Standby Metric Action
--Select--

Standby Metric
Allowed Range is 1 - 4294967295

Standby Local Preference
Allowed Range is 0 - 2147483647

OK Cancel

Field	Description
Standby AS Path	<p>Select the AS path action to take when the VOS device is an interchassis HA standby device:</p> <ul style="list-style-type: none"> ◦ No AS path action. ◦ Prepend the local AS the number of times specified by the local AS prepend count value. ◦ Remove all AS numbers that match the AS path. ◦ Remove all AS numbers that match the AS path and prepend the local AS the number of times specified by the local AS prepend count value.



Field	Description
Standby Local AS Prepend Count	<p>Enter the number of times the local AS number is prepended to the AS path.</p> <p><i>Range:</i> 1 through 255</p>
Standby AS Path Prepend	<p>Enter the number of times to prepend the specified AS numbers to an AS path when the device is a interchassis HA standby device</p> <p><i>Range:</i> 1 through 4294967295</p>
Standby Metric Action	<p>Enter the metric action to take when the VOS device is an interchassis HA standby device:</p> <ul style="list-style-type: none"> ◦ Add—Add a constant to the attribute. ◦ IGP—Track the IGP metric. ◦ Set value—Enter the absolute value of the metric to set. ◦ Subtract—Subtract a constant value from the attribute.
Standby Metric	<p>Enter the metric value.</p> <p><i>Range:</i> 1 through 4294967295</p>
Standby Local Preference	<p>Enter the local preference for the route while the device is an interchassis HA standby device.</p> <p><i>Range:</i> 1 through 2147483647</p>

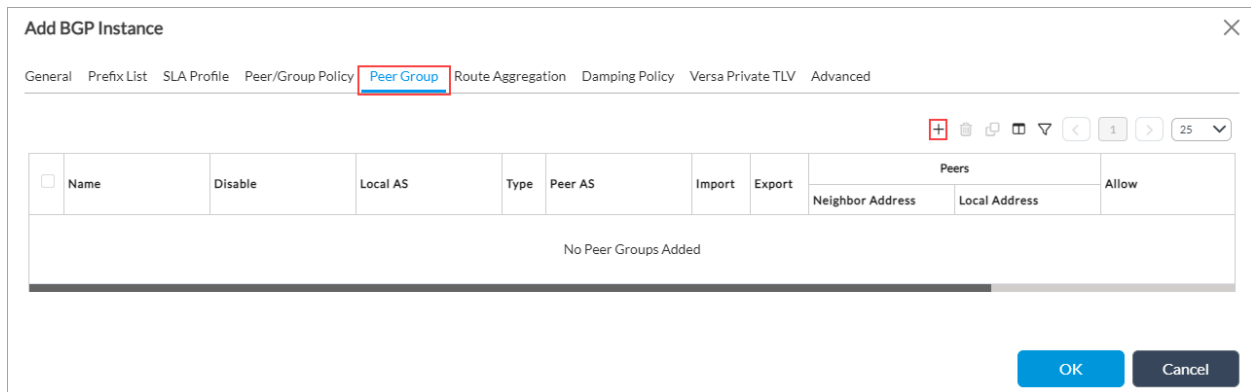
14. Click OK.

Configure a BGP Peer Group

To configure a group of BGP peers, or neighbors:









1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Peer Group tab.




Add BGP Instance

General Prefix List SLA Profile Peer/Group Policy **Peer Group** Route Aggregation Damping Policy Versa Private TLV Advanced







1

25


<input type="checkbox"/>	Name	Disable	Local AS	Type	Peer AS	Import	Export	Peers		Allow
								Neighbor Address	Local Address	
No Peer Groups Added										

OK
Cancel

9. Click the  Add icon. In the Add BGP Instance Add Peer Group popup window, enter information for the following fields.

Add BGP Instance Add Peer Group

Name

Description

Type

Peer AS

Local Address

Disable

Hold Time (seconds)

TTL

Password

AS Origination Interval

Local Network Name

Local AS

Local AS Mode

Weight

☐ Suppress Peer AS

☐ Relax First AS Check

☐ Soft Reconfiguration

☐ Next Hop UnChanged

General Neighbors Allow Advanced

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration	Next Hop UnChanged	
		Maximum	Threshold					
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfiguration	<input type="checkbox"/> Next Hop UnChanged	+

No Family Added

OK

Cancel

Field	Description
Name (Required)	Enter a name for the peer group.
Description	Enter a text description for the peer group.
Type	Select the type of peer group: <ul style="list-style-type: none"> EBGP IBGP
Peer AS	Enter the peer's AS number.
Local Address	Enter the IP address of the local end of a BGP session.
Disable	Click to disable all static neighbors in the BGP group.
Hold Time	Enter the hold time to use when negotiating with a peer. <i>Range:</i> 3 through 65535

Field	Description
TTL	<p>Enter the time-to-live value, which is the number of hops a packet can travel in a network before the packet expires.</p> <p><i>Range:</i> 1 through 255 <i>Default for EBGp:</i> 64 (Note that you do not need to enable EBGp multihop.) <i>Default for IBGP:</i> 64</p>
Password	Enter the MD5 password that the peer group uses.
AS Origination Interval	<p>Enter the minimum time that must elapse between successive advertisements of Update messages that report changes within the advertising BGP device's own AS.</p> <p><i>Range:</i> 1 through 65535</p>
Local Network Name	Select the network to which the peer group belongs. The name can be the network name or the local address of the peer group.
Local AS	Enter the local AS number.
Local AS Mode	<p>Select the BGP AS mode to use on the local device:</p> <ul style="list-style-type: none"> ◦ 1—Peering session is established with the local AS configured in the BGP instance or with a BGP group or neighbor. When BGP is importing routes, an AS number is not inserted in the AS path. When BGP is exporting routes, the selected local AS number is prepended to the AS path. ◦ 2—Peering session is established with local AS configured as a BGP group or neighbor. When BGP is importing routes, the local AS number of the group or neighbor is inserted in AS path. When BGP is exporting routes, the local AS number configured on the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to the AS path. This is the default. ◦ 3—Peering session is established with the local AS configured for the BGP group or neighbor.

Field	Description
	<p>When BGP is importing routes, no AS number is inserted in the AS path. When BGP is exporting routes, the local AS configured for the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to AS path.</p> <ul style="list-style-type: none"> 4—Peering session is established with the local AS number configured for the BGP group or neighbor. When BGP is importing routes, no AS number is inserted in the AS path. When BGP is exporting routes, the local AS number configured for the BGP group or neighbor is prepended to the AS path. 5—(For Releases 22.1.1 and later) Peering session is established with the local AS number configured for the BGP group or neighbor. When BGP is importing routes, the local AS in the BGP group or neighbor is inserted in the AS path. When BGP is exporting routes, the local AS number configured in the BGP group or neighbor is prepended to the AS path. <p><i>Default: 2</i></p>
Weight	<p>(For Releases 21.2.1 and later.) Enter a weight value to use when receiving routes from all neighbors in the peer group. The weight value is a locally significant parameter.</p> <p><i>Range: 1 through 2147483647</i></p> <p><i>Default: 0</i></p>
Suppress Peer AS	<p>(For Releases 21.2.1 and later.) Click to suppress and not advertise routes received from an EBGP neighbor to another neighbor that is in the same AS as originating neighbor.</p>
Relax First AS Check	<p>(For Releases 21.2.1 and later.) Click to relax the check that the first (left-most) AS number in an AS path receives from an EBGP neighbor is same as neighbor's AS.</p>


Field	Description
Soft Reconfiguration	(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects the routes.
Next Hop Unchanged	Click to preserve the BGP next hop when forwarding routes to the EBGp peer.

10. Select the General tab to configure global information for the BGP peer group. Enter information for the following fields.

Field	Description
Family (Required)	<p>Select the protocol family for the peer group:</p> <ul style="list-style-type: none"> ◦ IPv4 Unicast—Applicable to BGP ◦ IPv4 Multicast—Applicable to BGP ◦ IPv4 Versa Private—Applicable to SD-WAN ◦ IPv4 Layer 3 VPN Unicast—Applicable to Layer 3 VPN ◦ IPv4 VPN Multicast—Applicable to Layer 3 VPN ◦ IPv6 Unicast—Applicable to BGP ◦ IPv6 Multicast—Applicable to BGP ◦ IPv6 VPN Unicast—Applicable for Layer 3 VPN ◦ IPv6 VPN Multicast—Applicable for Layer 3 VPN ◦ L2VPN EVPN—Applicable for Layer 2 VPN
Loop Count	Enter the number of times the local AS is allowed in the received AS path. For example, if you set the loop value to 5, the local AS in received AS paths can appear five times.
Prefix Limit (Group of Fields)	Limit the number of prefixes received from a session with a BGP neighbor.
<ul style="list-style-type: none"> ◦ Maximum 	<p>Enter the maximum number of prefixes that can be received from the BGP neighbor.</p> <p><i>Range:</i> 1 through 2147483647</p>

Field	Description
<ul style="list-style-type: none"> Threshold 	<p>Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reached, the VOS device send an SNMP trap warning message.</p> <p><i>Range:</i> 1 through 100 percent</p>
Restart Interval	<p>When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached.</p> <p><i>Range:</i> 30 through 86400 seconds</p>
Action	<p>Select the action to take when the maximum prefix limit is exceeded:</p> <ul style="list-style-type: none"> Drop—Drop the BGP session to the neighbor. Warn—Send a warning message.
Soft Reconfiguration	<p>(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects the routes.</p>
Next Hop Unchanged	<p>Click to preserve the BGP next hop when forwarding routes to the EBGp peer.</p>

11. Select the Neighbors tab to configure BGP peers.

12. Click the  Add icon. In the Add BGP Instance Add Peer Group Add Neighbor popup window, enter information for the following fields.

Add BGP Instance Add Peer Group Add Neighbor

Neighbor IP
IPv4 Or IPv6 Address

Peer AS
1 to 4294967295 Or <0..65535>,<f

Local Address
IPv4 Or IPv6 Address

Hold Time (seconds)
Allowed Range is 3 - 65535

TTL
Allowed Range is 1 - 255

Password

Local Network Name
--Select--

Local AS
0 to 4294967295 Or <0..65535>,<f

Local AS Mode
--Select--

AS Origination Interval
Allowed Range is 1 - 65535

Weight
Allowed Range is 1 - 2147483647

☐ Suppress Peer AS

Description

Disable
--Select--

☐ Relax First AS Check

☐ Soft Reconfiguration

☐ Next Hop UnChanged

General Advanced

Family	Loop Count	Prefix Limit		Restart Interval	Action	Soft Reconfiguration
		Maximum	Threshold			
--Select--	Allowed Range is 1 - 2	Allowed Range is 1 - 2	Allowed Range is 1 - 1	Allowed Range is 30 -	--Select--	<input type="checkbox"/> Soft Reconfigurati

No Family Added

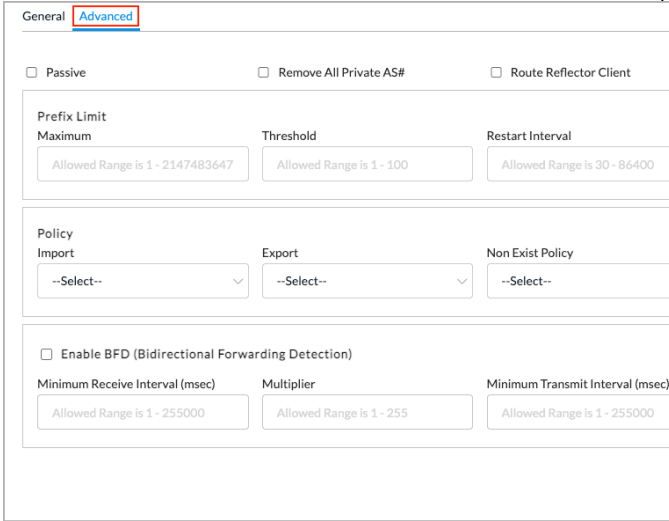
OK Cancel

Field	Description
Neighbor IP (Required)	Enter the peer's IP address.
Peer AS	Enter the peer's AS number.
Local Address	Enter the IP address of the the local end of the BGP session.
Hold Time	Enter the hold time to use when negotiating with the peer. Range: 3 through 65535 seconds
TTL	Enter the number of hops a packet can travel in a network before the packet expires.

Field	Description
	<p><i>Range:</i> 1 through 255</p> <p><i>Default for EBGp:</i> 64 (Note that you do not need to enable EBGp multihop.)</p> <p><i>Default for IBGP:</i> 64</p>
Password	Enter the MD5 password for the neighbor.
Local Network Name	Select the network to which the neighbor peer group belong. The name can be the network name or the local address of the peer group.
Local AS	Enter the local AS number.
Local AS Mode	<p>Select the BGP AS mode to use on the local device:</p> <ul style="list-style-type: none"> ◦ 1—Peering session is established with the local AS configured in BGP instance or with a BGP group or neighbor. When BGP is importing routes, an AS number is not inserted in the AS path. When BGP is exporting routes, the selected local AS number is prepended to the AS path. ◦ 2—Peering session is established with local AS configured as a BGP group or neighbor. When BGP is importing routes, the local AS number of the group or neighbor is inserted in AS path. When BGP is exporting routes, the local AS number configured on the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to the AS path. This is the default. ◦ 3—Peering session is established with the local AS configured for the BGP group or neighbor. When BGP is importing routes, no AS number is inserted in the AS path. When BGP is exporting routes, the local AS configured for the BGP group or neighbor and the local AS number configured for the BGP instance are prepended to AS path. ◦ 4—Peering session is established with the local AS number configured for the BGP group or neighbor. When BGP is importing routes, no AS number is inserted in the AS path. When BGP is exporting routes, the local AS number configured for the BGP group or neighbor is prepended to the AS path.

Field	Description
	<ul style="list-style-type: none"> 5—(For Releases 22.1.1 and later.) Peering session is established with the local AS number configured for the BGP group or neighbor. When BGP is importing routes, the local AS in the BGP group or neighbor is inserted in the AS path. When BGP is exporting routes, the local AS number configured in the BGP group or neighbor is prepended to the AS path. <p><i>Default: 2</i></p>
AS Origination Interval	<p>Enter the minimum amount of time that must elapse between successive advertisements of Update messages that report changes within the advertising BGP speaker's own AS.</p> <p><i>Range: 1 through 65535</i></p>
Weight	<p>(For Releases 21.2.1 and later.) Enter a weight value to use when receiving routes from all neighbors in the peer group. The weight value is a locally significant parameter.</p> <p><i>Range: 1 through 2147483647</i></p> <p><i>Default: 0</i></p>
Description	Enter a text description for the BGP peer.
Suppress Peer AS	(For Releases 21.2.1 and later.) Click to suppress and not advertise routes received from an EBGP neighbor to another neighbor that is in the same AS as originating neighbor.
Relax First AS Check	(For Releases 21.2.1 and later.) Click to relax the check that the first (left-most) AS number in an AS path receives from an EBGP neighbor is same as neighbor's AS.
Soft Reconfiguration	(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects

Field	Description
	the routes.
Next Hop Unchanged	Click to preserve the BGP next hop when forwarding routes to the EBGp peer.
Disable	Disable all static neighbors in the BGP group.
General (Tab)	
<ul style="list-style-type: none"> Family 	<p>Select the protocol family of the neighbor peer group:</p> <ul style="list-style-type: none"> IPv4 Layer 3 VPN Unicast—Use for Layer 3 VPN. IPv4 Multicast—Use for BGP. IPv4 Unicast—Use for BGP. IPv4 Versa Private—Use for SD-WAN. IPv4 VPN Multicast— Use for Layer 3 VPN. IPv6 Multicast—Use for BGP. IPv6 VPN Multicast—Use for Layer 3 VPN. IPv6 Unicast—Use for BGP. IPv6 VPN Unicast— Use for Layer 3 VPN. L2VPN EVPN—Use for Layer 2 VPN.
<ul style="list-style-type: none"> Loop Count 	Enter the number of times the local AS is allowed in the received AS path.
Prefix Limit (Group of Fields)	Limit the number of prefixes received from a session with a BGP neighbor.
<ul style="list-style-type: none"> Maximum 	<p>Enter the maximum number of prefixes that can be received from the BGP neighbor.</p> <p><i>Range:</i> 1 through 2147483647</p>
<ul style="list-style-type: none"> Threshold 	<p>Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reached, the VOS device send an SNMP trap warning message.</p> <p><i>Range:</i> 1 through 100 percent</p>

Field	Description
Restart Interval	When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached. <i>Range: 30 through 86400 seconds</i>
Action	Select the action to take when the maximum prefix limit is exceeded: <ul style="list-style-type: none"> Drop—Drop the BGP session to the neighbor. Warn—Send a warning message.
Soft Reconfiguration	(For Releases 21.2.1 and later.) Click to keep received routes even if the routing peer policy rejects the routes.
Next Hop Unchanged	Click to preserve the BGP next hop when forwarding routes to the EBGp peer.
Advanced (Tab)	<p>In the Advanced tab, enter information for the following fields.</p> 
<ul style="list-style-type: none"> Passive 	Select to have BGP accept traffic only and not transmit any routes.

◦ Remove All Private AS	Select to remove all private AS numbers before advertising routes.
◦ Route Reflector Client	For IBGP, select to have the router function as a route reflector and to broadcast the routes of all other routers in the network
◦ AS Override	Select to replace neighbor AS numbers with the local AS numbers from the AS path.
Prefix Limit (Group of Fields)	Limit the number of prefixes received from a BGP neighbor.
◦ Maximum	Enter the maximum number of prefixes that can be received from the BGP neighbor. <i>Range: 1 through 2147483647</i>
◦ Threshold	Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reach, the VOS device send an SNMP trap warning message. <i>Range: 1 through 100 percent</i>
◦ Restart Interval	When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached. <i>Range: 30 through 86400 seconds</i>
◦ Action	Select the action to take when the maximum prefix limit is exceeded: <ul style="list-style-type: none"> ◦ Drop—Drop the BGP session to the neighbor. ◦ Warn—Send a warning message.
Policy (Group of Fields)	
◦ Import	Select the peer group policy to apply to routing updates coming from remote BGP peers.

◦ Export	Select the peer group policy to apply to routing updates advertised to remote BGP peers.
◦ Non-Exit Policy	Select the policy that defines the route being withdrawn. Routes matching the advertised policy are advertised to peers only if no routes in the local route table match the non-exist policy.
◦ Advertise Policy	Select the policy that defines the route to be advertised to the BGP peer after the route in the non-exist policy is withdrawn.
Enable BFD	Click to enable BFD on the interface, to allow BFD to report when a static route becomes unavailable.
◦ Minimum Receive Interval	Enter the minimum time interval to receive routes, in milliseconds.
◦ Multiplier	Enter the multiplier value to use to calculate the final minimum receive interval and minimum transmit interval.
◦ Minimum Transmit Interval	Enter the time after which routes can be retransmitted, in milliseconds.

13. Click OK to add the BGP neighbor.

14. In the Add Peer Group popup window, select the Allow tab to allow BGP peers to form a session with the local device. When you enable allow, you do not have to configure a neighbor for the allowed addresses or address range in the Neighbors tab. Enter information for the following fields.

Field	Description
Allow All v4	Click to allow incoming BGP peering sessions from any IPv4 peer neighbor request.
Allow All v6	Click to allow incoming BGP peer sessions from any IPv6 peer neighbor request.
IP Address/Mask	Click the Add icon, and then add the IP address or IP address network range of peers that are allowed to

Field	Description
	form peering sessions with the local device.

15. In the Add Peer Group popup window, select the Advanced tab to configure the peer group routes to accept. Enter information for the following fields.

Field	Description
Passive	Click to have BGP accept traffic only and not transmit any routes.
Remove All Private AS Numbers	Click to remove all private AS numbers before advertising routes.
Route Reflector Client	For IBGP, click to have the router function as a route reflector and to broadcast the routes of all other routers in the network
Next-Hop Self	Click to use the IP address of the prefix list.
AS Override	Click to replace neighbor AS numbers with the local AS numbers from the AS path.
Share ARO	Click to share all the routes of the Adj-RIB-Out (ARO) RIB among all neighbors in an IBGP group. Enabling this option saves internal memory. This option works only when all members of the BGP peer group use the same outbound BGP policy. For this option to take

Field	Description
	effect after you configure it, you must bring down the established BGP peer sessions that are part of the peer group and then bring them back up again. One way to do this is to disable the peer group and then re-enable it.
Prefix Limit (Group of Fields)	Limit the number of prefixes received from a session with a BGP neighbor.
<ul style="list-style-type: none"> Maximum 	<p>Enter the maximum number of prefixes that can be received from the BGP neighbor.</p> <p><i>Range:</i> 1 through 2147483647</p>
<ul style="list-style-type: none"> Threshold 	<p>Enter a threshold of prefixes as a percentage of the maximum number of prefixes. When the threshold is reached, the VOS device send an SNMP trap warning message.</p> <p><i>Range:</i> 1 through 100 percent</p>
<ul style="list-style-type: none"> Restart Interval 	<p>When the Action field is set to Drop, enter how long to wait, in seconds, to re-establish a session that is dropped when the maximum prefix limit is reached.</p> <p><i>Range:</i> 30 through 86400 seconds</p>
<ul style="list-style-type: none"> Action 	<p>Select the action to take when the maximum prefix limit is exceeded:</p> <ul style="list-style-type: none"> Drop—Drop the BGP session to the neighbor. Warn—Send a warning message.
Policy (Group of Fields)	Advertise routes matching the advertise policy to peers only if no routes in the local route table match the non-exist-policy.
<ul style="list-style-type: none"> Import 	Select the peer group policy to apply to outgoing routing updates.

Field	Description
◦ Export	Select the peer group policy to apply to incoming routing updates.
◦ Non-Exist Policy	Select the name of a policy to use when you are configuring conditional route advertisements. In the Non-Exist Policy field, select the policy that defines the route being withdrawn. For more information, see Configure BGP Conditional Route Advertisements , below.
◦ Advertise Policy	Select the name of a policy to use when you are configuring conditional route advertisements. In the Advertise Policy field, select the policy that defines the route to be advertised to the BGP peer after the route in the non-exist policy is withdrawn. For more information, see Configure BGP Conditional Route Advertisements , below
Enable BFD	Click to enable BFD on the interface, to allow BFD to report when a static route becomes unavailable.
◦ Minimum Receive Interval	Enter the minimum time interval to receive routes, in milliseconds.
◦ Multiplier	Enter the multiplier value used to calculate the final minimum receive interval and minimum transmit interval.
◦ Minimum Transmit Interval	Enter the time after which routes can be retransmitted, in milliseconds.

8. Click OK.

Configure Route Aggregation

In BGP, you can aggregate routes to minimize the number of entries in a routing table and to minimize the number of routing tables required in an IP network.



To configure route aggregation:

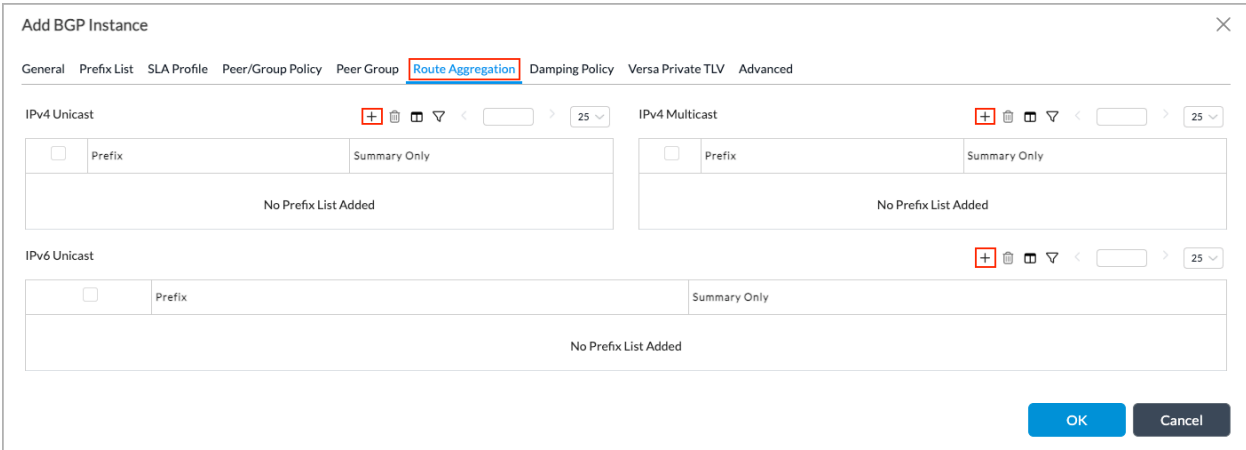
1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, in Director view:
 - a. Select the Administration tab in the top menu bar.


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

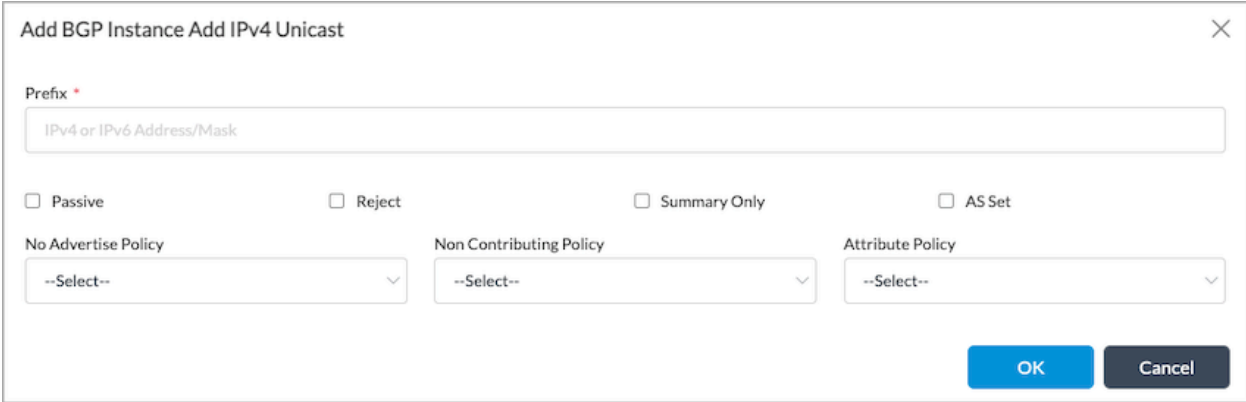
Updated: Wed, 23 Oct 2024 08:25:28 GMT

Copyright © 2024, Versa Networks, Inc.

- 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 BGP tab. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Route Aggregation tab.



9. Click the  Add icon in the IPv4 Unicast, IPv4 Multicast, or IPv6 Multicast section, and in the popup window, enter information for the following fields.





Field	Description
Prefix	Enter the IPv4 or IPv6 address to advertise as the aggregate route.

Field	Description
Passive	Click to create an aggregate route even when there are no contributing routes on the device.
Reject	Click to assign the reject next hop to the aggregate route. When you select this option, if a more specific route to the destination does not exist on the device, the packet is dropped and an ICMP unreachable message is sent to the sender.
Summary Only	Click to automatically suppress contributing routes and advertise only the aggregate (summary) route to peers.
AS Set	Click to add the AS numbers of contributing routes to the AS path of the aggregate route as an AS set.
No Advertise Policy	Select the routing peer policy that defines the contributing routes that should not be advertised.
Non-Contributing Policy	Select the routing peer policy that defines the set of routes that do not act as contributing routes.
Attribute Policy	Select the name of the policy that allows the setting of aggregated route attributes.

10. Click OK.

Configure Damping Policy

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Damping Policy tab.

Add BGP Instance

General

Prefix List

SLA Profile

Peer/Group Policy

Peer Group

Route Aggregation

Damping Policy

Versa Private TLV

Advanced

Damping

+

<

>

25

<input type="checkbox"/>	Name	Half Life Ng (min)	Half Life Ok (min)	Max Suppress Time (min)	Max Time Ng (min)	Max Time Ok (min)	Reuse	Suppress
No Damping Record Added								

OK

Cancel

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

Add BGP Instance Add Damping

Damping Name *

Maximum Suppress Time (min)

60

Half Life Ok (min)

15

Maximum Time Ok (min)

30

Suppress

125

Reuse

50

Half Life Ng (min)

15

Maximum Time Ng (min)

30

OK

Cancel

Field	Description
Damping Name	Enter a name for the damping policy.
Suppress	Enter the cutoff threshold limit. Routes exceeding this level are suppressed.

Field	Description
Maximum Suppress Time	Enter the maximum time a route can be suppressed (held), in minutes
Reuse	Enter the reuse threshold of a suppressed route.
Half Life OK	Enter the decay half life time, in minutes, to define the stability of the route v
Half Life Ng	Enter the decay half life time, in minutes, to define the stability of the route v
Maximum Time OK	Enter the maximum time, in minutes, any memory of a previous instability is
Maximum Time Ng	Enter the maximum time, in minutes, any memory of a previous instability is

- Click OK. The Add BGP Instance popup window displays the configured damping policies.


Enable BGP Versa Private TLVs


For Releases 21.2.1 and later.

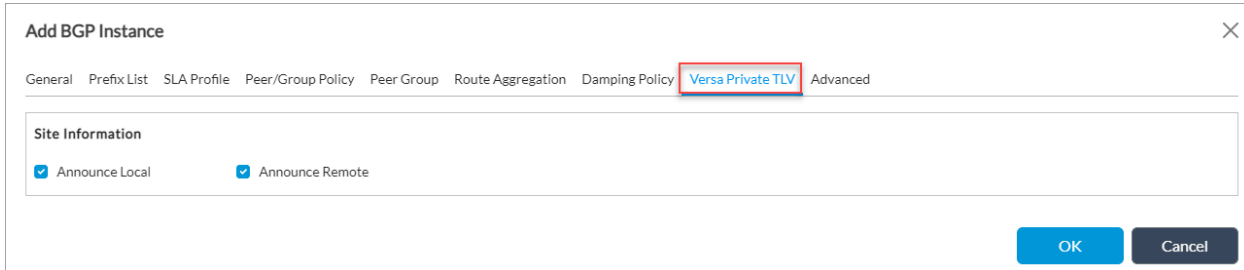
You can enable the BGP Versa private type-length-value (TLV) site information on the provider's virtual router (VR) so that the gateway and group FQDNs are distributed to all the other gateways. In this way, each gateway can learn which gateways are part of a group.

Note that in a multitenant deployment, that is, in a deployment with a provider that has additional tenants, you enable the Versa private TLV information in the multiprotocol BGP (MP-BGP) instance associated with the provider organization (that is, in the provider control VR), not in the tenant control virtual routers.

To enable BGP Versa private TLV site information:

- If you have already started configuring BGP, skip to Step 8.
- Otherwise, 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.
- Select the Configuration tab in the top menu bar.
- Select Networking > Virtual Routers in the left menu bar.
- Click the  Add icon. The Configure Virtual Router popup window displays.
- Select the BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.



7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Versa Private TLV tab, and then enter information for the following fields.



Fields	Description
Site Information (Group of Fields)	
<ul style="list-style-type: none"> ◦ Announce Local 	Click to enable gateways or hub-controller nodes (HCN) to support selection of the best gateway.
<ul style="list-style-type: none"> ◦ Announce Remote 	Click only if the gateways and hub-controller nodes are not in a full-mesh topology.

9. Click OK.

Configure Advanced BGP Settings

1. If you have already started configuring BGP, skip to Step 8.
2. Otherwise, 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 BGP tab in the left menu bar. The main pane displays a list of the BGP instances that are already configured.
7. Click the  Add icon. The Add BGP Instance popup window displays.
8. Select the Advanced tab and enter information for the following fields.

Add BGP Instance

General
Prefix List
SLA Profile
Peer/Group Policy
Peer Group
Route Aggregation
Damping Policy
Versa Private TLV
Advanced

Cluster ID

Path Selection

☐ Always Compare MED
☐ Cisco-Nondeterministic
☐ AS Path Ignore
☐ AS Path Multipath Relax

☐ Enable BFD (Bidirectional Forwarding Detection)

Minimum Receive Interval (msec)
Multiplier
Minimum Transmit Interval (msec)

Allowed Range is 1 - 255000
Allowed Range is 1 - 255
Allowed Range is 1 - 255000

Route Flap Options

Free Max Time (seconds)
Reuse Max Time (min)
Reuse Size
Reuse Array Size

180
60
256
1024

☒ Enable Helper Graceful Restart

☐ Enable Graceful Restart

Maximum Restart Time (seconds)
Recovery Time (seconds)
Dynamic Peer Restart Time
Stalepath Time (seconds)

Allowed Range is 1 - 3600
Allowed Range is 1 - 3600
Allowed Range is 0 - 3600
Allowed Range is 1 - 3600

Defer Time (seconds)
Multiplier

Allowed Range is 1 - 3600
Allowed Range is 1 - 255

Family

Family
Forwarding State Bit

--Select--
Forwarding State Bit

+

No Records to Display

OK
Cancel

Field	Description
Cluster ID	Enter the cluster ID of the reflector clients.
Path Selection (Group of Fields)	
<ul style="list-style-type: none"> Always Compare MED 	Click to compare multiexit discriminators when sending routes to another router. A route with a lower MED is given priority.
<ul style="list-style-type: none"> Cisco Nondeterministic 	<p>Click to use Cisco nondeterministic path selection.</p> <p>The active path is always first. All non-active, but eligible paths follow the active path and are maintained in the order in which they are received, with the most recent path first. Ineligible paths remain at the end of the list.</p> <p>When a new path is added to the routing table, path comparisons are made without removing from consideration those paths that should not be selected because those paths lose the MED tie-breaking rule.</p>
<ul style="list-style-type: none"> AS Path Ignore 	(For Releases 21.2.1 and later.) Click to exclude the AS path from BGP best path computation.
<ul style="list-style-type: none"> AS Path Multipath Relax 	(For Releases 21.2.1 and later.) Click to allow different AS paths to be considered for multipath if the AS path length is equal.
Enable BFD	Click to mark the link as down whenever the BFD is down.
<ul style="list-style-type: none"> Minimum Receive Interval 	Enter the time interval, in milliseconds, to mark the link as down if the routing updates are not received.
<ul style="list-style-type: none"> Multiplier 	Enter value to use to compute the final minimum receive interval.
<ul style="list-style-type: none"> Minimum Transmit Interval 	Enter how often BGP instances communicate with each other, in milliseconds.
Route Flap Option (Group of Fields)	

◦ Free Maximum Time	Enter the maximum time to remember an assigned penalty to the router, in seconds. A penalty is assigned to a router when its routes go up and down.
◦ Reuse Maximum Time	Enter the time corresponding to the last reuse list, in minutes.
◦ Reuse Size	Enter the number of reuse lists.
◦ Reuse Array Size	Enter the size of the reuse index arrays.
Enable Graceful Restart (Group of Fields)	Click to enable BGP graceful restart.
◦ Maximum Restart Time	Enter the restart time, in seconds, that is advertised to a neighbor on which graceful restart is enabled. <i>Range:</i> 1 through 3600 seconds (1 hour) <i>Default:</i> 3600 seconds (for Controller BGP sessions)
◦ Stale Path Time	Enter the maximum time, in seconds, that BGP waits before removing stale routes from a neighbor after a graceful restart of the neighbor's session. Enter the maximum amount of time, in seconds, that a helper device waits for an End-of-RIB marker from a peer. When this time period expires, all stale path are deleted. <i>Range:</i> 1 through 3600 seconds (1 hour) <i>Default:</i> 3600 seconds (for Controller BGP sessions)
◦ Recovery Time	Enter the estimated recovery time, in seconds, after a restart. <i>Range:</i> 1 through 3600 seconds (1 hour) <i>Default:</i> 120 seconds
◦ Defer Time	Enter how long, in seconds, a restarting router defers its BGP best-path calculation after a restart occurs and while BGP peering sessions are establishing themselves. This time should be long enough so that all peers have enough time to send all their routes to the restarting BGP router. <i>Range:</i> 1 through 3600 seconds (1 hour) <i>Default:</i> 30 seconds (for Controller BGP sessions)

◦ Dynamic Peer Restart Time	Enter the minimum time, in seconds, for a peer to dynamically reconnect after the BGP process restarts. <i>Range:</i> 1 through 3600 seconds (1 hour) <i>Default:</i> 120 seconds
◦ Multiplier	Enter a multiplier value that, when multiplied by the stale path time, provides a value that is used to hold the routes from a peer that are in RIB/RIB in the stale state after the BGP session with that peer goes down. Note that this multiplier value is not related to the BFD multiplier. <i>Range:</i> 1 through 255 <i>Default:</i> 8 (for Controller BGP sessions)
Family (Group of Fields)	Protocol family for NLRIs in updates.
◦ Family	Select the protocol: <ul style="list-style-type: none"> ◦ IPv4 Unicast—Use for BGP ◦ IPv4 Multicast—Use for BGP ◦ IPv4 Versa Private—Use for SD-WAN ◦ IPv4 Layer 3 VPN Unicast—Use for Layer 3 VPN ◦ IPv4 VPN Multicast—Use for Layer 3 VPN ◦ IPv6 Unicast—Use for BGP ◦ IPv6 Multicast—Use for BGP ◦ IPv6 VPN Unicast—Use for Layer 3 VPN ◦ IPv6 VPN Multicast—Use for Layer 3 VPN ◦ L2VPN EVPN—Use for Layer 2 VPN
◦ Forwarding State Bit	Select the forwarding state bit to preserve the forwarding state associated with the AFI/SAFI.

9. Click OK.

Configure BGP Conditional Route Advertisements

To have BGP to advertise a route based on a specific situation, you configure a conditional route advertisement. To configure the conditional route, you define the prefixes and then you create policies and apply the policies to the BGP peer group.


To illustrate how to configure BGP conditional route advertisements, let's consider a situation where you want BGP to

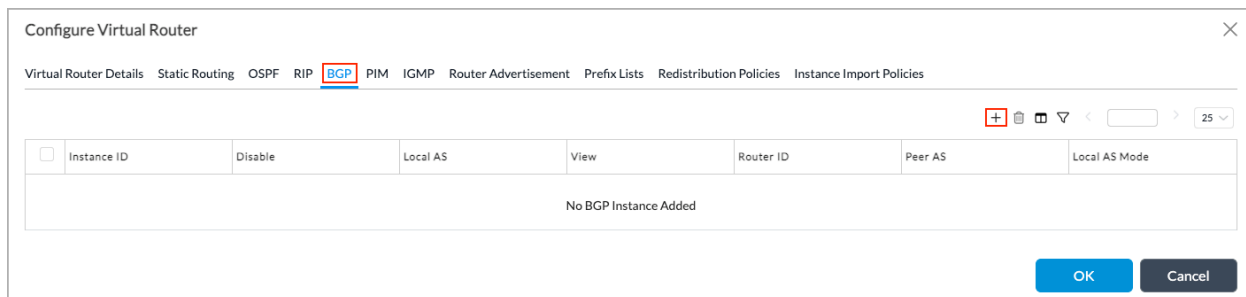
advertise a route only when another route is withdrawn and becomes unavailable. For this example, you configure the following:


- Two prefix lists, one for the unavailable prefix and one for the backup prefix to advertise.
- Two policies, one with a term that matches the unavailable prefix (which here is called *Non-exist*) and one with a term that matches the backup prefix to advertise (which here is called *Advertise*).
- A BGP peer group that refers to the two policies

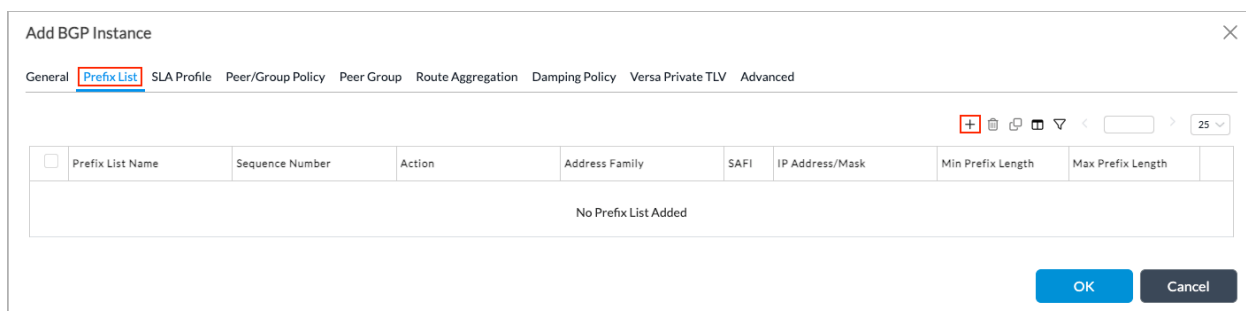
In the example, the two routes are for the prefixes 192.168.0.0/24, which is the primary prefix that is used in the *non-exist* policy, and 192.168.1.0/24, which is the backup prefix used in the *advertise* policy.

To configure a BGP conditional route advertisement:

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 BGP tab The main pane displays a list of the BGP instances that are already configured.




6. Click the  Add icon. The Add BGP Instance popup window.
7. Select the Prefix List tab. Here, you create two prefix lists, *Non-Existent*, for the prefix 192.168.0.0/24, and *Advertise*, for 192.168.1.0/24.

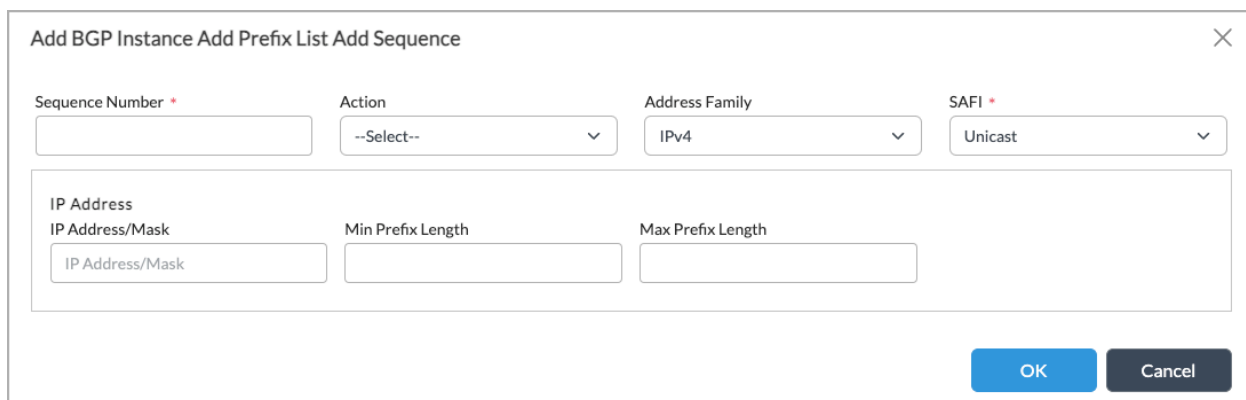


8. To create the Non-Existent prefix list, click the  Add icon and enter the prefix list name as Non-Existent.





The dialog box is titled "Add BGP Instance Add Prefix List" and has a close button (X) in the top right corner. It contains a text field for "Prefix List Name" with a red asterisk indicating it is required. Below this is a "Sequence" section with a toolbar containing icons for adding (+), deleting (trash), copying, pasting, and a dropdown menu. To the right of the toolbar is a text input field and a dropdown menu showing "25". Below the toolbar is a table with two columns: "Sequence Number" and "Action". The table is currently empty, and the text "No Sequence Added" is centered below it. At the bottom right are "OK" and "Cancel" buttons.

9. To add a prefix list sequence, click the  Add icon, and then select Permit in the Action field and enter the prefix 192.168.0.0/24.



The dialog box is titled "Add BGP Instance Add Prefix List Add Sequence" and has a close button (X) in the top right corner. It contains several fields: "Sequence Number" (required, indicated by a red asterisk), "Action" (a dropdown menu with "--Select--" selected), "Address Family" (a dropdown menu with "IPv4" selected), and "SAFI" (a dropdown menu with "Unicast" selected). Below these fields is a section for "IP Address" with three sub-fields: "IP Address/Mask", "Min Prefix Length", and "Max Prefix Length". At the bottom right are "OK" and "Cancel" buttons.

10. Click OK.
11. To create the Advertise prefix list, click the  Add icon on the Prefix List tab, and then enter the prefix list name as Advertise. To add a prefix list sequence, click the  Add icon, and then select Permit in the Action field and enter the prefix 192.168.1.0/24.
12. Click OK.
13. Click OK to return to the BGP Instance screen.
14. Select the Peer/Group Policy tab. Here, you create two peer group policies, one for the Non-Existent prefix list and the second for the Advertise prefix list. You must create both policies.

Add BGP Instance

General Prefix List SLA Profile **Peer/Group Policy** Peer Group Route Aggregation Damping Policy Versa Private TLV Advanced

☐ Peer/Group Policy Name Term Name Action

No Routing Peer Policy Added

OK Cancel

15. To create the Non-Existent peer group policy, click the **+** Add icon and enter a name for the policy.

Add BGP Instance Add Peer/Group Policy

Name *

Terms

☐ Term Name

No Term Added

OK Cancel

16. To create a term, click the **+** Add icon. Enter a name for the term. Then, select the Match tab, and in the NLRI field, select the prefix list Non-Existent. In the Action tab, use the default action, which is Accept.

Add BGP Instance Add Peer/Group Policy Add Term

Term Name *

Match

Action

Standby Action

Family
--Select--

AS Path

Metric

NLRI
--Select--

Source Address
--Select--

Nexthop
--Select--

Well Known Community
--Select--

Community

Extended Community

Origin
--Select--

SLA Profile
Name
--Select--

Nexthop Name
--Select--

Local Circuit Name
--Select--

Nexthop List

☐ Nexthop List
+

Nexthop List Not Configured

Local Circuit List

☐ Local Circuit List
+


Local Circuit List Not Configured

OK

Cancel

17. Click OK.

18. To create the Advertise peer group policy, click the  Add icon and enter a name for the policy.

19. To create a term. Click the  Add icon. Then, select the Match tab, and in the NLRI field, select the prefix list Advertise. In the Action tab, use the default action, which is Accept.

Add BGP Instance Add Peer/Group Policy Add Term

Term Name *

Match
Action
Standby Action

Accept/Reject
Accept

Origin
--Select--

AS Path
--Select--

Community Action
--Select--

Community

Extended Community

Next Term
--Select--

Damping

Nexthop

Local AS Prepend Count
Allowed Range is 1 - 255

Route Preference

Metric Action
--Select--

Weight
Allowed Range is 1 - 2147483647

☐ Enable ECMP for BGP Routes in RIB

Local Preference
Allowed Range is 0 - 2147483647

AS Path Prepend
Allowed Range is 1 - 4294967295

Well Known Community
--Select--

Extended Community Action
--Select--

Metric
Allowed Range is 1 - 4294967295

Next Term Action
--Select--

OK
Cancel

20. Click OK.
21. Click OK to return to the BGP Instance popup window.
22. To associate the policies with the BGP peer group, select the Peer Group tab. In this example, we want to advertise the prefix 192.168.1.0/24 to the peer only if the prefix 192.168.0.0/24 is withdrawn from the route table (RIB). Select the peer group, and then select the Advanced tab. In the Policy group of fields, in the Non-Exist Policy. field select the Non-Existent policy, and in the Advertise Policy field select the Advertise policy. With this configuration, the BGP peer does not receive the route shown in the Advertise field until the route show in the Non-Exist field is withdrawn.

General
Neighbors
Allow
Advanced

☐ Passive
☐ Remove All Private AS#
☐ Route Reflector Client
☐ Nexthop Self

☐ As Override
☐ Share ARO

Prefix Limit
Maximum
Allowed Range is 1 - 2147483647
Threshold
Allowed Range is 1 - 100
Restart Interval
Allowed Range is 30 - 86400
Action
Drop

Policy
Import
--Select--
Export
--Select--
Non Exist Policy
--Select--
Advertise Policy
--Select--

☐ 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

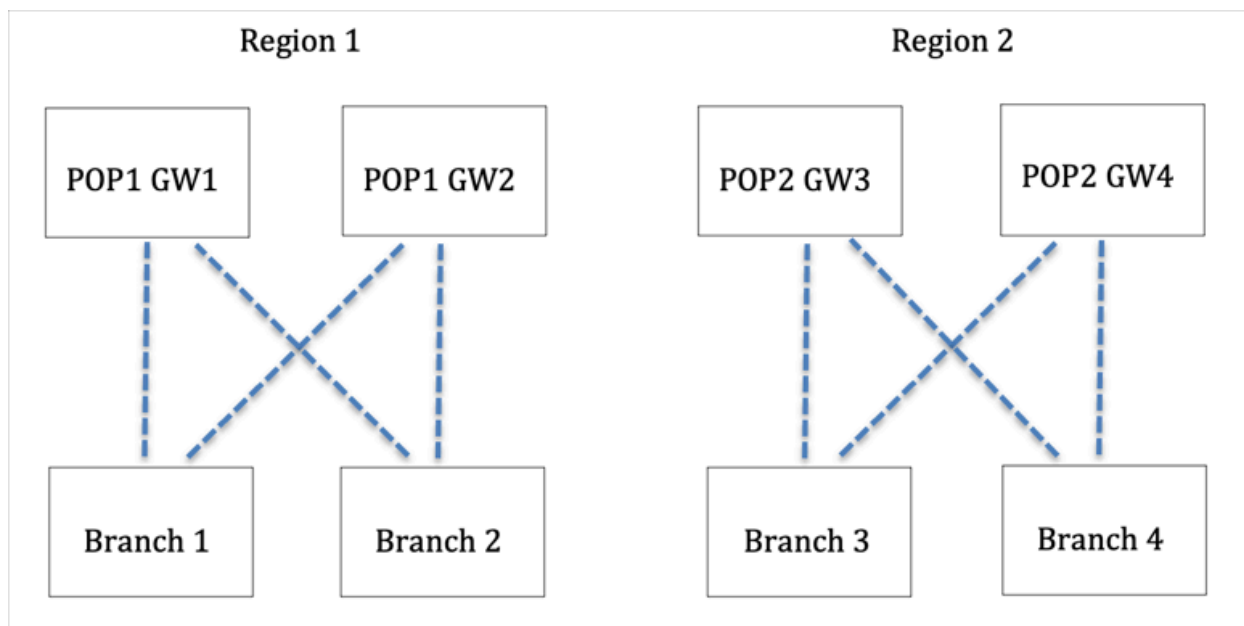
23. Click OK.

Example of Configuring BGP SLA-Based Routing

For Releases 22.1.1 and later.

This section shows an example of how to configure BGP SLA-based routing. In this example, gateways propagate application SLA metrics using multiprotocol BGP messages to all reachable branch devices. The branches can use these metrics in routing policies to influence the priority of routes, to mark specific communities, and to influence AS path manipulation, so that the branch can select the best route based on SLA metrics.

In the example, we configure peer and peer group policies on two VOS devices, Branch1 and Gateway1 (POP1 GW1), as illustrated in the topology shown in the following figure. The topology consists of two regions, with two branch devices and two gateway devices in each region. Each branch device has a circuit to each gateway in its region.



In the example, we configure the following types of profiles and policies:

- On the VOS branch devices:
 - SLA profiles to use in the peer and peer group policies. See [Configure SLA Profiles on the VOS Branch Devices](#).
 - A peer and peer group import policy. See [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#).
 - A peer and peer group export policy. See [Configure the Peer and Peer Group Export Policy on the VOS Branch Devices](#).
 - A peer and peer group export policy to support equal-cost multipath routing (ECMP) across gateways. See [Configure Support for ECMP across Gateways](#).
- On the gateways:
 - A peer and peer group policy to influence the AS paths length. See [Configure Terms on the Gateways To Influence the AS Path Length](#).

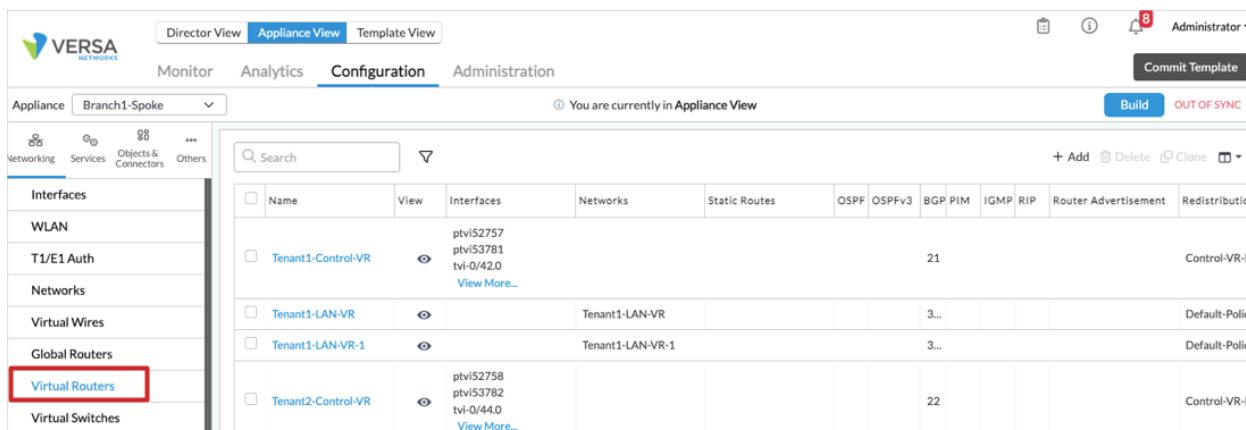
Configure SLA Profiles on the VOS Branch Devices

For this example, we configure the following SLA profiles, which are used by the peer and peer group policy terms that we configure below:

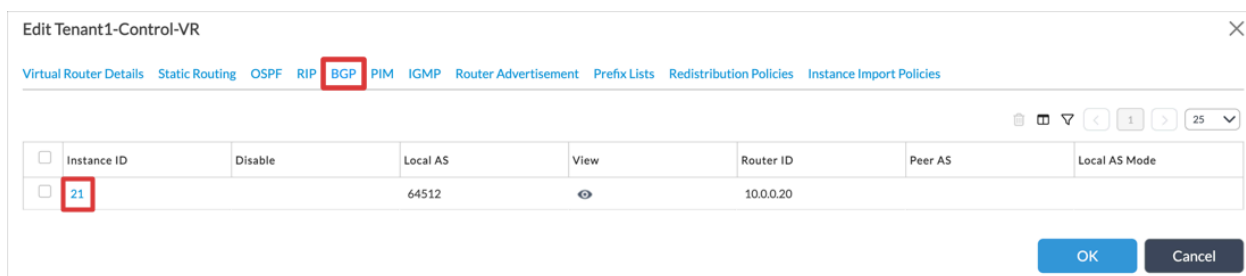
- pop1-sla—For use in the policy terms on Gateway 1 and Gateway 2 to set the latency and loss.
- pop2-sla—For use in the policy terms on Gateway 3 and Gateway 4 to set the latency and loss.
- all-gateways-monitor-profile—For use in the terms that configure the best SLA selection. To calculate the best SLA, the SLA profile uses least latency criteria.

To configure SLA profiles for the peer and peer group policies:

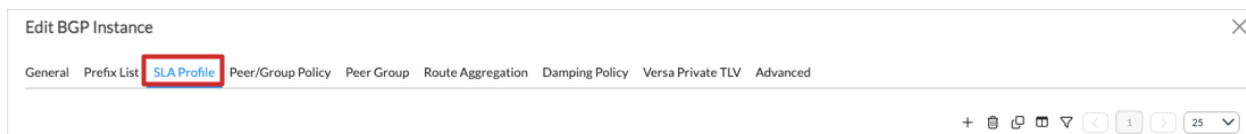
1. In Appliance view, select Networking > Virtual Routers. The main pane displays the virtual routers that are already configured.



2. Select an existing virtual router, or click **+** Add icon. The Edit *routing-instance-name* or Configure Virtual Router popup window displays.



3. Select the BGP tab, and then select an Instance ID or click **+** Add icon in the main pane. The Edit/Add BGP popup window displays.
4. Select the SLA Profile tab.



5. Click **+** Add icon. The Add BGP Instance Add SLA Profile popup window displays.
6. In the Profile Name field, enter the name pop1-sla.

Add BGP Instance Add SLA Profile

Profile Name *

Sequence

+ [Icons]

<input type="checkbox"/>	Sequence Number	Application Monitor
No Sequence Added		

OK Cancel

7. Click Add icon. The Add BGP Instance Add SLA Profile Add Sequence popup window displays.

Add BGP Instance Add SLA Profile Add Sequence

Sequence Number * Application Monitor SLA Measurement Scope Best Nexthop Selection Criteria

Max Threshold

Latency (milliseconds) Loss (%) Forwarding Class

OK Cancel

8. Select or enter the following information for the listed fields.

Field	Value
Sequence Number	1
Application Monitor	app-monitor-http-1
SLA Measurement Scope	Site to Gateway
Maximum Threshold (Group of Fields)	
◦ Latency	50
◦ Loss	2
Forwarding Class	Forwarding Class 4 (expedited-forwarding)

9. Click OK twice to return to the Edit/Add BGP Instance popup window.

10. Repeat Steps 6 through 9 to create an SLA profile named pop2-sla. Select or enter the following information for the listed fields.

Field	Value
Profile Name	pop2-sla
Sequence Number	1
Application Monitor	app-monitor-http-1
SLA Measurement Scope	Site to Gateway
Maximum Threshold (Group of Fields)	
◦ Latency	80
◦ Loss	4

11. Repeat Steps 6 through 9 to create an SLA profile named all-gateways-monitor-profile. Select or enter the following information for the listed fields.

Field	Value
Profile Name	all-gateways-monitor-profile
Sequence Number	1
Application Monitor	app-monitor-http-1
SLA Measurement Scope	Site to application
Best Next-Hop Selection Criteria	Least latency

12. Click OK twice to return to the Edit/Add BGP Instance popup window.

Configure the Peer and Peer Group Import Policy on the VOS Branch Devices

For this example, we configure an import policy that first selects a gateway or gateways in the first point of presence (POP1) and then in the second point of presence (POP2) if the SLA to those gateways is met. If the SLA to those gateways not met, the VOS devices calculates the best SLA using the set of gateways from POP1 and POP2 as part of a best SLA selection term. The default term sets an inferior local preference in case this route's SLA is not the best.

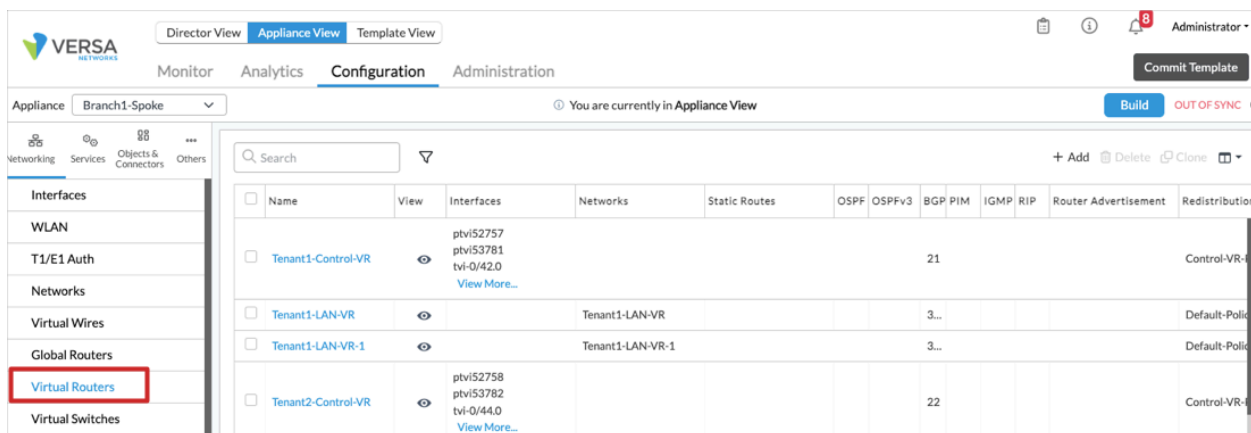
For this example, we configure the following peer and peer group policy information:

- Import_From_Hubs_Policy—Name of the peer and peer group policy.

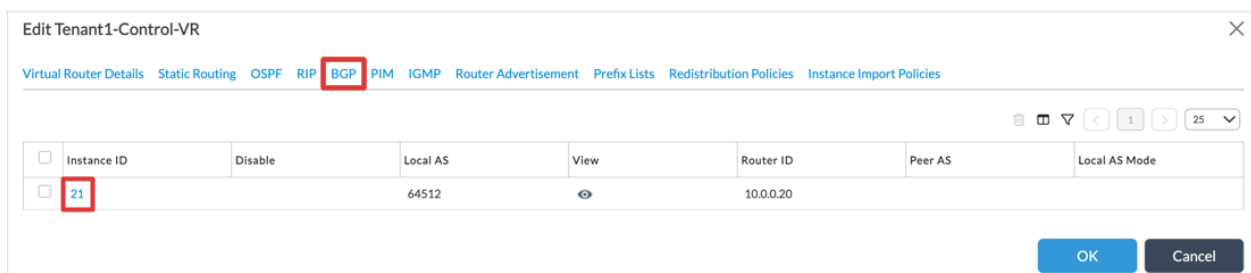
- POP1-GW1, POP1-GW2, POP2-GW3, and POP2-GW4—Name of the policy terms for selecting a specific gateway from a set of gateways if the application SLA through that gateway is met based on a user-defined order of gateways.
 - Term POP1-GW1 sets the local preference to 102 for routes received from this gateway if the application SLA through this gateway is met.
 - Term POP1-GW2 sets the local preference to 101 if the SLA is met.
 - Term POP2-GW3 sets the local preference to 104 if the SLA is met.
 - Term POP2-GW4 sets the local preference to 103 if the SLA is met.
- best-SLA-section-term—Name of the policy term to select the gateway or gateways with the best application SLA if the application SLA through the gateways in the previous terms is not met. This term sets the local preference to a fixed value based on comparing the SLAs through multiple gateways and then selects the best SLA using specific configuration information from the SLA profile.
- A default policy term sets the default preference for the routes if a specific route is not selected as the best path in the previous terms.

To configure the peer and peer group import policy on the VOS branch devices:

1. In Appliance view, select Networking > Virtual Routers. The main pane displays the virtual routers that are already configured.



2. Select an existing virtual router, or click **+** Add icon. The Edit *routing-instance-name* or Configure Virtual Router popup window displays.



3. Select the BGP tab, and then select an Instance ID or click **+** Add icon in the main pane. The Edit/Add BGP popup window displays.

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

Updated: Wed, 23 Oct 2024 08:25:28 GMT

Copyright © 2024, Versa Networks, Inc.

4. Select the Peer/Group Policy tab.

The screenshot shows the 'Edit BGP Instance' window. At the top, there are several tabs: 'General', 'Prefix List', 'SLA Profile', 'Peer/Group Policy' (which is highlighted with a red box), 'Peer Group', 'Route Aggregation', 'Damping Policy', 'Versa Private TLV', and 'Advanced'. Below the tabs, there is a toolbar with a red box around the '+' icon. Below the toolbar, there is a table with columns: 'Peer/Group Policy Name', 'Term Name', and 'Action'.

5. Select the BGP tab, and then select an Instance ID or click Add icon in the main pane. The Edit/Add BGP popup window displays.

6. Click Add icon. The Add BGP Instance Add Peer/Group Policy popup window displays.

The screenshot shows the 'Add BGP Instance Add Peer/Group Policy' window. At the top, there is a 'Name' field with a red asterisk, containing the text 'Import-From-Hubs-Policy'. Below the name field, there is a 'Terms' section with a toolbar containing a '+' icon and other icons. Below the toolbar, there is a table with columns: 'Term Name'. The table is currently empty, and the text 'No Term Added' is displayed in the center. At the bottom right, there are 'OK' and 'Cancel' buttons.

7. In the Name field, enter the name Import-From-Hubs-Policy.

8. Click the Add icon. The Add BGP Instance Add Peer/Group Policy Add Term popup window displays.

Add BGP Instance
Add Peer/Group Policy
Add Term

Term Name *

Match

Action

Standby Action

Family

--Select--

AS Path

Metric

NLRI

--Select--

Source Address

--Select--

Nexthop

--Select--

Well Known Community

--Select--

Community

Extended Community

Origin

--Select--

SLA Profile

Name

--Select--

Nexthop Name

--Select--

Local Circuit Name

--Select--

Nexthop List

☐

Nexthop List

Nexthop List Not Configured


Local Circuit List

☐

Local Circuit List

Local Circuit List Not Configured

9. Select the Match tab, and then select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW1
Extended Community	target:16021L:GW1-Site-ID target:8021L:GW1-Site-ID
SLA Profile (Group of Fields)	
<ul style="list-style-type: none"> Name 	pop1-sla. This is the SLA profile that we configured in Configure SLA Profiles on the VOS Branch Devices , above.
<ul style="list-style-type: none">  Add (in Next-Hop List field) 	Gateway1. This is the site name of GW1.

10. Select the Action tab, and then select or enter the following information for the listed fields.

Add BGP Instance
Add Peer/Group Policy
Add Term

Term Name *

Match
Action
Standby Action

Accept/Reject
Accept

Damping

☐ Enable ECMP for BGP Routes in RIB

Origin
--Select--

Nexthop

Local Preference
Allowed Range is 0 - 2147483647

AS Path
--Select--

Local AS Prepend Count
Allowed Range is 1 - 255

AS Path Prepend
Allowed Range is 1 - 4294967295

Community Action
--Select--

☐ SLA Community Action

Well Known Community
--Select--

Community

Route Preference

Extended Community Action
--Select--

Extended Community

Metric Action
--Select--

Metric
Allowed Range is 1 - 4294967295

OK
Cancel

Field	Value
Accept/Reject	Accept
Local Preference	102
Community Action	Append the set-community
Community	8009:8009

- Click OK.
- Repeat Steps 7 through 11 to create an term named POP1-GW2. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW2
Extended Community	target:16021L:GW2-Site-ID target:8021L:GW2-Site-ID
SLA Profile (Group of Fields)	
◦ Name	pop1-sla
◦ Add (in Next-Hop List field)	Gateway2
Accept/Reject	Accept
Local Preference	101
Community Action	Append the set-community
Community	8001:POP1-GW2-Site-ID;

13. Repeat Steps 7 through 11 to create an term named POP2-GW3. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW3
Extended Community	target:16021L:GW3-Site-ID target:8021L:GW3-Site-ID
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in Next-Hop List field)	Gateway3
Accept/Reject	Accept
Local Preference	104
Community Action	Append the set-community
Community	8001:POP2-GW3-Site-ID;

14. Repeat Steps 7 through 11 to create an term named POP2-GW4. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW4
Extended Community	target:16021L:GW4-Site-ID target:8021L:GW4-Site-ID
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in Next-Hop List field)	Gateway4
Accept/Reject	Accept
Local Preference	103
Community Action	Append the set-community
Community	8001:POP2-GW4-Site-ID;

15. Repeat Steps 7 through 11 to create an term named best-SLA-section-term. Select or enter the following information for the listed fields.

Field	Value
Term Name	best-SLA-section-term
SLA Profile (Group of Fields)	
◦ Name	all-gateways-monitor-profile
Add (in Next-Hop List field)	Gateway1
◦ Add (in Next-Hop List field)	Gateway2
◦ Add (in Next-Hop List field)	Gateway3
◦ Add (in Next-Hop List field)	Gateway4
Accept/Reject	Accept
Local Preference	100

16. Repeat Steps 7 through 11 to create an term named default-term. Select or enter the following information for the listed fields.

Field	Value
Term Name	default-term
Accept/Reject	Accept
Local Preference	99

17. Click OK to add the policy.

Configure the Peer and Peer Group Export Policy on the VOS Branch Devices

For this example, we configure the following export peer and peer group policy information:

- TO_SD-WAN—Name of the peer and peer group policy.
- POP1-GW1, POP1-GW2, POP2-GW3, and POP2-GW4—Name of the policy terms that, when the application SLA through the gateways is met, set the community of the exported routes to help the gateways set the right AS path length, to influence the routes being announced to the data center.
- best-SLA-section-term—Name of the policy term to select the gateway or gateways with the best application SLA if the application SLA through the gateways in the previous terms is not met. This term to set communities based on the best application SLA calculation.

To configure the peer and peer group export policy on the VOS branch devices:

1. Repeat Steps 1 through 6 in the previous section, [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#), above.
2. In the Add BGP Instance Add Peer/Group Policy popup window displays, in the Name field, enter the policy name TO_SD_WAN.
3. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW1. Select or enter the following information for the listed fields.

Field	Value
Name	TO_SDWAN
Term Name	POP1-GW1
SLA Profile (Group of Fields)	
◦ Name	pop1-sla. This is the SLA profile that we configured in Configure SLA Profiles on the VOS Branch Devices , above.
◦ Add (in the Next-Hop List field)	Gateway1. This is the site name of GW1.
Accept/Reject	Accept
Community	community 8001:POP1-GW1-Site-ID;

4. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW2. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW2
SLA Profile (Group of Fields)	
◦ Name	pop1-sla
◦ Add (in the Next-Hop List field)	Gateway2
Accept/Reject	Accept
Community	community 8001:POP1-GW2-Site-ID;

5. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW3. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW3
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in the Next-Hop List field)	Gateway3
Accept/Reject	Accept
Community	community 8001:POP2-GW3-Site-ID;

6. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW4. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW4
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in the Next-Hop List field)	Gateway4
Accept/Reject	Accept
Community	community 8001:POP2-GW3-Site-ID;

7. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named best-SLA-section-term. Select or enter the following information for the listed fields.

Field	Value
Term Name	best-SLA-section-term
SLA Profile (Group of Fields)	
◦ Name	all-gateways-monitor-profile
◦ Add (in the Next-Hop List field)	Gateway1
◦ Add (in the Next-Hop List field)	Gateway2
◦ Add (in the Next-Hop List field)	Gateway3
◦ Add (in the Next-Hop List field)	Gateway4
Accept/Reject	Accept
SLA Community Action	Click to enable the VOS device to automatically insert the appropriate community based upon the gateway selection with the best SLA.

8. Click OK to add the policy.

Configure Support for ECMP across Gateways

To use equal-cost multipath (ECMP) load balancing across a set of gateways, we configure the following import and export policies on the gateways:

- Import policy—For traffic from the gateways, we set the same local preference value for each gateway.
- Export policy—Configure a sequence of terms that use OR logic, called an OR series, with one term per gateway participating in the ECMP load balancing. For each gateway term except the last one, we specify the next gateway in the sequence using the Next Term field in the Action tab, and we select the value OR-series in Next-Term Action field. When the policy starts evaluating the terms in the OR series, when it encounters a match, that route is accepted and no further terms in the OR series are evaluated.

To configure peer and peer group export policy on Gateway 1 to support ECMP across gateways:

1. Repeat Steps 1 through 6 in the previous section, [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#), above.
2. In the Add BGP Instance Add Peer/Group Policy popup window displays, in the Name field, enter the policy name TO_SDWAN.

3. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW1. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW1
SLA Profile (Group of Fields)	
◦ Name	pop1-sla
◦ Add (in the Next-Hop List field)	Gateway1
Accept/Reject	Accept
Next Term	POP1-GW2
Community	8001:POP1-GW1-Site-ID;
Next Term Action	OR-series

4. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW2. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW2
SLA Profile (Group of Fields)	
◦ Name	pop1-sla
◦ Add (in the Next-Hop List field)	Gateway2
Accept/Reject	Accept
Next Term	POP2-GW3
Community	8001:POP1-GW2-Site-ID;
Next Term Action	OR-series

5. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW3. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW3
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in the Next-Hop List field)	Gateway3
Accept/Reject	Accept
Next Term	POP2-GW4
Community	8001:POP2-GW3-Site-ID;
Next Term Action	OR-series

6. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW4. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP2-GW4
SLA Profile (Group of Fields)	
◦ Name	pop2-sla
◦ Add (in the Next-Hop List field)	Gateway4
Accept/Reject	Accept
Community	8001:POP2-GW4-Site-ID;

7. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named best-SLA-section-term. Select or enter the following information for the listed fields.

Field	Value
Term Name	best-SLA-section-term
SLA Profile (Group of Fields)	
◦ Name	all-gateways-monitor-profile
◦ Add (in the Next-Hop List field)	Gateway1
◦ Add (in the Next-Hop List field)	Gateway2
◦ Add (in the Next-Hop List field)	Gateway3
◦ Add (in the Next-Hop List field)	Gateway4
Accept/Reject	Accept
SLA Community Action	Click to enable. This option causes VOS to automatically insert the appropriate community based upon the gateway selection with the best SLA.

- Click OK to add the policy.

Configure Terms on the Gateways To Influence the AS Path Length

To influence the AS path length of routes being announced to the data center, on the gateway, we configure peer and peer group export policy terms using the Local AS Prepend Count fields, which indicates the number of times to prepend the local AS number to the AS path. The example here configures a peer and peer group policy for the gateway POP1-GW1.

To configure policy terms on Gateway 1 to influence the AS path length:

- Repeat Steps 1 through 6 in the previous section, [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#), above.
- In the Add BGP Instance Add Peer/Group Policy popup window displays, in the Name field, enter the policy name Export-To-EBGP-Peer-Policy.
- Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create a term named POP1-GW1-Priority1. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW1-Priority1
Community	8001:GW1-Site-ID;
Accept/Reject	Accept
Local AS Prepend Count	1

4. Repeat Steps 7 through 11 in [Configure the Peer and Peer Group Import Policy on the VOS Branch Devices](#) to create an term named POP1-GW1-Priority2. Select or enter the following information for the listed fields.

Field	Value
Term Name	POP1-GW1-Priority2
Community	8002:GW1-Site-ID;
Accept/Reject	Accept
Local AS Prepend Count	2

5. Click OK to add the policy.

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 First AS Check, Soft Reconfiguration, Suppress Peer AS, Weight, Well-Known Community, and Private TLV .
- Release 22.1.1 adds support for configuring next-term action and SLA profiles.

Additional Information

[Configure Interchassis HA](#)

[Configure IP Multicast](#)

[Configure IP SLA Monitor Objects](#)

[Configure Virtual Routers](#)

[Troubleshoot Routing Protocols](#)