IPv6 Functionality

This chapter describes the options for enabling IPv6 functionality for Cisco SD-WAN templates and policies. Use the information in this chapter if your deployment uses IPv6.

Configure IPv6 Functionality for an Interface or Subinterface Template

To configure IPv6 functionality for an interface or subinterface template, perform the following steps.

Cisco SD-WAN supports dual stack: you can configure IPv4 and IPv6 in the same deployment. You can configure up to three global IPv6 addresses per interface.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. From **Basic Configuration**, click **IPv6** and configure the parameters that the following table describes:

Parameter Name	Description
Static	This radio button is selected by default because IPv6 addresses are static.
IPv6 Address	Enter the IPv6 address of the interface or subinterface.

Configure IPv6 Functionality for an OMP Template

To configure IPv6 functionality for an Overlay Management Protocol (OMP) template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco OMP** from the list of templates.

4. Click **Advertise** and choose **IPv6** to configure the parameters that the following table describes:

Parameter Name	Description
Connected	Click **Off** to disable advertising connected routes to OMP. By default, connected routes are advertised to OMP.
Static	Click **Off** to disable advertising static routes to OMP. By default static routes are advertised to OMP.
BGP	Click **On** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.

Configure IPv6 Functionality for a BGP Template

To configure IPv6 functionality for a Border Gateway Protocol (BGP) template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco BGP** from the list of templates.

4. Click **Unicast Address Family** and choose **IPv6** to configure the parameters that the following table describes:

Tab	Parameter Name	Description
	Maximum Paths	Specify the maximum number of parallel IBGP paths that can be installed into a route table to enable IBGP multipath load sharing.*Range:* 0 to 32
	Address Family	Enter the BGP IPv6 unicast address family.
RE-DISTRIBUTE		Click the **Redistribute** tab, and then click **Add New Redistribute**.
	Protocol	Select the protocols from which to redistribute routes into BGP, for all BGP sessions. Options are Connected, NAT, OMP, OSPF, and Static. At a minimum, select the following: • For service-side BGP routing, select OMP. By default, OMP routes are not redistributed into BGP. • For transport-side BGP routing, select Connected, and then under Route Policy, specify a route policy that has BGP advertise the loopback interface address to its neighbors.

Tab	Parameter Name	Description
	Route Policy	Enter the name of the route policy to apply to redistributed routes.
		Click **Add** to save the redistribution information.
NETWORK		Click the **Network** tab, and then click **Add New Network**.
	Network Prefix	Enter a network prefix, in the format of *prefix*/*length*, to be advertised by BGP.
		Click **Add** to save the network prefix.
AGGREGATE ADDRESS		Click the **Aggregate Address** tab, and then click **Add New Aggregate Address**.
	Aggregate Prefix	Enter the prefix of the addresses to aggregate for all BGP sessions, in the format prefix/length.
	AS Set Path	Click **On** to generate set path information for the aggregated prefixes.
	Summary Only	Click **On** to filter out more specific routes from BGP updates.
		Click **Add** to save the aggregate address.

1. In the Neighbor area, click **IPv6**, create a new neighbor or edit an existing one, and then configure the parameters that the following table describes.

Parameters marked with an asterisk are required.

Parameter Name	Description
IPv6 Address*	Specify the IPv6 address of the BGP neighbor.
Description	Enter a description of the BGP neighbor.
Remote AS*	Enter the AS number of the remote BGP peer.
Address Family	Select **Global** from the drop-down list, click **On** and select the address family. Enter the address family information.
Shutdown	To shut down a BGP neighbor when you push the template, select **Global** from the drop-down list and then click **Yes**.*Default:* Off

Configure IPv6 Functionality for a VRRP Template

To configure IPv6 functionality for a Virtual Router Redundancy Protocol (VRRP) template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. Click **VRRP** and choose **IPv6**.
5. Click **New VRRP**.
6. Configure the parameters that the following table describes:

Parameter Name	Description
Group ID	Enter a virtual router ID, which represents a group of routers. Range: 1 through 255
Priority	Enter the priority level of the router within a VRRP group. • *Range:* 1 through 254 • *Default:* 100
Timer	Not used.
Track OMP	Select **On** to track the Overlay Management Protocol (OMP) session running on the WAN connection when determining the primary VRRP virtual router.*Default:* Off
Track Prefix List	Enter a value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy.
Link Local IPv6 Address	Enter a virtual link local IPv6 address, which represents the link local address of the group. The address should be in standard link local address format. For example, FE80::AB8.
Global IPv6 Address	Enter a virtual global unicast IPv6 address, which represents the global address of the group. The address should be an IPv6 global prefix address that has the same mask as the interface forwarding address on which the VRRP group is configured. For example, 2001::2/124. You can configure up to 3 global IPv6 addresses.

Configure IPv6 Functionality for an ACL Template or a QoS Template

To configure IPv6 functionality for an ACL and QoS template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco VPN Interface Ethernet** from the list of templates.
4. From **ACL/QoS**, configure the parameters that the following table describes:

Parameter Name	Description
Ingress ACL – IPv6	Click **On** to enable the IPv6 ingress access list.
IPv6 Ingress Access List	Enter the name of the IPv6 ingress access list.
Egress ACL – IPv6	Click **On** to enable the IPv6 egress access list.
IPv6 Egress Access List	Enter the name of the IPv6 egress access list.

Configure IPv6 Functionality for a Logging Template

To configure IPv6 functionality for a Logging template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template** and then select an appropriate device model.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

3. Select **Cisco Logging** from the list of templates.
4. From **Server**, click **IPv6**.
5. Configure the parameters that the following table describes.

Parameter Name	Description
IPv6 Hostname/IPv6 Address	Host name or IP address of the server to direct the logging information.
VPN ID	VPN ID of the VPN source interface.
Source Interface	Name of the source interface.
Priority	Choose the maximum severity of messages that are logged.

Configure IPv6 Functionality for a New Prefix List

To configure an IPv6 address for a new prefix list, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.

2. From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Prefix** from the list on the left and then select **New Prefix List**.
4. Click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 Functionality for a Data Prefix

To configure an IPv6 address for a new prefix list, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. From the Custom Options drop-down list, select **Lists**. You can make this selection for a Centralized Policy or a Localized Policy
3. Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.
4. From **Internet Protocol**, click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 Functionality for a Centralized Policy

To configure a centralized policy to apply to IPv6 address families, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select **Traffic Data**.
4. Select **Add Policy** and click **Create New**.
5. Click **Sequence Type** and then select **Traffic Engineering**.
6. Click **Sequence Rule**.
7. From the **Protocol** drop-down list, select **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.
8. Click **Sequence Type** and then select **QoS**.
9. Click **Sequence Rule**.
10. From the Protocol drop-down list, click **IPv6** to apply the policy only to IPv6 address families, or select **Both** to apply the policy IPv4 and IPv6 address families.

Configure IPv6 Functionality for a Localized Policy

To configure a localized policy to apply to IPv6 address families, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. From the **Custom Options** drop-down list, select **Access Control Lists** under Localized Policy.
3. Click **Add Access Control List Policy** and choose **Add IPv6 ACL Policy**. The policy you create will apply only to IPv6 address families.