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. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button 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.

CLI equivalent:

```
interface GigabitEthernet1
  no shutdown
  ipv6 address 2001:DB8:1::1/64
  ipv6 enable
```

Configure IPv6 Functionality for an OMP Template

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

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **OMP** from the list of templates.

4. In the Basic Configuration area, click the **IPv6** button in the ADVERTISE area and 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.

CLI equivalent:

First enable Service VRF for IPv6:

```
config-transaction
vrf definition 1
  rd 1:1
  address-family ipv6
```

Next enable OMP.

OMP supports global IPv6 configuration. In addition, per VRF level configuration is allowed. Per VRF level configuration overrides global configuration.

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    advertise static
```

Global configuration is the default configuration, so IPv6 is enabled by default for OMP. To disable IPv6 OMP route redistribution for a particular VRF, configure the redistribution protocol to no as follows:

```
config-transaction
sdwan
  omp
  !
  address-family ipv6
   advertise bgp
   advertise connected

   address-family ipv6 vrf 1
    no advertise connected
    no advertise static
    no advertise bgp
```

Configure IPv6 Functionality for a BGP Template

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

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **BGP** from the list of templates.
4. In the Unicast Address Family area, click the **IPv6** button and 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.
	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 the **IPv6** button, 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

CLI equivalent:

```
config-transaction
router bgp 1
 bgp log-neighbor-changes
  address-family ipv6 unicast vrf 1
  neighbor 2001:DB8:19::1 remote-as 2
  neighbor 2001:DB8:19::1 activate
  neighbor 2001:DB8:19::1 advertisement-interval 1
  neighbor 2001:DB8:19::1 password cisco
  redistribute omp
  redistribute static
  exit-address-family
```

Configure IPv6 Functionality for a VRRP Template

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

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the VRRP area, click the **IPv6** button and then click **New VRRP**.
5. 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

Parameter Name	Description
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.

CLI equivalent:

```
config-transaction
interface GigabitEthernet1

 vrrp 10 address-family ipv6
   priority 20
   track omp shutdown
   address FE80::10:100:1 primary
   address 2001:10:100::1/64

Prefix-list tracking
track 1 ipv6 route 1:1::1/128
 reachability
 ipv6 vrf 1

 track 2 ipv6 route 2:2::2/128
 reachability
 ipv6 vrf 2

 track 20 list boolean or
  object 1
  object 2

vrrp 10 address-family ipv6
  track 20 shutdown
```

Configure IPv6 Functionality for an SNMP Template

To configure IPv6 functionality for an SNMP template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **SNM**P from the list of templates.

4. In the SNMP Version area, click the **SNMP Version** button ► **TRAP TARGET SERVER** and create or edit an SNMP trap target.

1. Configure the parameters that the following table describes.

Parameter Name	Description
VPN ID	Enter the number of the VPN to use to reach the trap server.*Range:* 0 through 65530
IP Address	Enter the IP address of the SNMP server.
UDP Port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Trap Group Name	Select the name of a trap group that was configured under the Group tab.
User Name	Select the name of a community that was configured under the Community tab.
Source Interface	Enter the interface to use to send traps to the SNMP server that is receiving the trap information.

Note Make sure that you have already configured the SNMP community and trap target group.

CLI equivalent:

The following example permits any SNMP to access all objects with read-only permission using the community string named public. The device also will send Border Gateway Protocol(BGP) traps IPv6 host 3ffe:b00:c18:1::3/127 using SNMP v1.The community string named public will be sent with the traps.

```
Device# config-transaction
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps bgp
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

In the following example, the SNMP context A is associated with the views in SNMPv2c group GROUP1 and the IPv6 named access list public2:

```
Device# config-transaction
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list comm AVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c contextA read viewA write viewA notify access
 ipv6 public2
```

The following example configures the IPv6 host as the notification server:

```
Device> enable
Device# config-transaction
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group publicv2c access ipv6 public2
Device(config)# snmp-server hosthost1.com2c vrf trap-vrf
Device(config)# snmp-server user user1 bldg1 remote3ffe:b00:c18:1::3/127 v2c access ipv6
```

```
public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```

Configure IPv6 Functionality for a DHCP Relay Agent Template

To configure IPv6 functionality for a DHCP Relay Agent template, follow these steps:

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the Basic Configuration area, click the **IPv6** button.
5. Click **Add** next to DHCP Helper.
6. Configure the parameters that the following table describes.

Table 1:

Parameter Name	Description
DHCPv6 Helper #	IP address of the DHCP helper
DHCPv6 Helper VPN	VPN ID of the VPN source interface for the DHCP helper.

CLI equivalent:

```
device-configuration
interface GigabitEthernet8
 vrf forwarding 2
 no ip address
 ipv6 address 2001:A14:99::F/64
 ipv6 dhcp relay destination vrf 1 2001:A14:19::12 GigabitEthernet2
```

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. In Cisco vManage NMS, select the Configuration ► **Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **VPN Interface Ethernet** from the list of templates.
4. In the ACL/QoS area, 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.

Parameter Name	Description
IPv6 Egress Access List	Enter the name of the IPv6 egress access list.

CLI Equivalent for Configuring IPv6 Functionality for an ACL Template:

```
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#    sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-ip 2001:380:1::64/128
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     action accept
Device(config-action)#

Device(config)# sdwan interface GigabitEthernet6 ipv6 access-list ipv6_acl in
Device(config-interface-GigabitEthernet6)#
Device(config-interface-GigabitEthernet6)#

Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64

Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv_ipv6_prefix
Device(config-access-list-ipv_ipv6_prefix)# sequence 11
Device(config-sequence-11)#     match
Device(config-match)#       source-data-prefix-list data-ipv6-prefix-list
Device(config-match)#       destination-data-prefix-list source_ipv6_list
Device(config-match)#      destination-ip 2001:3c0:1::64/128
Device(config-match)#      source-port      4000
Device(config-match)#      destination-port 3000
Device(config-match)#      traffic-class    6
Device(config-match)#      next-header      6
Device(config-match)#      packet-length    1000
Device(config-match)#     !
Device(config-match)#     action accept
```

CLI Equivalent for Configuring IPv6 Functionality for a QoS Template:

```
Device(config)# class-map match-any class0
Device(config-cmap)#  match qos-group 0
Device(config-cmap)# class-map match-any class1
Device(config-cmap)#  match qos-group 1
Device(config-cmap)# !
Device(config-cmap)# policy-map qos_map_for_data_policy
Device(config-pmap)#  class class0
Device(config-pmap-c)#   bandwidth percent 10
Device(config-pmap-c)#   random-detect
Device(config-pmap-c)#  class class1
Device(config-pmap-c)#   bandwidth percent 10
Device(config-pmap-c)#   random-detect
Device(config-pmap-c)#
Device(config-pmap-c)# policy
Device(config-policy)#  no app-visibility
Device(config-policy)#  class-map
Device(config-class-map)#   class class0 queue 0
Device(config-class-map)#   class class1 queue 1
```

```
Device(config-class-map)# !
Device(config-class-map)#  ipv6
Device(config-ipv6)#   access-list fwd_class_data_policy
Device(config-access-list-fwd_class_data_policy)#    sequence 5
Device(config-sequence-5)#     match
Device(config-match)#      traffic-class 0
Device(config-match)#     !
Device(config-match)#     action accept
Device(config-action)#      count fwd_class_data_policycnt_5
Device(config-action)#      class class0
Device(config-action)#     !
Device(config-action)#    !
Device(config-action)#    sequence 6
Device(config-sequence-6)#     match
Device(config-match)#      traffic-class 1
Device(config-match)#     !
Device(config-match)#     action accept
Device(config-action)#      count fwd_class_data_policycnt_6
Device(config-action)#      class class1
Device(config-action)#     !
Device(config-action)#    !
Device(config-action)#    !
Device(config-action)#    default-action drop

class-map match-any class0
match qos-group 0
class-map match-any class1
match qos-group 1
!
policy-map qos_map_for_data_policy
class class0
  bandwidth percent 10
  random-detect
class class1
  bandwidth percent 10
  random-detect

policy
no app-visibility
class-map
  class class0 queue 0
  class class1 queue 1
!
ipv6
  access-list fwd_class_data_policy
   sequence 5
    match
     traffic-class 0
    !
    action accept
     count fwd_class_data_policycnt_5
     class class0
    !
   sequence 6
    match
     traffic-class 1
    !
    action accept
     count fwd_class_data_policycnt_6
     class class1
!
default-action drop
```

Configure IPv6 Functionality for a Logging Template

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

1. In Cisco vManage NMS, select the **Configuration ► Templates** screen.
2. Select **Feature ► Add Template** and then select an appropriate device model.
3. Select **Logging** from the list of templates.
4. In the Server area, click the **IPv6** button.
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.

CLI equivalent:

```
config-transaction
Device(config)# logging host ipv6
AAAA:BBBB:CCCC:DDDD::FFFF
```

Configure IPv6 Functionality for a New Prefix List

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

1. In Cisco vManage NMS, select **Configuration ► Policies**.
2. From the Custom Options drop-down menu, 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. Select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

CLI equivalent:

```
config-transaction
Device(config)# policy
Device(config-policy)# ipv6
Device(config-ipv6)# access-list ipv6_acl
Device(config-access-list-ipv6_acl)#  sequence 11
Device(config-sequence-11)#  match
Device(config-match)# source-ip 2001:380:1::64/128
Device(config-match)# destination-ip 2001:3c0:1::64/128
```

Configure IPv6 Functionality for a Data Prefix

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

1. In Cisco vManage NMS, select **Configuration ► Policies**.

2. From the Custom Options drop-down menu, 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. In the Internet Protocol area, select the **IPv6** radio button and enter the IPv6 address in the Add Prefix field.

CLI equivalent:

```
Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:380:1::/64
```

Configure IPv6 Functionality for a Centralized Policy

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

1. In Cisco vManage NMS, select **Configuration ► Policies**.
2. From the Custom Options drop-down menu, select **Traffic Policy** under Centralized Policy.
3. Select the **Traffic Data** tab.
4. Select Add Policy ► Create New.
5. Click the **Sequence Type** button and then select **Traffic Engineering**.
6. Click the **Sequence Rule** button.
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 the **Sequence Type** button and then select **QoS**.
9. Click the **Sequence Rule** button.
10. 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.

CLI equivalent:

```
config-transaction
(config)# policy
(config-policy)# lists ipv6-prefix-list foo ipv6-prefix 1::1/64
                 ipv6-prefix-list ipv6-1
                 ipv6-prefix 1::1/128
```

Configure IPv6 Functionality for a Localized Policy

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

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

CLI equivalent:

In the following example, IPv6 routes that have addresses specified by the prefix list named marketing are matched:

```
config-transaction
Device(config)# route-map name
Device(config-route-map)# match ipv6 address prefix-list marketing
```