IPv6 Functionality

Configure IPv6 functionality for an Interface or Subinterface using templates

Before you begin

Perform these steps to configure IPv6 functionality for an interface or subinterface template.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 From **Basic Configuration**, click **IPv6** and configure these parameters.

Field	Description
Static	Selected by default because IPv6 addresses are static.
IPv6 Address	IPv6 address of the interface or subinterface.

Configure IPv6 functionality for an interface or subinterface using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure according to this example.

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

Configure IPv6 functionality for OMP using templates

Before you begin

Perform these steps to configure IPv6 functionality for OMP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

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

Step 4 In the **Advertise** section, select **IPv6** and configure these parameters.

Field	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 **Off** to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.

Configure IPv6 functionality for OMP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Enable service VRF for IPv6, according to this example.

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

Step 3 Enable OMP, according to this example.

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
```

Step 4 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**.

```
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 BGP using templates

Before you begin

Perform these steps to configure IPv6 functionality for BGP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

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

Step 4 In the **Unicast Address Family** section, select **IPv6** and configure these parameters.

Tab	Field	Description
	Maximum Paths	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	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 these: • 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	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	Network prefix in the format of prefix/length, for BGP to advertise.
		Click **Add** to save the network prefix.

Tab	Field	Description
AGGREGATE ADDRESS		Click the **Aggregate Address** tab, and then click **Add New Aggregate Address**.
	Aggregate Prefix	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.

Step 5 In the **Neighbor** section, select **IPv6**, create a new neighbor or edit an existing one, and then configure these parameters.

Field	Description
IPv6 Address*	IPv6 address of the BGP neighbor.
Description	Description of the BGP neighbor.
Remote AS*	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 BGP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure according to this example.

```
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 VRRP using templates

Before you begin

Perform these steps to configure IPv6 functionality for Virtual Router Redundancy Protocol (VRRP).

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **VRRP** section, select **IPv6**.

Step 5 Click **New VRRP** and configure these parameters.

Field	Description
Group ID	Virtual router ID, which represents a group of routers. Range: 1 to 255
Priority	Priority level of the router within a VRRP group. Range: 1 to 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	Value to track a list of IPv6 remote prefixes. This value is an alphanumeric string that is configured under Policy.
Link Local IPv6 Address	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.

Field	Description
Global IPv6 Address	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. Example: 2001::2/124 Maximum: 3 global IPv6 addresses

Configure IPv6 functionality for VRRP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure VRRP, according to this example.

```
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 SNMP using templates

Before you begin

Configure the SNMP community and trap target group.

Perform these steps to configure IPv6 functionality for SNMP.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco SNMP** from the list of templates.

Step 4 In the **Trap** section, create or edit an SNMP trap target.

Note the prerequisites for this procedure.

Step 5 Configure these parameters.

Field	Description
VPN ID	Number of the VPN to use to reach the trap server. Range: 0 to 65530
IP Address	IP address of the SNMP server.
UDP Port	UDP port number for connecting to the SNMP server. Range: 1 to 65535
Trap Group Name	Name of a trap group configured in the **Group** tab.
User Name	Name of a community configured in the **Community** tab.
Source Interface	Interface to use to send traps to the SNMP server that is receiving the trap information.

Configure IPv6 functionality for SNMP using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure SNMP, according to these examples.

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

This 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 mgr
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 using templates

Before you begin

Perform these steps to configure IPv6 functionality for a DHCP relay agent.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **Basic Configuration** section, select **IPv6**.

Step 5 In the **DHCP Helper** area, click **Add** and configure these parameters.

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

Configure IPv6 functionality for a DHCP relay agent using CLI commands

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a DHCP relay agent, according to this example.

```
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 ACL and QoS using templates

Before you begin

Perform these steps to configure IPv6 functionality for access control lists (ACL) and quality of service (QoS).

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco VPN Interface Ethernet** from the list of templates.

Step 4 In the **ACL/QoS** section, configure these parameters.

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 ACL and QoS using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for access control lists (ACL) and quality of service (QoS).

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure ACL according to this example.

```
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
```

Step 3 Configure QoS according to this example.

```
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 host using templates

Before you begin

Perform these steps to configure IPv6 functionality for a logging host.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

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

Step 3 Select **Cisco Logging** from the list of templates.

Step 4 From **Server**, click **IPv6** and configure these parameters.

Field	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.

Field	Description
Source Interface	Name of the source interface.
Priority	Maximum severity of messages that are logged.

Configure IPv6 functionality for a logging host using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a logging host.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a logging host, according to this example.

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

Note
Creating and deleting the logging host configurations in same transaction causes unexpected behavior. For example, deleting **logging host** *ipv6-address* and creating **logging host** *ipv6-address* **vrf** *vrf-name* configuration in same transaction causes both configurations to disappear from the device. Send the two requests in separate transactions.

Configure IPv6 functionality for a prefix list using templates

Before you begin

Perform these steps to configure IPv6 functionality for a prefix list.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a centralized policy or a localized policy.

Step 3 Select **Prefix** from the list on the left and then select **New Prefix List**.

Step 4 Click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 functionality for a prefix list using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a prefix list.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a prefix list, according to this example.

```
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:DB8:1::64/128
Device(config-match)# destination-ip 2001:DB8:1::64/128
```

Configure IPv6 functionality for a data prefix using templates

Before you begin

Perform these steps to configure IPv6 functionality for a data prefix.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Lists**. You can make this selection for a centralized policy or a localized policy.

Step 3 Select **Data Prefix** from the list on the left and then select **New Data Prefix List**.

Step 4 From **Internet Protocol**, click **IPv6** and enter the IPv6 address in **Add Prefix**.

Configure IPv6 functionality for a data prefix using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a data prefix.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a data prefix, according to this example.

```
Device(config)# policy lists data-ipv6-prefix-list source_ipv6_list
Device(config-data-ipv6-prefix-list-source_ipv6_list)# ipv6-prefix 2001:DB8:1::/64
```

Configure IPv6 functionality for a centralized policy using templates

Before you begin

Perform these steps to configure IPv6 functionality for a centralized policy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Traffic Policy** under **Centralized Policy**.

Step 3 Select **Traffic Data**.

Step 4 Select **Add Policy** and click **Create New**.

Step 5 Click **Sequence Type** and then select **Traffic Engineering**.

Step 6 Click **Sequence Rule**.

Step 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.

Step 8 Click **Sequence Type** and then select **QoS**.

Step 9 Click **Sequence Rule**.

Step 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 centralized policy using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a centralized policy.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a IPv6 in a centralized policy, according to this example.

```
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 using templates

Before you begin

Perform these steps to configure IPv6 functionality for a localized policy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

Step 2 From the **Custom Options** drop-down list, select **Access Control Lists** under **Localized Policy**.

Step 3 Click **Add Access Control List Policy** and choose **Add IPv6 ACL Policy**. The policy you create applies only to IPv6 address families.

Configure IPv6 functionality for a localized policy using CLI commands

Before you begin

Perform these steps to configure IPv6 functionality for a localized policy.

Procedure

Step 1 Create a CLI add-on profile or CLI add-on template.

Step 2 Configure a IPv6 in a localized policy, according to this example.

The example matches IPv6 routes that have addresses specified by the prefix list called marketing.

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