IPv6 Functionality

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

This chapter describes the options for enabling IPv6 functionality for Cisco Catalyst 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 Catalyst 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 SD-WAN Manager 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.

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. From the Cisco SD-WAN Manager 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.

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. From the Cisco SD-WAN Manager 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.
	Route Policy	Enter the name of the route policy to apply to redistributed routes.
		Click **Add** to save the redistribution information.

Tab	Parameter Name	Description
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

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. From the Cisco SD-WAN Manager 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.

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. From the Cisco SD-WAN Manager 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. Click **Cisco SNMP** from the list of templates.
4. Choose **SNMP Version** > **TRAP TARGET SERVER** and create or edit an SNMP trap target.
5. 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 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 Template

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

1. From the Cisco SD-WAN Manager 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**.
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. From the Cisco SD-WAN Manager 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.

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. From the Cisco SD-WAN Manager 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.

CLI equivalent:

```
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 behaviour. 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. We recommend you to send the two requests in separate transactions.

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 SD-WAN Manager 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**.

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. From the Cisco SD-WAN Manager 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**.

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. From the Cisco SD-WAN Manager 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.

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. From the Cisco SD-WAN Manager 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.

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
```


DHCP for IPv6

Table 2: Feature History

Feature Name	Release Information	Description
DHCP for IPv6	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature allows you to configure DHCP for IPv6 (DHCPv6) on Cisco IOS XE Catalyst SD-WAN devices to assign IPv6 addresses to hosts on an IPv6-enabled network. Assigning of IPv6 addresses is accomplished using SLAAC, DHCPv6, DHCPv6 Prefix Delegation, or DHCPv6 Relay. A Cisco IOS XE Catalyst SD-WAN device can be configured for DHCPv6 as a DHCP server, DHCP client, or as a DHCP relay agent.

Prerequisites for DHCPv6

- Basic IPv6 connectivity for assigning IPv6 addresses to hosts connected to the Cisco IOS XE Catalyst SD-WAN devices.

Restrictions For DHCPv6

- This feature is supported only through CLI configuration.

- A unique DHCPv6 pool name must be provied for each VRF.

Information About DHCPv6

You can configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to assign addresses on an IPv6-enabled network. Alternatively, you can also configure Stateless Address Autoconfiguration (SLAAC) to assign addresses on an IPv6-enabled network.

SLAAC

The most common method for IPv6 client address assignment is SLAAC. SLAAC provides simple plug-and-play connectivity where hosts self-assign an address based on the IPv6 prefix.

SLAAC is configured as follows:

- Host sends a router solicitation message.
- Hosts waits for a Router Advertisement (RA) message.
- Hosts take the first 64 bits of the IPv6 prefix from the RAmessage and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the RA message, as its default gateway.
- Duplicate Address Detection (DAD) is performed by IPv6 clients in order to ensure that random addresses that are picked do not collide with other clients.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IP v6 address can be learned based on the following 2 algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated.

SLAAC and DHCPv6

DHCPv6

IPv6 devices use multicast to acquire IP addresses and to find DHCPv6 servers. The basic DHCPv6 client-server concept is similar to DHCP for IPv4. If a client wants to receive configuration parameters, it sends out a request on the attached local network to detect available DHCPv6 servers. The server responds with the requested information in a Reply message.

The DHCPv6 client knows whether to use DHCPv6 based upon the instruction from a router on its link-local network. The default gateway has two configurable bits in its RA available for this purpose:

- O bit—When this bit is set, the client can use DHCPv6 to retrieve other configuration parameters (for example, TFTP server addressor DNS server address) but not the client's IP address.
- M bit—When this bit is set, the client can use DHCPv6 to retrieve a managed IPv6 address and other configuration parameters from a DHCPv6 server.

Stateless DHCP

Stateless DHCPv6 is a combination of SLAAC and DHCPv6. With this option SLAAC is still used to retrieve an IP address while DHCP is used to obtain additional information such as TFTP server addressor, DNS server

address. In this case, the device sends an RA with the O bit set but does not set the M bit. This is known as Stateless DHCPv6 because the DHCPv6 server does not have to track the client address bindings.

Stateful DHCP

Stateful DCHPv6 functions exactly the same as DHCP IPv4 in which hosts receive both their IPv6 address and additional parameters from the DHCP server. When a device sends an RA with the M bit set, this indicates that clients must use DHCP to obtain their IP addresses. When the M bit is set, the setting of the O bit is irrelevant because the DHCP server also returns other configuration information together with the addresses. This is known as Stateful DHCPv6 because the DHCPv6 server tracks the client address bindings.

DHCPv6 Prefix Delegation

The DHCPv6 prefix delegation feature is a stateful mode of operation for simple delegation of prefixes from a delegating edge device (DHCP server) to requesting edge device (DHCP clients).

DHCPv6 prefix delegation feature is ideal for the following situations where:

- A delegating edge device that does not have the information about the topology of the networks to which the requesting edge device is attached to.
- A delegating edge device does not require other information apart from the identity of the requesting edge device to choose a prefix for delegation. This mechanism is appropriate for use by an ISP to delegate a prefix to a subscriber. After the ISP has delegated prefixes to a subscriber, the subscriber may further subnet and assign prefixes to the links within the subscriber's network.

DHCPv6 Relay

A DHCPv6 relay agent is an edge device, residing on the client's network, is used to relay messages between the client and the server when a DHCPv6 server is not in the same network as the DHCPv6 clients.

Benefits of DHCPv6

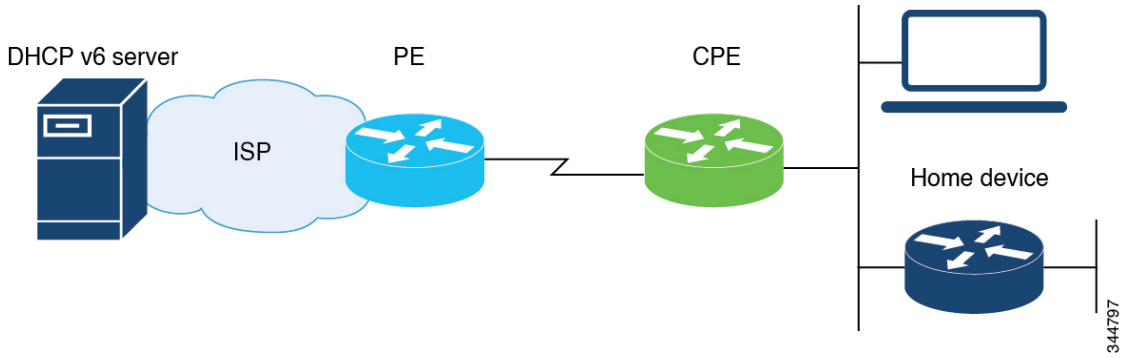
Configuring DHCP for IPv6 allows you to have more IP address compared to IPv4. With IPv6, there can be no depletion of IP addresses.

Use Cases For DHCPv6

Cisco IOS XE Catalyst SD-WAN devices can be configured for DHCPv6 as a server, client, or a relay agent. As a server, a Cisco IOS XE Catalyst SD-WAN device can be configured for SLAAC, Stateless DHCP or for prefix delegation.

SLAAC with DHCP

The figure below shows a typical broadband deployment.



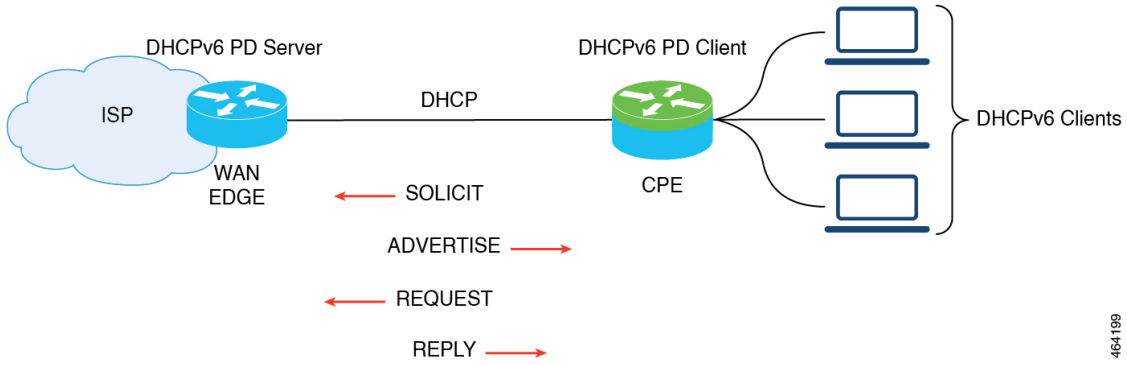
A Cisco IOS XE Catalyst SD-WAN device deployed on a customer premises (CPE) and connected to a ISP edge (PE) device can be a stateless or stateful DHCPv6 client. In either case, the ISP-side DHCPv6 server might provide configuration parameters such as Domain Name System (DNS) server addresses, domain names, and Simple Network Time Protocol (SNTP) servers to the DHCP client on the CPE. Such information can be specific to ISPs.

In addition to being a DHCPv6 client (toward the ISP), the CPE can act as a DHCPv6 server to the home network. For example, neighbor discovery followed by a stateless or stateful DHCPv6 client can occur on the link between the CPE and the home devices. In some cases, the information to be provided to the home network is the same as that obtained from the ISP-side DHCPv6 server. Therefore, the DHCPv6 component on the CPE allows automatic importing of configuration parameters from the DHCPv6 client to the DHCPv6 server pool.

DHCPv6 Prefix Delegation

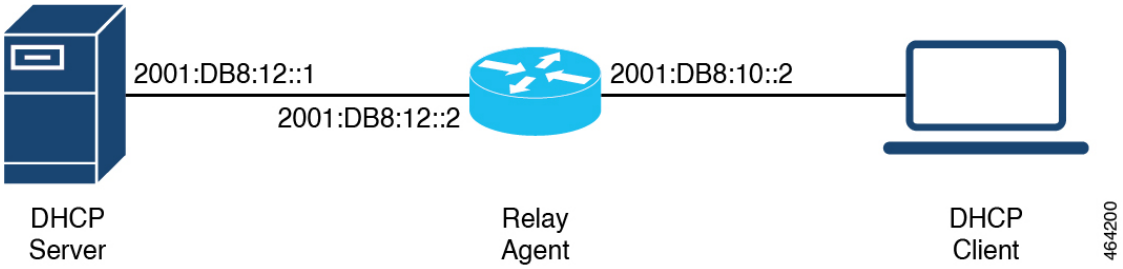
The model of operation for prefix delegation is as follows. In this sample topology, an edge device is configured as a DHCP server which is provisioned with prefixes to be delegated to a DHCP client. A Cisco IOS XE Catalyst SD-WAN device is configured as a DHCP client and requests prefix(es) from the server. The server chooses prefix(es) for delegation and responds with prefix(es) to the DHCP client. The DHCP client is then responsible for the delegated prefix(es).

For example, the client might assign a subnet from a delegated prefix to one of its interfaces and begin sending Router Advertisements for the prefix on that link. Each prefix has an associated preferred lifetime and valid lifetime, which constitute an agreement about the length of time over which the client is allowed to use the prefix. A client can request an extension of the lifetimes on a delegated prefix and is required to terminate the use of a delegated prefix if the valid lifetime of the prefix expires.



DHCPv6 Relay

In this sample topology, the DHCP server is not in the same network as DHCP client. A Cisco IOS XE Catalyst SD-WAN device residing on the client's network acts as a relay agent to relay messages between the client and the server.



Configure DHCPv6

1. From Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

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

3. From **Create Template** drop-down, choose **CLI Template**.

Note You can also use the CLI Add-on template to configure DHCP for IPv6 for client and server. For more information, see Create a CLI Add-On Feature Template.

4. From **Device Model**, choose a device model for which you are creating the template.
5. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any character and spaces.
7. In the **CLI Configuration** field, enter the DHCP configuration for IPv6 for client and server by typing it, cutting and pasting it, or uploading a file.
8. Click **Save**.

Configure SLAAC

This example shows how to configure SLAAC on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
```

```
device(config-if)# ipv6 enable
device(config-if)# end
```

This example shows how to configure SLAAC on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

Configure SLAAC and DHCPv6 Pool for Options

This example shows how to configure SLAAC and DHCPv6 pool on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address autoconfig
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure SLAAC and DHCPv6 pool on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd other-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

Configure DHCPv6 (stateful) Address Assignment

This example shows how to configure DHCPv6 address assignment on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure DHCPv6 address assignment on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
```

```
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# address prefix 2010:AB8:0:1::1/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
```

Configure DHCPv6 with Prefix Delegation (stateful)

This example shows how to configure DHCPv6 with prefix delegation on the client side.

```
device(config)# interface GigabitEthernet0/0/2
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 dhcp client pd prefix_from_provider
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# end
```

This example shows how to configure DHCPv6 with prefix delegation on the server side.

```
device(config)# interface GigabitEthernet1
device(config-if)# ipv6 address 2010:AB8:0:1::1/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 nd autoconfig default-route
device(config-if)# ipv6 nd managed-config-flag
device(config-if)# ipv6 nd ra interval 20
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool1 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:DB8:3000:3000::42
device(config-dhcpv6)# domain-name example.com
device(config-dhcpv6)# vendor-specific 100
device(config-dhcpv6)# suboption 1 address 2001:CC:1234:44::10
device(config-dhcpv6)# suboption 2 ascii "ip phone"
device(config)# ipv6 local pool dhcpv6-pool1 2001:DB8:1200::/40 48
```

Configure DHCPv6 with Relay

This example shows how to configure DHCPv6 with relay on the client side.

```
device(config)# interface GigabitEthernet3
device(config-if)# ipv6 address dhcp
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp client pd pr-from-pd
device(config-if)# ipv6 dhcp client request vendor
device(config-if)# no mop enabled
```

```
device(config-if)# no mop sysid
device(config-if)# end
```

This example shows the configurations on the client facing WAN edge device that acts as the relay agent.

```
device(config)# interface TenGigabitEthernet0/0/5
device(config-if)# vrf forwarding 10
device(config-if)# load-interval 30
device(config-if)# ipv6 address 2001:BB:1000::10/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp relay destination 2001:BB8:1200::2
device(config-if)# ipv6 dhcp relay option vpn
device(config-if)# end
```

This example shows the configurations on the server facing WAN edge device.

```
device(config)# interface GigabitEthernet0/0/3
device(config-if)# vrf forwarding 10
device(config-if)# no ip address
device(config-if)# negotiation auto
device(config-if)# ipv6 address 2001:BB8:1200::1/64
device(config-if)# ipv6 enable
device(config-if)# end
```

This example shows how to configure DHCPv6 with relay on the server side.

```
device(config)# interface GigabitEthernet2
device(config-if)# ipv6 address 2001:BB8:1200::2/64
device(config-if)# ipv6 enable
device(config-if)# ipv6 dhcp server dhcpv6
device(config-if)# end

device(config)# ipv6 dhcp pool dhcpv6
device(config-dhcpv6)# prefix-delegation pool dhcpv6-pool10 lifetime infinite infinite
device(config-dhcpv6)# address prefix 2001:BB:1000::/64 lifetime 200 200
device(config-dhcpv6)# dns-server 2001:BB:1200::42
device(config-dhcpv6)# domain-name relay.com
device(config)# ipv6 local pool dhcpv6-pool10 8001:ABCD::/40 48
```

Verify DHCPv6 Client and Server Configuration

Verify DHCPv6 Interface Information

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x00080001, T1 100, T2 160
        Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
                preferred lifetime 200, valid lifetime 200
                expires at Oct 26 2021 07:28 AM (170 seconds)
```

```
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00080001, T1 100, T2 160
        Prefix: 2001:DB8:1202::/48
                preferred lifetime 200, valid lifetime 200
                expires at Oct 26 2021 07:30 AM (194 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
  Prefix name: prefix_from_server
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

The following is a sample output from the **show ipv6 dhcp interface** command that provides details about SLAAC with DHCP.

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:59:49
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

View DHCPv6 Pool Information

The following is a sample output from the **show ipv6 dhcp pool** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in use,
0 conflicts)
```

```
              preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

The following is a sample output from the **show ipv6 dhcp pool** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in use,
0 conflicts)
              preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

View DHCPv6 Bindings

The following is a sample output from the **show ipv6 dhcp binding** command that provides details about DHCPv6 address allocation.

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  IA NA: IA ID 0x00080001, T1 10000, T2 16000
    Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
             preferred lifetime 20000, valid lifetime 20000
             expires at Oct 26 2021 01:17 PM (19925 seconds)
```

The following is a sample output from the **show ipv6 dhcp binding** command that provides details about DHCPv6 prefix delegation.

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  Interface : GigabitEthernet0/0/3
  IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:BB8:1602::/48
             preferred lifetime 200, valid lifetime 200
             expires at Oct 26 2021 08:01 AM (173 seconds)
```

View DHCPv6 Database

The following is a sample output from the **show ipv6 dhcp database** command.

```
Device# show ipv6 dhcp database
Database agent bootflash:
  write delay: 300 seconds, transfer timeout: 300 seconds
  last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2
  failed write times 0
```

View DHCPv6 Relay Bindings

The following is a sample output from the **show ipv6 dhcp relay bindings** command that provides details about DHCPv6 relay.

```
Device# show ipv6 dhcp relay binding

Relay Bindings associated with default vrf:

Relay Bindings associated with vrf 10:
Prefix: 2001:AA8:1100::/48 (GigabitEthernet3)
  DUID: 00030001001E49674C00
  IAID: 851969
  lifetime: INFINITE
  expiration: INFINITE
Summary:
  Total number of Relay bindings = 1
  Total number of IAPD bindings = 1
  Total number of IANA bindings = 0
  Total number of Relay bindings added by Bulk lease = 0
```

IPv6 as Preferred Address Family in a Dual Stack Environment

Table 3: Feature History

Feature Name	Release Information	Description
IPv6 as Preferred Address Family in a Dual Stack Environment	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco Catalyst SD-WAN Control Components Release 20.10.1	This feature allows you to select IPv6 as the preferred address family for control and data connections in a dual stack network environment. For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller, configure IPv6 as the preferred address family by using the feature template or the CLI template. For Cisco IOS XE Catalyst SD-WAN devices, configure IPv6 as the preferred address family using the Configuration Groups, Quick Connect or a CLI template.

Information About IPv6 as Preferred Address Family in a Dual Stack Environment

Cisco Catalyst SD-WAN provides you the option to select a preferred address family—IPv4 or IPv6—to establish control and data connections in a dual stack network environment. Use the **Dual Stack IPv6 Default** drop-down list in Cisco SD-WAN Manager to set IPv6 or IPv4.

On a Cisco IOS XE Catalyst SD-WAN device, when you choose the **True** option from the **Dual Stack IPv6 Default** drop-down list, the device establishes an IPv6 control connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose the **False** option from the **Dual Stack IPv6 Default** drop-down list, an IPv4 connection is established to connect to Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller.

Data connections or Bidirectional Forwarding Detection (BFD) sessions are established based on the IPv6 option set in local, remote Cisco IOS XE Catalyst SD-WAN devices. In a dual stack environment, when the **True** option is chosen in a local or remote Cisco IOS XE Catalyst SD-WAN device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

When you choose the **True** option from the **Dual Stack IPv6 Default** drop-down list in Cisco SD-WAN Manager or Cisco Catalyst SD-WAN Controller, IPv6 connections to other Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller instances are established. When you choose the **False** option from the **Dual Stack IPv6 Default** drop-down list, an IPv4 connection is established.

Note

- The connections from Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller and Cisco IOS XE Catalyst SD-WAN devices to the Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual stack network environment whether the **Dual Stack IPv6 Default** drop-down list options set to **True** or **False.**
- The **Dual Stack IPv6 Default** drop-down list options applies to Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller, and not to Cisco Catalyst SD-WAN Validator.
- An IPv6 connection can be configured on Cisco IOS XE Catalyst SD-WAN devices in sites that are behind NAT44 and NAT66.

Benefits of IPv6 as Preferred Address Family in a Dual Stack Environment

You have the option to migrate from IPv4 to IPv6, which allows you to have more IP addresses compared to IPv4. With IPv6, there can be no depletion of IP addresses.

Use Cases for IPv6 as Preferred Address Family in a Dual Stack Environment

From Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco Catalyst SD-WAN Control Components Release 20.10.1—to migrate from IPv4 to IPv6, you have the option to select a default connectivity option—IPv4 or IPv6—for control connections and data connections.

Configure IPv6 as Preferred Address Family in a Dual Stack Environment

Using Cisco SD-WAN Manager, you can configure Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager, and Cisco Catalyst SD-WAN Controller to set IPv6 as the default connectivity option for control and data connections.

Configure Cisco IOS-XE SD-WAN Devices for IPv6 Connectivity

You can use one of these options to configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices:

- CLI template and CLI add-on template
- Configuration groups
- Quick connect

CLI Template and CLI Add-On Template

Use the CLI template or the CLI add-on template to configure IPv6 for a Cisco IOS XE Catalyst SD-WAN device. The CLI configuration for Cisco IOS XE Catalyst SD-WAN devices is provided in Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template section. For more information about using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

Configuration Groups

To configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices using configuration groups, perform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Deploy**.
5. In the **Process Overview** window, click **Next**.
6. The **Selected Devices to Deploy** page displays the Cisco IOS XE Catalyst SD-WAN devices you selected previously. Check or uncheck one or more Cisco IOS XE Catalyst SD-WAN devices and then click **Next**.

7. From the **Dual Stack IPv6 Default** drop-down list, choose **True** to set IPv6 as a default connection, and click **Next**.

   The **True** option enables Cisco IOS XE Catalyst SD-WAN devices to establish an IPv6 connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose **False**, an IPv4 connection is established.

   BFD sessions are established based on the IPv6 option set in local, remote Cisco IOS XE Catalyst SD-WAN devices. In a dual stack environment, when the **True** option is chosen in a local or remote Cisco IOS XE Catalyst SD-WAN device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

Note The connections from the Cisco IOS XE Catalyst SD-WAN devices to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment whether the **Dual Stack IPv6 Default** drop-down list options set to **True** or **False.**

8. In the Summary window, click **Deploy**.

For more information on using configuration groups, see Configuration Groups and Feature Profiles.

Quick Connect

To configure an IPv6 connection on Cisco IOS XE Catalyst SD-WAN devices using the quick connect workflow, perform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Quick Connect**.
2. In the **Process Overview** window, click **Next**.
3. Choose an option to sync your devices, and then click **Next**

   For more information, see Quick Connect Workflow
4. In the **Selected devices to bring up** window, check one or more Cisco IOS XE Catalyst SD-WAN devices, and then click **Next**.
5. From the **Dual Stack IPv6 Default** drop-down list, choose **True** to set IPv6 as a default connection and click **Apply**, and then click **Next**.

   The **True** option enables Cisco IOS XE Catalyst SD-WAN devices to establish an IPv6 connection with Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller it is connected to. When you choose **False**, an IPv4 connection is established.

   BFD sessions are established based on the IPv6 option set in local, remote Cisco IOS XE Catalyst SD-WAN devices. In a dual stack environment, If you choose the **True** option in a local or remote Cisco IOS XE Catalyst SD-WAN device, the BFD session is an IPv6 connection. Otherwise, it is IPv4.

Note The connections from the Cisco IOS XE Catalyst SD-WAN devices to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment whether you choose the **True** or the **False** option.

6. In the Summary window, click **Deploy**.

Configure Cisco SD-WAN Manager and Cisco SD-WAN Controller for IPv6 Connectivity

You can use one of these options to configure an IPv6 connection on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller:

- CLI template and CLI add-on template
- Feature template

CLI Template

Use the CLI template to configure IPv6 in Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. The CLI configuration for Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller is provided in Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template. For more information about using CLI templates, see CLI Templates.

Feature Template

To configure an IPv6 connection in Cisco SD-WAN Manager using the feature template, peform this procedure:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and choose **Add Template**.
3. Choose a Cisco SD-WAN controller.
4. Under **BASIC INFORMATION**, click **System**.
5. In the **Template Name** field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
6. In the **Description** field, enter a description for the feature template. This field is mandatory, and it can contain all characters and spaces.
7. Under the **Basic Information** tab, click the **On** radio button adjacent to **Dual Stack IPv6 Default** field to set IPv6 as a default connection.

   The **On** option sets Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller to establish an IPv6 connection with all other Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller instances. When you click the **Off** radio button, an IPv4 connection is established.

Note The connections from Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller to Cisco Catalyst SD-WAN Validator is always dual (IPv4 and IPv6) in a dual IP stack environment irrespective of whether you click the **On** or **Off** radio button.

8. Click **Save**.

Configure IPv6 as Preferred Address Family in a Dual Stack Environment Using a CLI Template

Configure Cisco IOS-XE SD-WAN Devices for IPv6 in Dual IP Stack Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides sample CLI configurations of IPv6 as the preferred address family in Cisco IOS XE Catalyst SD-WAN devices:

1. Enable IPv6 on the tunnel interface:

   ```
   interface tunnel1
   no shutdown
   ipv6 enable
   ```

2. Enable IPv6:

   ```
   system
   ipv6-strict-control true
   ```

The following example shows how to configure IPv6 as the preferred address family in Cisco IOS XE Catalyst SD-WAN devices.

```
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 tunnel source GigabitEthernet1
 tunnel mode sdwan
 ipv6 enable
exit

system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 10.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "Cisco"
vbond vbond
```

Configure Cisco SD-WAN Manager and Cisco SD-WAN Controller for IPv6 in a Dual IP Stack Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

The following example shows how to configure IPv6 as the preferred address family in a Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager:

Enable IPv6:

```
system
ipv6-strict-control true
```

Here is the complete configuration example for configuring IPv6 as the preferred address family on a Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

```
system
host-name vm9
system-ip 10.16.255.19
site-id 400
ipv6-strict-control true
port-offset 9
no daemon-restart
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name "Cisco"
vbond vbond
```

Monitor IPv6 as Preferred Address Family in a Dual Stack Environment

After you successfully configure an IPv6 connection, the BFD connections will be up and running in Cisco SD-WAN Manager. To view the BFD connections in Cisco SD-WAN Manager:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**
2. Verify the status of the connection under the **BFD** column.

Monitor IPv6 as Preferred Address Family in a Dual Stack Environment Using the CLI

Use the following **show** commands to view control and data connection information for IPv4 and IPv6.

Cisco IOS XE Catalyst SD-WAN Devices

- **show sdwan control connections**
- **show sdwan control local-properties**
- **show sdwan bfd sessions**
- **show sdwan omp tlocs**

- **show sdwan bfd tloc-summary-list**

For more information on these **show** commands, see the chapter Troubleshooting Commands in the Cisco IOS XE SD-WAN Qualified Command Reference guide.

Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller

- **show control connections**
- **show control local-properties**

For more information on these **show** commands, see the chapter Operational Commands.

Troubleshooting

Problem

BFD sessions are down.

Possible Causes

Verify the IP address connections.

Solution

Verify the configuration for IPv4 or IPv6 in the Cisco IOS XE Catalyst SD-WAN devices and in Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller. For more information, see Troubleshoot Common BFD Errors.

Configuration Example for IPv6 as Preferred Address Family in a Dual Stack Environment

Configuration Example for IPv6 configured on a Cisco IOS-XE SD-WAN Device

This example shows how to configure IPv6 as the preferred address family on a Cisco IOS XE Catalyst SD-WAN device.

```
show sdwan running-config system
system
gps-location latitude 32.0
gps-location longitude -100.0
system-ip 10.16.255.14
domain-id 1
site-id 400
ipv6-strict-control true
admin-tech-on-failure
organization-name "Cisco"
vbond vbond
```

Configuration Example for IPv6 configured on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller

This example shows how to configure IPv6 as the preferred address family on Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller.

```
show running-config system
system
host-name vm9
system-ip 10.16.255.19
site-id 400
ipv6-strict-control true
port-offset 9
no daemon-restart
admin-tech-on-failure
no vrrp-advt-with-phymac
organization-name "Cisco"
vbond vbond
```