



CHAPTER 23

IPv6 and 6VPE Support in MPLS VPN

This chapter provides an overview of IPv6 and 6VPE support in MPLS VPN.



Note

For information on how MPLS VPN features are implemented and supported in the Prime Fulfillment GUI, see the appropriate sections of this guide, as indicated by the references provided.

Overview of IPv6 and 6VPE

The Prime Fulfillment MPLS VPN management application supports the configuration and management of Cisco devices running IOS and IOS XR for provisioning of IPv6 VPNs and 6VPEs for Prime Fulfillment Layer 3 VPN services.



Note

For the most current information about IOS and IOS XR versions and hardware platforms supporting IPv6, see [Release Notes for Cisco Prime Fulfillment 6.1](#).

This section provides an overview of IPv6 and 6VPE technologies. For an overview of how Prime Fulfillment supports IPv6, see [MPLS VPN Support for IPv6 and 6VPE, page 23-3](#).

Internet Protocol Version 6 (IPv6)

IPv6 is an IP protocol designed to replace IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, or approximately 3.4×10^{38} addressable nodes. This provides more than enough globally unique IP addresses for every network device on the planet. Cisco Systems has added IPv6 to its Cisco IOS and IOS XR Software. This means that current Cisco Systems-based networks are IPv6-capable, enabling coexistence and parallel operation between IPv4 and IPv6, thereby allowing network managers to configure IPv6 when it is required. While many see IPv6 as a way to build a larger global Internet, it does not eliminate the need to create VPNs for Intranets and other similar applications.

A variety of deployment strategies are available for deploying IPv6 over MPLS backbones. Currently, service providers have two approaches to support IPv6 without making any changes to the current IPv4 MPLS backbones:

- **6PE.** Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS. 6PE lets IPv6 domains communicate with each other over an IPv4 cloud without explicit tunnel setup, requiring only one IPv4 address per IPv6 domain. The 6PE technique allows service providers to provide global IPv6 reachability over IPv4 MPLS. It allows one shared routing table for all other devices.
- **6VPE.** Cisco IPv6 VPN Provider Edge Router (6VPE) over MPLS. This facilitates the RFC 2547bis-like VPN model for IPv6 networks. 6VPE is more like a regular IPv4 MPLS VPN provider edge, with the addition of IPv6 support within Virtual Routing and Forwarding (VRF). It provides logically separate routing table entries for VPN member devices.

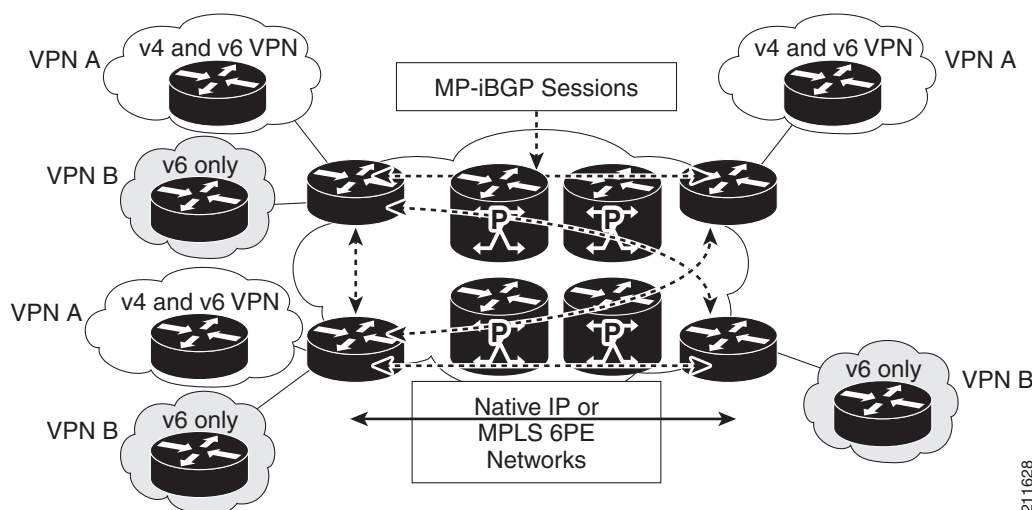
MPLS VPN in Prime Fulfillment uses 6VPE to manage Layer 3 VPN services for deployment of IPv6 over a MPLS backbone.

IPv6 VPN Provider Edge Router (6VPE)

Cisco Systems's 6VPE solution smoothly introduces IPv6 VPN service in a scalable way, without any IPv6 addressing restrictions. It does not jeopardize a well-controlled service provider IPv4 backbone or any customer networks. VPN service backbone stability is a key issue for those service providers who have recently stabilized their IPv4 infrastructure. For IPv4 VPN customers, IPv6 VPN service is exactly the same as MPLS VPN for IPv4.

The IPv6 MPLS VPN service model is similar to that of IPv4 MPLS VPNs. Service providers who have already deployed MPLS IPv4 VPN services over an IPv4 backbone can deploy IPv6 MPLS VPN services over the same IPv4 backbone by upgrading the PE router IOS version and dual-stack configuration, without any change on the core routers. IPv4 services can be provided in parallel with IPv6 services. A PE-CE link can be an IPv4 link, an IPv6 link, or a combination of an IPv4 and IPv6 link, as shown in Figure 23-1.

Figure 23-1 6VPE Deployment



IPv6 VPN service is exactly the same as MPLS VPN for IPv4. 6VPE offers the same architectural features as MPLS VPN for IPv4. It offers IPv6 VPN and uses the same components, such as:

- Multiprotocol BGP (MP-BGP) VPN address family
- Route distinguishers
- VPN Routing and Forwarding (VRF) instances

- Site of Origin (SOO)
- Extended community
- MP-BGP

The 6VPE router exchanges either IPv4 or IPv6 routing information through any of the supported routing protocols, and switches IPv4 and IPv6 traffic using the respective fast switching CEF or distributed CEF path over the native IPv4 and IPv6 VRF interfaces. The 6VPE router exchanges reachability information with the other 6VPE routers in the MPLS domain using Multiprotocol BGP, and shares a common IPv4 routing protocol (such as OSPF or IS-IS) with the other P and PE devices in the domain. Separate routing tables are maintained for the IPv4 and IPv6 stacks. A hierarchy of MPLS labels is imposed on an incoming customer IPv6 packet at the edge LSR:

- Outer label (IGP Label) for iBGP next-hop, distributed by LDP.
- Inner label (VPN Label) for the IPv6 prefix, distributed by MP-BGP.

Incoming customer IPv6 packets at the 6VPE VRF interface are transparently forwarded inside the service provider's IPv4 core, based on MPLS labels. This eliminates the need to tunnel IPv6 packets. P routers inside the MPLS core are unaware that they are switching IPv6 labelled packets.

MPLS VPN Support for IPv6 and 6VPE

This section summarizes how the MPLS VPN management application supports IPv6 and 6VPE.

See [Chapter 21, “Setting Up the Cisco Prime Fulfillment Services,”](#) for information setting up Prime Fulfillment services mentioned in this section. For additional information on setting up basic Prime Fulfillment services, see the *Setting Up Services* part.

IOS and IOS XR Support for IPv6

IPv6 services are available in Prime Fulfillment for supported versions of IOS and IOS XR and hardware platforms for both PE and CE roles.



Note

For the most current information about IOS and IOS XR versions and hardware platforms supporting IPv6, see [Release Notes for Cisco Prime Fulfillment 6.1](#).

The IPv6 features described in the following sections are supported for both IOS and IOS XR devices, unless otherwise noted.

Inventory and Device Management

To activate MPLS VPN services, you must configure Prime Fulfillment so it “knows” about the preconfiguration information, such as devices, providers, customers, and so on, that Prime Fulfillment is going to manage. Prime Fulfillment features that support inventory and device management for IPv6 and 6VPE include:

Discovery:

- Prime Fulfillment Inventory Manager supports bulk-import of 6VPE devices into the Prime Fulfillment repository.

Collect Config Task:

- The Collect Config task retrieves the OS type and the version information. If the device is a Cisco 12000 Series router, Cisco CRS-1 Carrier Routing System, or ASR 9000 Series router and is running IOS XR, the device will be marked as 6VPE supported. (By default, the “6VPE” check box in the Create PE Device window will be checked for XR devices). The “6VPE” check box in the Create PE Device window must be checked manually to designate an N-PE device as 6VPE for IOS devices.
- The Collect Config task for an IOS device with IPv6 services is the same as for IPv4 IOS devices.

Device Configuration:

- 6VPE devices with IPv6 addressing can be created and managed in the Prime Fulfillment GUI.
 - A “6VPE” check box in the Create PE Device window must be checked to designate an N-PE device as a 6VPE. IPv6 services for IOS and IOS XR devices are only available in MPLS and VRF service requests if this check box is checked.



Note

If the 6VPE check box is checked for a device in the Prime Fulfillment GUI and the device does not actually support IPv6 services, MPLS VPN service requests deployed on that device will result in a Failed Deploy state.

- A column in the Interface Attributes window shows IPv6 addresses. It is not possible to bulk change the IPv6 addresses by selecting multiple interfaces. The IPv6 Address column is noneditable.
- The Edit Device Interface window shows IPv6 addresses on interfaces. In case of dual-stack interfaces containing both IPv4 and IPv6 addresses, both addresses are displayed.
- Prime Fulfillment supports multiple IPv6 addresses on the PE interface for IOS XR PE and IOS 6VPE devices.
- The Create CPE Device window displays IPv6 addresses on interfaces. In case of dual-stack interfaces containing both IPv4 and IPv6 addresses, both addresses are displayed.
- You cannot create an IPv6 interface using the existing Create Interface feature. This screen currently lets you create interfaces in the repository only, with the device configuration remaining unchanged. This feature does not support IPv6 addresses. The IPv6 interface creation in the device is supported through the MPLS VPN service deployment.

VPN Creation and Configuration

There are no changes in the Prime Fulfillment VPN workflow for IPv6 and 6VPE.

Multicast VPN support for IPv6 is not available on IOS devices this release. Currently, it is only available for supported IOS XR devices. See the following sections for more information:

- [Multicast Routing on IOS and IOS XR Devices, page 23-7](#)
- [Multicast Support for IPv6 \(IOS XR Only\), page 23-8](#)

Independent VRF Object Support

Prime Fulfillment allows you to specify VPN and VRF information in an independent VRF object, which is subsequently deployed to a PE device and then associated with an MPLS VPN link via an MPLS VPN service request. Prime Fulfillment supports IPv4, IPv6, and dual-stack addressing in VRF objects.

For details on using creating and managing independent VRF objects, see [Chapter 22, “Independent VRF Management.”](#)

Resource Pools

Prime Fulfillment uses resource pools to automatically assign critical parameters like VLAN, VCID, and IP Addresses during the service provisioning. IPv6 address pools are not supported in this release.

MPLS VPN Service Provisioning

Prime Fulfillment MPLS VPN management application supports the provisioning of IPv6 Layer 3 VPNs on an IPv6 Provider Edge router (6VPE). Prime Fulfillment provides the ability to configure the following on the 6VPE:

- Use IPv6 addressing on 6VPE (optionally, IPv4, IPv6, or both IPv6+IPv4 addresses).
- Assign a static route to the 6VPE facing interface on a CE device.
- Enable MP-BGP peering with target 6VPE.
- Redistribute connected (if needed).

The following sections describe features of MPLS VPN policy definition, service request creation, and service request auditing to support IPv6 and 6VPE in Prime Fulfillment.

MPLS VPN Policies

Support for MPLS VPN policy definition for IPv6 and 6VPE includes:

- MPLS VPN service policy design supports the configuration of IPv6 on a 6VPE router for the following policy types:
 - Regular: PE-CE (with unmanaged CE)
 - Both Unmanaged CE and no-CE scenarios are supported for IPv6.
- Service policies support the following addressing schemes:
 - IPv4
 - IPv6
 - Dual-stacked (both IPv4 and IPv6)
- The IP Numbering Scheme field in the MPLS Policy Editor - IP Address Scheme window allows you to specify each of the supported address schemes.
- IPv4 routing and IPv6 routing are independent. The Prime Fulfillment GUI allows you to input the same or different routing protocols for IPv4 and IPv6.
- When setting up the policy, the following PE-CE routing protocols are supported for the IPv6 addressing scheme:
 - Static
 - BGP
 - EIGRP (only supported for IOS XR devices)
 - None
- IPv6 multicast VPNs are not supported for IOS 6VPE configurations. For information on support for multicast VPNs for IOS XR devices, see [Multicast Routing on IOS and IOS XR Devices](#), page 23-7.

- IPv6 validity checks. The following checks will be performed on addresses entered in the IPv6 address fields:
 - The address can be specified eight consecutive blocks of 16-bit each separated by the “:” (colon) character. Each 16-bit block can be specified as 4-digit hexadecimal number. Example: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A.
 - The leading zeros can be skipped in each hexadecimal block. Here is the modified valid address from the previous example: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A.
 - Where there are consecutive “0:” blocks, they can be replaced with “::”. Example: 21DA:D3:0:0:0:FF:FE28:9C5A can be represented as 21DA:D3::FF:FE28:9C5A.
 - The string “::” cannot appear more than once in the address. Example: 21DA:0000:0000:2F3B:0000:0000:0000:9C5A can be represented as 21DA::2F3B:0000:0000:0000:9C5A or 21DA:0000:0000:2F3B::9C5A, but not as 21DA::2F3B::9C5A.

See [Chapter 24, “MPLS VPN Service Policies”](#) for information on defining MPLS VPN service policies.

MPLS VPN Service Requests

Attributes set during MPLS VPN policy creation to support IPv6 and 6VPE are carried over to the corresponding windows in the service request creation workflow. If the options were set as editable during policy creation, they can be modified when the service request is created.

- The IP Numbering Scheme field in the MPLS Link Attribute Editor - IP Address Scheme window allows you to specify each of the supported address schemes.
- The IPv4 and IPv6 Unnumbered schemes are not supported on IOS XR devices. When you select an IOS XR (or IOS 6VPE) device and go to the IP Addressing Scheme window, only the following options are displayed:
 - IPv4 Numbered
 - IPV6 Numbered
 - IPV4+IPV6 Numbered
- As part of the regular PE-CE MPLS service, the required VRF will be configured on the PE device. The CE-facing interface will be configured with the IPv6 address and the interface will be assigned to the VRF. The IPv6 address-family configuration in BGP along with the PE-CE routing information will be configured.
- If the PE Interface is dual-stacked (contains both IPv4 and IPv6 addresses), you can enter the routing information for both IPv4 and IPv6 independently. The GUI provides steps to enter the IPv6 routing information in addition to the existing IPv4 routing information.
- Prime Fulfillment supports the scenario of the CE device not present in the service request. This release also supports the Unmanaged CE devices being present in the service request. In the later case, the configlets for service provisioning will be generated but not rolled onto the CE device.
- It is possible to modify a 6VPE service request.
- If the PE device is an IOS XR device, all of the configuration operations will be performed using the IOS XR interface.
- For IOS XR 6VPE devices, all configlets generated are in XML format. Different versions of IOS XR will generate different XML configlets. However, the configurations will be almost identical, except for changes in the XML schema.
- For IOS 6VPE devices, all configurations are generated in CLI format.

See [Chapter 25, “MPLS VPN Service Requests,”](#) and subsequent chapters in this guide for information on creating MPLS VPN service requests.

MPLS Service Request Audits

L3 VPN functional audit supports IPv6 VPNs (IPv6 addresses and 6VPE devices). This includes checking the routes to remote CEs in the VRF route tables on the PE devices. See [Chapter 47, “Viewing Audit Reports Service Requests,”](#) for information on auditing service requests.

Multicast Routing on IOS and IOS XR Devices

Multicast VRF deployments for IOS XR devices are supported for IPv4, IPv6, IPv4+IPv6 services. Currently, multicast on IOS XR is supported only for specified versions of IOS XR versions. For a list of supported IOS XR versions in this release, see [Release Notes for Cisco Prime Fulfillment 6.1](#).

This section describes how Prime Fulfillment supports multicast routing on IOS XR devices. There are no changes in the GUI (Create VPN window) to support this feature. The IOS XR XML does not support multicast routing command, so the corresponding IOS XR CLI is used to push the configuration to the device.

The following sections shows an example of the relevant IOS commands and the corresponding IOS XR commands to enable multicast routing.

IOS Commands

The following is a sample IOS configuration:

```
ip vrf V27:MulticastCERC3
rd 100:124
address-family ipv4
route-target import 100:406
route-target import 100:407
route-target export 100:406
mdt default 226.2.3.4
mdt data 226.5.6.7 0.0.0.15 2000
mdt mtu 2000
ip multicast-routing vrf V27:MulticastCERC3
ip pim vrf V28:VPN13 ssm default
ip pim vrf V27:MulticastCERC3 rp-address 10.20.1.1
ip pim vrf V27:MulticastCERC3 rp-address 10.20.3.1 test2
ip pim vrf V27:MulticastCERC3 rp-address 10.20.2.1 test1 override
```

IOS XR Commands

The following IOS commands are not supported on the IOS XR devices, because the corresponding commands do not exist in IOS XR.

- **ip multicast vrf <vrfName> route-limit.** The reason for not supporting this is that the command to set the route limit per VRF is not available on IOS XR devices.
- **ip pim vrf <vrfName> sparse-dense-mode.** Sparse-dense mode is not supported by IOS XR. Only sparse mode and bidirectional modes are supported.

The following IOS commands are enabled on the IOS XR device by default when the multicast routing is enabled. They cannot be disabled.

- **ip pim vrf <vrfName> sparse-mode**
- **ip pim vrf <vrfName> ssm default**

- `ip pim vrf <vrfName> autorp listener`

Multicast Support for IPv6 (IOS XR Only)

Multicast on IPv6 is only supported on IOS XR devices. Specifically, in this release this feature is only supported on Cisco 12000 series routers. Prime Fulfillment allows the following on supported PE devices and versions of IOS XR:

- A multicast VPN to be deployed on an IPv6 PE-CE link.
- Multicast to be enabled during the creation of the VRF object.

When creating a VPN or a VRF object, you can enable multicast for IPv4, IPv6, or both. You can enter IPv6 addresses as static Rendezvous Point (RP) addresses if IPv6 multicast is enabled during the creation of a VPN or VRF object.

You can also modify an existing VPN or VRF object to enable multicast for IPv4, IPv6, or both. When IPv4 multicast is enabled, all deployed service requests containing IPv4 links of the same VPN or VRF are moved into Requested state.

In addition, you can specify within the MPLS service request whether you want to enable multicast for IPv4, IPv6, or both on a given MPLS link.

When IPv6 multicast is enabled, all deployed service requests containing IPv6 links of the same VPN or VRF are moved into Requested state. If IPv4 is previously configured and only IPv6 multicast is enabled in a VPN, only the service requests with IPv6 links are moved into Requested state.

You can modify an existing VPN or VRF object and add IPv6 static RP addresses when IPv6 multicast is enabled. Any service requests already in Deployed state are then moved to the Requested state.

You can create a service policy or an MPLS VPN link in the service request with IPv6 Numbered or IPv4+IPv6 Numbered as the IP addressing scheme and a multicast VPN or a VRF with multicast enabled.

DCPL Properties Updated for IOS 6VPE Support

Two DCPL properties have been updated to support certain IOS commands that require a delay after being downloaded to a device. This may cause a delay when deploying MPLS VPN service requests on IOS devices containing IPv6 configuration commands.

- The DCPL property `GTL/CSL/ios/delayAfterDownloadingCmd` has been added to Prime Fulfillment to support IOS commands that require a delay after they are downloaded via a terminal session protocol such as Telnet. The List element format is:

```
cmd_regex:delay_in_seconds; no vrf definition *:105
```

After the “no vrf definition” command is pushed to the device, there is a delay of 105 seconds before it takes effect on the device.

- The DCPL property `GTL/CSL/ios/delayBeforeDownloadingCmd` has been added to Prime Fulfillment to support certain IOS commands that require a delay before they are downloaded via a terminal session protocol such as Telnet. The List element format is:

```
cmd_regex:delay_in_seconds;
vrf definition *:70;
```

After the “vrf definition” command is pushed to the device, there is a delay of 70 seconds before it takes effect on the device.

MPLS Reports

MPLS VPN reports support IPv6 addresses and 6VPE devices. See [Chapter 55, “Generating MPLS Reports”](#) for information on generating MPLS VPN reports for IPv6 and 6VPE.

Upgrading an Existing IPV4 VRF to Be a Dual-Stack (IPV4+IPV6) VRF

This section describes VRF upgrading on IOS 6VPE devices using MPLS service requests. Key points to keep in mind are as follows:

- This feature is only supported for IOS 12.2(33) SRE2 version and above.
- Any IPv4 deployment on a VRF always generates the command “ip vrf vrf-name” on the device. When it is upgraded to dual stack (IPv4+IPv6) or IPv6, then:
 - Any links sharing the same VRF on the same device are upgraded to “vrf definition vrf-name” in the device.
 - All the related service requests sharing the same VRF on the same device are moved to the Requested state.
 - All service requests have to be redeployed for an audit pass.
- The VRF upgrade scenarios from Prime Fulfillment work for IOS 6VPE devices only if the “vrf upgrade-cli multi-af-mode non-common-policies vrf vrf-name force” command is supported in the device. If not the service request results in FAILED-DEPLOYED state. This command is available in IOS version 12.2 (33) SRE2.
- Most upgrade scenarios will likely involve starting with existing IPv4 service requests, rather than starting from scratch with IOS-based IPv6. The scenarios below cover various upgrade scenarios for the typical cases.

The following are typical VRF modification scenarios:

- IPv4 to Dual-Stack (IPv4+IPv6). Configlets are generated for the IPv6 link. The command “ip vrf vrf-name ” is upgraded to “vrf definition vrf-name” by using the command “vrf upgrade-cli multi-af-mode non-common-policies vrf vrf-name force”.
- IPv4 to IPv4. There is no change in the configlets.
- IPv4 to IPv6. “No” commands (“no ip vrf vrf-name”) are generated on the IPv4 link, and new configlets (“vrf definition vrf-name”) get deployed on the IPv6 link.
- IPv6 to IPv4. “No” commands (“no vrf definition vrf-name”) are generated on the IPv6 link, and new configlets (“ip vrf vrf-name”) are issued for the IPv4 link.
- Rehoming (that is, moving from one PE to another) issues “no” commands on the old device and new commands on the rehomed PE.

An example VRF modification scenario is provided below for reference.

An IPv4 link has VRF configured as:

```
ip vrf V8:stellavpn8
rd 64512:1572
route-target export 64512:15870
route-target import 64512:15870
route-target import 64512:15871
!
```

An IPv6 link has VRF configured as:

```
vrf definition V4:stellavpn4
```

```

rd 64512:1568
!
address-family ipv6
route-target export 64512:15862
route-target import 64512:15862
exit-address-family
!

```

An IPv4+IPv6 link (which has been upgraded from IPv4 to dual-stack) has VRF configured as:

```

vrf upgrade-cli multi-af-mode non-common-policies vrf V9:stellavpn9 force !
vrf definition V9:stellavpn9
rd 64512:1573
!
address-family ipv4
route-target export 64512:15872
route-target import 64512:15872
route-target import 64512:15873
exit-address-family
!
address-family ipv6
route-target export 64512:15872
route-target import 64512:15872
route-target import 64512:15873
exit-address-family

```

Unsupported IPv6 and 6VPE Features

The following features are **not** supported for IPv6 and 6VPE:

- Discovery of existing IPv6 VPN services on the device.
- IPv6 addressing as part of a CPE device definition and configuration.
- IPv6 address pools.
- IPv6 multicast address pools.
- The IPv4 and IPv6 Unnumbered address schemes are not supported for 6VPE and IOS XR.
- Grey management VPN support for 6VPE and IOS XR.
- Staging service request deployment to support eBGP route maps on IOS XR devices.
- Managed CE services (if the device does not support IPv6 services).
- Multi-VRF CE (MVRFCCE) support.
- One-time setup operations on the 6VPE device like enabling IPv6 routing, BGP VPNv6 configuration.
- Tunnel interface. An IPv6 address cannot be specified as the Tunnel Source Address value.