



Route Leaking Between VPNs



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.

Table 1: Feature History

Feature Name	Release Information	Description
Route Leaking Between Global VRF and Service VPNs	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables you to leak routes bidirectionally between the global VRF and service VPNs. Route leaking allows service sharing and is beneficial in migration use cases because it allows bypassing hubs and provides migrated branches direct access to nonmigrated branches.
Redistribution of Replicated BGP Routes to OSPF, EIGRP Protocols	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows you to leak (or replicate) BGP routes between the global VRF and service VPNs, and redistribute the leaked BGP routes. The redistribution of the leaked routes to the EIGRP and OSPF protocols occurs after replicating the BGP routes into the corresponding VRF.

Feature Name	Release Information	Description
Redistribution of Replicated Routes to BGP, OSPF, and EIGRP Protocols	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to configure the following: - Redistribution of leaked or replicated routes between the global VRF and service VPNs for BGP, OSPF, and EIGRP protocols on Cisco IOS XE Catalyst SD-WAN devices - OMP administrative distance option to prefer OMP routes over MPLS routes - VRRP tracking to track whether a leaked route is reachable.
Route Leaking between Inter-Service VPN	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	With this feature, you can leak routes between the service VPNs at the same edge device. Route leaking feature allows redistribution of replicated routes between the inter-service VPN for Connected, Static, BGP, OSPF, and EIGRP on Cisco IOS XE Catalyst SD-WAN devices.

- [Supported Protocols, on page 2](#)
- [Restrictions for Route Leaking and Redistribution, on page 3](#)
- [Information About Route Leaking , on page 4](#)
- [Workflow to Configure Route Leaking Using Cisco SD-WAN Manager, on page 6](#)
- [Configure and Verify Route Leaking Using the CLI, on page 11](#)
- [Configure Route Redistribution Between Global VRF and Service VPNs Using the CLI, on page 17](#)
- [Verify Route Redistribution, on page 20](#)
- [Configure Route Leaking Between Service VPNs Using a CLI Template, on page 21](#)
- [Verify Route-Leaking Configurations Between Service VPNs Using the CLI, on page 22](#)
- [Configure VRRP Tracker for Tracking Leaked Service VPNs Using the CLI, on page 23](#)
- [Verify VRRP Tracking, on page 25](#)
- [Configuration Example for Route Leaking, on page 26](#)

Supported Protocols

The following protocols are supported for route leaking between the global VRF and service VPNs.

- Connected
- Static
- BGP
- OSPF
- EIGRP

The following protocols are the supported destination and source protocols for route redistribution between the service VPNs and global VRF.

Source Protocols

- Connected
- Static
- BGP
- OSPF
- EIGRP

Destination Protocols

- BGP
- OSPF
- EIGRP

**Note**

The EIGRP protocol can be used only on service VPNs and not on the global VRF. Therefore, route leaking is supported only for routes from service VPNs to the global VRF.

Restrictions for Route Leaking and Redistribution

- The EIGRP protocol can be used only on service VRFs and not on the global VRF. Therefore, route leaking isn't supported for routes from the global VRF to the service VRFs, and between service VRFs for the EIGRP protocol.
- Service-side NAT isn't supported with route leaking between the global VRF and service VRFs.
- NAT isn't supported with transport VRF route leaking.
- IPv6 address family is not supported.
- Each service VRF can leak (import and export) a maximum of 1000 routes.
- Only prefix-lists, tags, and metrics can be matched in route maps that are used to filter leaked routes.
- Inter-service VRF route leaking on Cisco IOS XE Catalyst SD-WAN devices with multitenancy is not supported.
- Overlay Management Protocol (OMP) routes do not participate in VRF route leaking to prevent overlay looping.
- Route leaking across different devices or sites using export policies in Cisco SD-WAN is not supported.
- Redistribution in EIGRP requires bandwidth, load, reliability, delay, and MTU settings to select the best path.
- Route replicate with **all** keyword is not recommended.
- Route leaking using centralized policy is not supported.

- While configuring route leaking for a VRF, the **route-replicate** command under the **global-address-family ipv4** command shouldn't have the keyword **all** specified as the protocol for the unicast option to prevent route looping.

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast all
```

- In this example, the keyword **all** should be replaced with specific protocol name as shown here:

```
global-address-family ipv4
  route-replicate from vrf <vrf> unicast connected
```

Information About Route Leaking

Route Leaking Between Global VRF and Service VPNs

The Cisco Catalyst SD-WAN solution lets you segment the network using VPNs. Route leaking between the global or default VRF (transport VPN) and service VPNs allows you to share common services that multiple VPNs need to access. With this feature, routes are replicated through bidirectional route leaking between the global VRF (also known as transport VPN) and service VPNs. Route leaking between VRFs is done using Routing Information Base (RIB).



Note In the context of Cisco Catalyst SD-WAN, the terms VRF and VPN are used interchangeably. Although Cisco IOS XE Catalyst SD-WAN devices use VRFs for segmentation and network isolation, the VPN feature template is used to configure them using Cisco SD-WAN Manager. When you use Cisco SD-WAN Manager to configure VPNs for Cisco IOS XE Catalyst SD-WAN devices, Cisco SD-WAN Manager automatically converts the VPN configuration to VRF configuration.

To leak routes to the routing neighbors, redistribute the leaked routes between the global VRF and service VPNs.

OMP Administrative Distance for Leaked Routes

You can configure the Cisco SD-WAN Overlay Management Protocol (OMP) administrative distance to a lower value that sets the OMP routes as the preferred and primary route over any leaked routes in a branch-to-branch routing scenario.

Ensure that you configure the OMP administrative distance on Cisco IOS XE Catalyst SD-WAN devices based on the following points:

- If you configure the OMP administrative distance at both the global VRF and service VRF level, the VRF-level configuration overrides the global VRF-level configuration.
- If you configure the service VRF with a lower administrative distance than the global VRF, then except the service VRF, all the remaining VRFs take the value of the administrative distance from the global VRF.

To configure the OMP administrative distance using Cisco SD-WAN Manager, see [Configure Basic VPN Parameters](#) and [Configure OMP Using SD-WAN Manager Templates](#).

To configure the OMP administrative distance using the CLI, see the [Configure OMP Administrative Distance](#) section in [Configure OMP Using the CLI](#).

Inter-Service VRF Route Leaking

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1.

The Inter-Service VRF Route Leaking feature provides the ability to leak selective routes between service VRFs back to the originating device on the same site.

To resolve routing-scalability challenges introduced when you use Cisco SD-WAN Controllers, you can leak routes between the VRFs at the edge device.

To configure the inter-service VRF route leaking feature using Cisco SD-WAN Manager, see [Configure Route Leaking Between Service VRFs](#).

To configure the inter-service VRFs route leaking feature using the CLI, see [Configure Route Leaking Between Service VRFs Using the CLI](#).

Use VRRP Tracker for Leaked Service VPNs

The Virtual Router Redundancy Protocol (VRRP) can track whether a leaked route is reachable. If tracked route is not reachable, VRRP changes the priority of the VRRP group. It can trigger a new primary router election. The VRRP tracker determines whether a route is reachable based on the existence of the route in the routing table of the routing instance that is included in the VRRP configuration.

To configure the VRRP tracker to track a leaked service VPNs using Cisco SD-WAN Manager, see [Configure VRRP for Cisco VPN Interface Ethernet template](#).

To configure the VRRP tracker to track any leaked service VPNs using the CLI, see [Configure VRRP Tracker for Tracking Leaked Service VPNs Using the CLI](#).

Features of Route Leaking

- Routes between the global VRF and service VPNs can be leaked directly.
- Multiple service VPNs can be leaked to the global VRF.
- Multiple service VRFs leaking into the same service VRF is supported.
- When routes are leaked or replicated between the global VRF and service VPNs, route properties such a metric, source VPN information, tags, administrative distance, and route origin are retained.
- You can control leaked routes using route maps.
- Route-maps can filter routes using match operations before leaking them.
- The feature can be configured using both—Cisco SD-WAN Manager and CLI.

Use Cases for Route Leaking

- **Service Provider Central Services:** SP Central services under MPLS can be directly accessed without having to duplicate them for each VPN. This makes accessing central services easier and more efficient.
- **Migration:** With route leaking, branches that have migrated to Cisco SD-WAN can directly access non-migrated branches bypassing the hub, thus providing improved application SLAs.

- **Centralized Network Management:** You can manage the control plane and service-side equipment through the underlay.
- **Retailer Requirements for PCI compliance:** Route leaking for service VRFs is used where the VRF traffic goes through a zone-based firewall on the same branch router while being PCI compliant.

How Route Preference is Determined

If a route is replicated or leaked between the global VRF and service VPNs, the following rule determines the route preference.

For a device that receives route from two sources where both these routes use the same source VRFs and one of the routes is replicated, the non-replicated route is preferred.

If the mentioned rule doesn't apply, the following rules determine the route preference in this sequence:

1. Prefer the route with smaller administrative distance.
2. Prefer the route with smaller default administrative distance.
3. Prefer a non-replicated route over a replicated route.
4. Compare original VRF-names. Prefer the route with the lexicographically smaller VRF-name.
5. Compare original subaddress families. Prefer unicast routing over multicast routing.
6. Prefer the oldest route.

Workflow to Configure Route Leaking Using Cisco SD-WAN Manager

1. Configure and enable the Localized Policy and attach the Route Policy.
2. Configure and enable the Route Leaking feature between Global and Service VPN.
3. Configure and enable the Route Leaking feature between Service VPNs.
4. Attach the Service Side VPN Feature Template to the Device Template.

Configure Localized Route Policy

Configure Route Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Policies**.
2. Select **Localized Policy**.
3. From the **Custom Options** drop-down, under Localized Policy, select **Route Policy**.
4. Click **Add Route Policy**, and select **Create New**.
5. Enter a name and description for the route policy.

6. In the left pane, click **Add Sequence Type**.
7. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. Match is selected by default.
8. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.
9. Click a match condition.
10. On the left, enter the values for the match condition.
11. On the right enter the action or actions to take if the policy matches.
12. Click **Save Match and Actions** to save a sequence rule.
13. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
 - a. Click **Default Action** in the left pane.
 - b. Click the **Pencil** icon.
 - c. Change the default action to **Accept**.
 - d. Click **Save Match and Actions**.
14. Click **Save Route Policy**.

Add the Route Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Policies**.
2. Choose the **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next** in the Local Policy Wizard until you arrive at the **Configure Route Policy** option.
5. Click **Add Route Policy** and choose **Import Existing**.
6. From the **Policy** drop-down choose the route policy that is created. Click **Import**.
7. Click **Next**.
8. Enter the **Policy Name** and **Description**.
9. Click **Preview** to view the policy configurations in CLI format.
10. Click **Save Policy**.

Attach the Localized Policy to the Device Template



Note The first step in utilizing the Localized Policy that was created previously is to attach it to the device template.

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

2. Click **Device Templates** and select the desired template.
3. Click ..., and click **Edit**.
4. Click **Additional Templates**.
5. From the **Policy** drop-down, choose the **Localized Policy** that is created.
6. Click **Update**.



Note Once the localized policy has been added to the device template, selecting the **Update** option immediately pushes a configuration change to all of the devices that are attached to this device template. If more than one device is attached to the device template, you will receive a warning that they are changing multiple devices.

7. Click **Next** and then **Configure Devices**.
8. Wait for the validation process and push configuration from Cisco SD-WAN Manager to the device.

Configure and Enable Route Leaking between Global and Service VPNs

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. To configure route leaking, click **Feature Templates**.



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

Do one of the following:

- To create a feature template:
 - a. Click **Add Template**. Choose a device from the list of devices. The templates available for the selected device display in the right pane.
 - b. Choose the **Cisco VPN** template from the right pane.



Note Route leaking can be configured on service VPNs only. Therefore, ensure that the number you enter in the **VPN** field under **Basic Configuration** is one of the following: 1—511 or 513—65527.

For details on configuring various VPN parameters such as basic configuration, DNS, Virtual Router Redundancy Protocol (VRRP) tracking, and so on, see [Configure a VPN Template](#). For details specific to the route leaking feature, proceed to Step c.

- c. Enter Template Name and Description for the feature template.
- d. Click **Global Route Leak** below the **Description** field.
- e. To leak routes from the global VRF, click **Add New Route Leak from Global VPN to Service VPN**.

1. In the **Route Protocol Leak from Global to Service** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
 2. In the **Route Policy Leak from Global to Service** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.
 3. For the **Redistribute to protocol (in Service VPN)** field, click **Add Protocol**.
In the **Protocol** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
In the **Redistribution Policy** drop-down list, choose **Global**. Next, choose one of the available redistribution policies from the drop-down list.
 4. Click **Add**.
- f. To leak routes from the service VPNs to the global VRF, click **Add New Route Leak from Service VPN to Global VPN**.
1. In the **Route Protocol Leak from Service to Global** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
 2. In the **Route Policy Leak from Service to Global** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.
 3. For the **Redistribute to protocol (in Global VPN)** field, click **Add Protocol**.
In the **Protocol** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.
In the **Redistribution Policy** drop-down list, choose **Global**. Next, choose one of the available redistribution policies from the drop-down list.
 4. Click **Add**.
- g. Click **Save/Update**. The configuration does not take effect till the feature template is attached to the device template.
- h. To redistribute the leaked routes using Cisco SD-WAN Manager, use [CLI Add-on Feature templates](#) to enter the configuration applicable to your environment. Here's an example.

```
Device(config)# router ospf 65535
Device(config-router)# redistribute vrf 1 ospf 103
```

```
Device(config)# router eigrp vpn
Device(config-router)# address-family ipv4 vrf 1 autonomous-system 50
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global ospf 65535
metric 1 2 3 4 5
```

After you create the CLI add-on template, you need to attach it to the protocol template to which you are redistributing routes. In this example, you would attach it to the EIGRP template.

- To modify an existing feature template:
 - a. Choose a feature template you wish to modify.

- b. Click ... next to the row in the table, and click **Edit**.
- c. Click **Global Route Leak**.
- d. To edit information, from the table under **Add New Route Leak from Global VPN to Service VPN** or **Add New Route Leak from Service VPN to Global VPN**, click **Edit**.
The update route leak dialog box appears.
- e. Perform all operations from Step d of creating a feature template.
Perform all operations from Step c of creating a feature template.
- f. Click **Save Changes**.
- g. Click **Update**.

**Note**

- The configuration does not take effect till the Service VPN feature template is attached to the device template.

Configure Route Leaking Between Service VPNs

Minimum supported release: Cisco vManage Release 20.9.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Feature Templates**.
3. Navigate to the **Cisco VPN** template for the device.

**Note**

To create a **VPN** template, see [Create VPN Template](#)

4. Click **Route Leak**.
5. Click **Route Leak between Service VPN**.
6. Click **Add New Inter Service VPN Route Leak**.
7. From the **Source VPN** drop-down list, choose **Global** to configure the service VPN from where you want to leak the routes. Otherwise, choose **Device-Specific** to use a device-specific value.
You can configure service VPNs within the range VPNs 1 to 511, and 513 to 65530, for service-side data traffic on Cisco IOS XE Catalyst SD-WAN devices. (VPN 512 is reserved for network management traffic. VPN 0 is reserved for control traffic using the configured WAN transport interfaces.)
8. From the **Route Protocol Leak to Current VPN** drop-down list, choose **Global** to select a route protocol to enable route leaking to the current VPN. Otherwise, choose **Device-Specific** to use a device-specific value.

You can choose **Connected**, **Static**, **OSPF**, **BGP**, and **EIGRP** protocols for route leaking.

9. From the **Route Policy Leak to Current VPN** drop-down list, choose **Global** to select a route policy to enable route leaking to the current VPN. Otherwise, choose **Device-Specific** to use a device-specific value.

This field is disabled if no route policies are available.

10. To configure **Redistribute to protocol (in Service VPN)**, click **Add Protocol**.

From the **Protocol** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.

You can choose **Connected**, **Static**, **OSPF**, **BGP**, and **EIGRP** protocols for redistribution.

(Optional) From the **Redistribution Policy** drop-down list, choose **Global**. Next, choose one of the available redistribution policies from the drop-down list.

This field is disabled if no route policies are available.

11. Click **Add**.

12. Click **Save**.

Attach the Service Side VPN Feature Template to the Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Device Templates** and select the desired template.
3. Click **...**, and click **Edit**.
4. Click **Service VPN**.
5. Click **Add VPN**. Select the Service VPN feature template listed in the Available VPN Templates pane. Click right-shift arrow and add the template to Selected VPN Templates list.
6. Click **Next** once it moves from the left (Available VPN Templates) to the right side (Selected VPN Templates).
7. Click **Add**.
8. Click **Update**.
9. Click **Next** and then **Configure Devices**.
10. Finally, wait for the validation process and push configuration from Cisco SD-WAN Manager to the device.

Configure and Verify Route Leaking Using the CLI

Example: Leak Routes between Global VRF and Service VPNs

These examples show how to configure route leaking between a global VRF and a service VPN. In this example, VRF 103 is the service VPN. This example shows that connected routes are leaked into VRF 103 from the global VRF, similarly, the same connected routes are leaked from VRF 103 to the global VRF.

```
vrf definition 103
!
  address-family ipv4
    route-replicate from vrf global unicast connected
!
global-address-family ipv4
  route-replicate from vrf 103 unicast connected
exit-address-family
```

Verify Configuration



Note In the output, leaked routes are represented by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O 10.1.14.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.15.0/24 is directly connected, GigabitEthernet1
L 10.1.15.15/32 is directly connected, GigabitEthernet1
O 10.1.16.0/24 [110/11] via 10.1.15.13, 00:02:22, GigabitEthernet1
C 10.1.17.0/24 is directly connected, GigabitEthernet2
L 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
[170/10880] via 192.168.24.17(103), 01:04:13, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C + 192.0.2.0/24 is directly connected, GigabitEthernet5.103
L & 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 203.0.113.0/24 is directly connected, GigabitEthernet6
L 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 198.51.100.0/24 is directly connected, GigabitEthernet7
L 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
O E2 100.100.100.100 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
172.16.0.0/32 is subnetted, 1 subnets
O E2 172.16.255.14 [110/20] via 10.1.15.13, 00:02:22, GigabitEthernet1
```

View Routes Leaked From Global VRF to Service VRF Table

Use the **show ip route vrf <vrf id>** command to view the routes leaked from the global VRF to the service VRF table.



Note In the output, leaked routes are denoted by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route vrf 103
Routing Table: 103
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C + 10.0.1.0/24 is directly connected, GigabitEthernet9
L & 10.0.1.15/32 is directly connected, GigabitEthernet9
C + 10.0.20.0/24 is directly connected, GigabitEthernet4
L & 10.0.20.15/32 is directly connected, GigabitEthernet4
C + 10.0.100.0/24 is directly connected, GigabitEthernet8
L & 10.0.100.15/32 is directly connected, GigabitEthernet8
C + 10.1.15.0/24 is directly connected, GigabitEthernet1
L & 10.1.15.15/32 is directly connected, GigabitEthernet1
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
172.16.0.0/12 is subnetted, 1 subnets
D EX 172.16.20.20
[170/10880] via 192.168.24.17, 01:04:07, GigabitEthernet5.103
192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.0/24 is directly connected, GigabitEthernet5.103
L 192.168.24.15/16 is directly connected, GigabitEthernet5.103
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 203.0.113.0/24 is directly connected, GigabitEthernet6
L & 203.0.113.15/32 is directly connected, GigabitEthernet6
10.20.0.0/8 is variably subnetted, 2 subnets, 2 masks
C + 198.51.100.0/24 is directly connected, GigabitEthernet7
L & 198.51.100.15/24 is directly connected, GigabitEthernet7
192.0.2.0/32 is subnetted, 1 subnets
```

Example: Filter Routes Before Leaking

To further filter the routes leaked between the global VRF and the service VRF, you can apply a route map as shown in this example.

```
vrf definition 103
!
 address-family ipv4
   route-replicate from vrf global unicast connected route-map myRouteMap permit 10
   match ip address prefix-list pList seq 5 permit 10.1.17.0/24
!
```

Verify Configuration



Note In this output, leaked routes are denoted by a + sign next to the route leaked. Example: C+ denotes that a connected route was leaked.

```
Device#show ip route vrf 103
```

```
Routing Table: 1
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
```

```
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
H - NHRP, G - NHRP registered, g - NHRP registration summary
```

```
o - ODR, P - periodic downloaded static route, l - LISP
```

```
a - application route
```

```
+ - replicated route, % - next hop override, p - overrides from PfR
```

```
& - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
```

```
C + 10.1.17.0/24 is directly connected, GigabitEthernet2
```

```
L & 10.1.17.15/32 is directly connected, GigabitEthernet2
```

```
m 10.1.18.0/24 [251/0] via 172.16.255.14, 19:01:28, Sdwan-system-intf
```

```
m 10.2.2.0/24 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
```

```
m 10.2.3.0/24 [251/0] via 172.16.255.11, 17:26:50, Sdwan-system-intf
```

```
C 10.20.24.0/24 is directly connected, GigabitEthernet5
```

```
L 10.20.24.15/32 is directly connected, GigabitEthernet5
```

```
m 10.20.25.0/24 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
```

```
172.16.0.0/32 is subnetted, 3 subnets
```

```
m 172.16.255.112 [251/0] via 172.16.255.11, 17:28:44, Sdwan-system-intf
```

```
O E2 172.16.255.117 [110/20] via 10.20.24.17, 1d11h, GigabitEthernet5
```

```
m 172.16.255.118 [251/0] via 172.16.255.11, 16:14:18, Sdwan-system-intf
```

To monitor leaked routes, use the **show ip cef** command. The output shows replicated or leaked routes.

```
Device#show ip cef 10.1.17.0 internal
```

```
10.1.17.0/24, epoch 2, flags [rcv], refcnt 6, per-destination sharing
```

```
[connected cover 10.1.17.0/24 replicated from 1]
```

```
sources: I/F
```

```
feature space:
```

```
Broker: linked, distributed at 4th priority
```

```
subblocks:
```

```
gsb Connected receive chain(0): 0x7F6B4315DB80
```

```
Interface source: GigabitEthernet5 flags: none flags3: none
```

```
Dependent covered prefix type cover need deagg, cover 10.20.24.0/24
```

```
ifnums: (none)
```

```
path list 7F6B47831168, 9 locks, per-destination, flags 0x41 [shble, hwc]
```

```
path 7F6B3D9E7B70, share 1/1, type receive, for IPv4
```

```
receive for GigabitEthernet5
```

```
output chain:
```

```
receive
```

Example: Redistribute BGP Route into OSPF and EIGRP Protocols

These examples show how to replicate BGP route from global VRF to service VRF.

```
Device#config-transaction
```

```
Device(config)# vrf definition 2
```

```
Device(config-vrf)# address-family ipv4
Device(config-ipv4)# route-replicate from vrf global unicast bgp 1
Router(config-ipv4)# commit
```

Configure to Redistribute BGP Routes in Global VRF to EIGRP in Service VRF



Note The redistribution of BGP routes into other protocols is supported only if the `bgp redistribute-internal` configuration is present in the BGP route.

```
Device#config-transaction
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast vrf 2 autonomous-system 100
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute vrf global bgp 1 metric 10000 100 200 1
1500
Device(config-ipv4)# commit
```

* Here we are redistributing BGP routes in global VRF to EIGRP in VRF 2.
 * Routes replication must be done before doing inter VRF redistribution.

Verify Configuration

View BGP Route is Present in Global VRF Before Configuring

```
Device#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.0.0.0/9 is subnetted, 1 subnets
B 172.16.255.1 [200/20] via 10.1.15.14, 00:00:25
Device#
```

* We have a BGP route in the global VRF.

View BGP Route is not Present in Service VRF Before Configuring

Use the `show ip route vrf <vrf id> [protocol]` command to view the BGP route in the service VRF table.

```
Device#show ip route vrf 2 bgp

Routing Table: 2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

```

Gateway of last resort is not set

Device#

* We do not have any BGP route in VRF 2.

View BGP Route After Configuring

Use the **show running-config** [*configuration-hierarchy*] | **details** command to verify if the replication configuration exists.

```

Device#show running-config | section vrf definition 2
vrf definition 2
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  !
  address-family ipv4
    route-replicate from vrf global unicast bgp 1
  exit-address-family
Device#

```

* We have successfully applied the route-replicate configuration.

* In our example we are replicating bgp 1 routes from global VRF to VRF 2.

View BGP Route From Global VRF is Replicated into Service VRF After Configuring

Use the **show ip route vrf <vrf id> [protocol]** command to view the BGP route in the service VRF table.

Device#show ip route vrf 2 bgp

```

Routing Table: 2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

```

Gateway of last resort is not set

```

      10.0.0.0/9 is subnetted, 1 subnets
B    +   172.16.255.1 [200/20] via 10.1.15.14, 00:04:01
Device#

```

* After route replication, we can see that the BGP route in the global VRF has been replicated into VRF 2.

* + sign indicates replicated routes.

View EIGRP Configuration Without BGP Redistribution Information

```
Device#show running-config | section router eigrp
router eigrp test
!
address-family ipv4 unicast vrf 2 autonomous-system 100
!
topology base
exit-af-topology
network 10.0.0.0
exit-address-family
Router#
```

View EIGRP Topology Table

Use the **show eigrp address-family ipv4 vrf<vrf-num>topology** command to view the BGP route in the service VRF table.

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.0.0.0/8, 1 successors, FD is 1310720
   via Connected, GigabitEthernet2

Device#

* EIGRP 100 is running on VRF 2.
-----
```

View EIGRP Route After BGP Redistribution

Use the **show eigrp address-family ipv4 vrf<vrf-num>topology** command to view the BGP route is redistributed into the EIGRP protocol.

```
Device#show eigrp address-family ipv4 vrf 2 topology
EIGRP-IPv4 VR(test) Topology Table for AS(100)/ID(10.10.10.2)
Topology(base) TID(0) VRF(2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.0/8, 1 successors, FD is 1310720
   via Connected, GigabitEthernet2
P 172.16.0.0/12, 1 successors, FD is 131072000
   via +Redistributed (131072000/0)

-Device#

* BGP route has been redistributed into EIGRP.
```

Configure Route Redistribution Between Global VRF and Service VPNs Using the CLI

1. Enter the global configuration mode, and create a BGP routing process.



Note You can use the **router eigrp**, or **router ospf** to configure a routing process for a specific routing protocol. This example shows the syntax for BGP routing protocol. To know about the command syntax for various protocols, see the [Cisco IOS XE SD-WAN Qualified Command Reference](#) Guide.

```
Device# config-transaction
```

```
Device(config)# router bgp autonomous-system-number
```

2. Configure an IPv4 address family for service VPNs. This example shows the command syntax for the BGP and EIGRP protocols.

- BGP protocol:

```
Device(config-router-af)# address-family ipv4 [unicast] [vrf vrf-name]
```

- EIGRP protocol:

```
Device(config-router-af)# address-family ipv4 vrf vrf-number
```

3. Redistribute routes between the global VRF and service VPNs. Here, we're showing the syntaxes for the BGP, OSPF, and EIGRP protocols.

- Redistribute routes from service VPNs to the global VRF.

- BGP protocol:

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol  
[src_protocol_id] [route-map route-map-name]
```

- OSPF protocol:

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol  
[src_protocol_id] [match {internal|external 1|external 2}] [metric  
{metric-value}] [subnets] [route-map route-map-name]
```

- EIGRP protocol:

```
Device(config-router-af)# redistribute vrf vrf-name src_protocol  
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric  
effective-bandwidth-metric mtu-bytes] [route-map route-map-name]
```

- Redistribute routes from the global VRF to service VPNs.

- BGP protocol:

```
Device(config-router-af)# redistribute vrf global src_protocol  
[src_protocol_id] [route-map route-map-name]
```

- OSPF protocol:

```
Device(config-router-af)# redistribute vrf global src_protocol  
[src_protocol_id] [match {internal|external 1|external 2}] [subnets]  
[route-map route-map-name]
```

- EIGRP protocol:

```
Device(config-router-af)# redistribute vrf global src_protocol
[src_protocol_id] [metric bandwidth-metric delay-metric reliability-metric
effective-bandwidth-metric mtu-bytes]
```

The following is a sample configuration for configuring route redistribution between a global VRF and service VPN. In this example, VRF 103 and VRF 104 are the service VPNs. The example shows that BGP routes are redistributed from the global VRF to VRF 103, VRF 104.

```
config-transaction
router bgp 100

address-family ipv4 vrf 103
redistribute vrf global bgp 100 route-map test2
!
address-family ipv4 vrf 104
redistribute vrf global bgp 100 route-map test2
!
```

The following is a sample configuration for configuring the OSPF internal and external routes that are redistributed from the global VRF 65535 to the service VRF.

In this case, all OSPF routes are redistributed into the service VRF by using both the **internal** and **external** keywords.

```
config-transaction
router ospf 1
redistribute vrf global ospf 65535 match internal external 1 external 2 subnets route-map
ospf-route-map
```

The following is a sample configuration for configuring the OSPF internal and external routes that are redistributed from service VPNs to the global VRF.

```
config-transaction
router ospf 101
redistribute vrf 101 ospf 101 match internal external 1 external 2 metric 1 subnets route-map
ospf-route-map
```

The following is a sample configuration for configuring the BGP routes that are redistribution from a service VPN to the global VRF.

```
config-transaction
router bgp 50000
address-family ipv4 unicast
redistribute vrf 102 bgp 50000 route-map BGP-route-map
```

The following is a sample configuration for configuring the BGP routes that are redistribution from the global VRF to a service VPN.

```
config-transaction
router bgp 50000
address-family ipv4 vrf 102
redistribute vrf global bgp 50000
```

The following is a sample configuration for configuring route redistribution of BGP, connected, OSPF, and static protocols from the global VRF to VRF 1 when configuring under EIGRP routing process.

```
config-transaction
router eigrp 101
address-family ipv4 vrf 1
redistribute vrf global bgp 50000 metric 1000000 10 255 1 1500
redistribute vrf global connected metric 1000000 10 255 1 1500
redistribute vrf global ospf 65535 match internal external 1 external 2 metric 1000000 10
```

```
255 1 1500
redistribute vrf global static metric 1000000 10 255 1 1500
```

Verify Route Redistribution

Example 1:

The following is a sample output from the **show ip bgp** command using the **internal** keyword. This example shows that a route from VRF 102 is redistributed successfully to the global VRF after the route is replicated.

```
Device# show ip bgp 10.10.10.10 internal

BGP routing table entry for 10.10.10.10/8, version 515
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
700000 70707
10.10.14.17 from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 77775522, metric 7777, localpref 100, weight 32768, valid, sourced,
  replicated, best
Community: 0:7227 65535:65535
Extended Community: SoO:721:75 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB320235DC0, path: 0x7FB320245DF8, pathext: 0x7FB3203A4660
flags: net: 0x0, path: 0x808040003, pathext: 0x81
attribute: 0x7FB38E5B6258, ref: 14
Updated on Jul 1 2021 01:16:36 UTC
vm5#
```

In this output, the route is redistributed from VRF 102 to the global VRF.

The following is a sample output from the **show ip route** command that shows the routes replicated for redistribution.

```
Device# show ip route 10.10.10.10

Routing entry for 10.10.10.10/8
Known via "bgp 50000", distance 60, metric 7777
Tag 700000, type external,
  replicated from topology(102)
Redistributing via ospf 65535, bgp 50000
Advertised by ospf 65535
bgp 50000 (self originated)
Last update from 10.10.14.17 5d15h ago
Routing Descriptor Blocks:
* 10.10.14.17 (102), from 10.10.14.17, 5d15h ago
  opaque_ptr 0x7FB3202563A8
Route metric is 7777, traffic share count is 1
AS Hops 2
Route tag 700000
MPLS label: none
```

Example 2:

The following is a sample output from the **show ip bgp vpnv4 vrf** command using the **internal** keyword.

```
Device# show ip bgp vpnv4 vrf 102 209.165.201.0 internal

BGP routing table entry for 1:102:10.10.10.10/8, version 679
BGP routing table entry for 1:209.165.201.0/27, version 679
Paths: (1 available, best #1, table 102)
```

```

Advertised to update-groups:
4
Refresh Epoch 1
7111 300000
10.1.15.13 (via default) from 0.0.0.0 (172.16.255.15)
Origin IGP, aigp-metric 5755, metric 900, localpref 300, weight 32768, valid, sourced,
replicated, best
Community: 555:666
Large Community: 1:2:3 5:6:7 412789:412780:755
Extended Community: SoO:533:53 RT:50000:102
rx pathid: 0, tx pathid: 0x0
net: 0x7FB38E5C5718, path: 0x7FB3202668D8, pathext: 0x7FB38E69E960
flags: net: 0x0, path: 0x808040007, pathext: 0x181
attribute: 0x7FB320256798, ref: 7
Updated on Jul 6 2021 16:43:04 UTC

```

In this output, the route is redistributed from the global VRF to VRF 102.

The following is a sample output from the **show ip route vrf** command that shows the routes replicated for redistribution for VRF 102.

```

Device# show ip route vrf 102 209.165.201.0

Routing Table: 102
Routing entry for 209.165.201.0/27
Known via "bgp 50000", distance 20, metric 900
Tag 7111, type external,
replicated from topology(default)
Redistributing via bgp 50000
Advertised by bgp 50000 (self originated)
Last update from 10.1.15.13 00:04:57 ago
Routing Descriptor Blocks:
* 10.1.15.13 (default), from 10.1.15.13, 00:04:57 ago
opaque_ptr 0x7FB38E5B5E98
Route metric is 900, traffic share count is 1
AS Hops 2
Route tag 7111
MPLS label: none

```

Configure Route Leaking Between Service VPNs Using a CLI Template

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

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 to configure interservice VPN route leaking on Cisco IOS XE Catalyst SD-WAN devices.

- Replicate routes between interservice VRFs on the same device.

```
vrf definition vrf-number
```

```

address-family ipv4
route-replicate from vrf source-vrf-name unicast protocol [route-map map-tag]

```

- Redistribute the routes that are replicated between the service VPNs:

You can configure the subnets only for bgp, nhrp, ospf, ospfv3, and static protocol types.

```

router ospf process-id vrf vrf-number
redistribute vrf vrf-name protocol subnets [route-map map-tag]

```

The following is a complete configuration example for interservice VRF route replication and redistribution:

```

vrf definition 2
rd 1:2
!
address-family ipv4
route-replicate from vrf 1 unicast static route-map VRF1_TO_VRF2
exit-address-family
!
!
ip prefix-list VRF1_TO_VRF2 seq 5 permit 10.10.10.97/32
!
route-map VRF1_TO_VRF2 permit 1
match ip address prefix-list VRF1_TO_VRF2
!
router ospf 2 vrf 2
redistribute vrf 1 static route-map VRF1_TO_VRF2

```

Verify Route-Leaking Configurations Between Service VPNs Using the CLI

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

The following is a sample output from the **show ip route vrf** command that shows the routes that are replicated for the redistribution to VRF 2:

```

Device# show ip route vrf 2
Routing Table: 2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S   +   10.10.10.97/32 [1/0] via 10.20.1.2 (1)
C       10.20.2.0/24 is directly connected, GigabitEthernet5
L       10.20.2.1/32 is directly connected, GigabitEthernet5

```

The following is a sample output from the **show ip cef vrf** command that shows the replicated routes from VRF 1:

```
Device# show ip cef vrf 2 10.10.10.97 internal
10.10.10.97/32, epoch 0, RIB[S], refcnt 6, per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00048000
    Broker: linked, distributed at 3rd priority
  subblocks:
    Replicated from VRF 1
  ifnums:
    GigabitEthernet3(9): 10.20.1.2
  path list 7F890C8E2F20, 7 locks, per-destination, flags 0x69 [shble, rif, rcrsv, hwc]
  path 7F890FB18F08, share 1/1, type recursive, for IPv4
    recursive via 10.20.1.2[IPv4:1], fib 7F890B609578, 1 terminal fib, v4:1:10.20.1.2/32
  path list 7F890C8E3148, 2 locks, per-destination, flags 0x49 [shble, rif, hwc]
  path 7F890FB19178, share 1/1, type adjacency prefix, for IPv4
    attached to GigabitEthernet3, IP adj out of GigabitEthernet3, addr 10.20.1.2
7F890FAE4CD8
  output chain:
    IP adj out of GigabitEthernet3, addr 10.20.1.2 7F890FAE4CD8
```

Configure VRRP Tracker for Tracking Leaked Service VPNs Using the CLI

Configure a track.

1. Enter global configuration mode, and track the state of an IP route and enter tracking configuration mode.

```
Device# config-transaction
Device(config)# track object-number {ip} route address|prefix-length { reachability
| metric threshold}
```

2. Configure a VPN routing and forwarding (VRF) table.

```
Device(config-track)# ip vrf vrf-name
```

3. Return to privileged EXEC mode

```
Device(config-track)# end
```

Configure VRRP version 2 (VRRPv2).

1. Configure an interface type such as, Gigabit Ethernet.

```
Device(config)# interface type number [name-tag]
```

2. Associate a VRF instance with the Gigabit Ethernet interface.

```
Device(config-if)# vrf forwarding vrf-name
```

3. Set a primary IP address for the Gigabit Ethernet interface.

```
Device(config-if)# ip address ip-address [mask]
```

4. Enable the autonegotiation protocol to configure the speed, duplex mode, and flow control on a Gigabit Ethernet interface.

```
Device(config-if)# negotiation auto
```

5. Create a VRRP group and enter VRRP configuration mode.

```
Device(config-if)# vrrp group address-family ipv4
```

6. Enable the support of VRRP version 2 simultaneously with VRRP version 3.

```
Device(config-if-vrrp)# vrrpv2
```

7. Set the priority level for VRRP.

```
Device(config-if-vrrp)# priority level
```

8. Configure interface list tracking as a single entity.

```
Device(config-if-vrrp)# track track-list-name [decrement priority]
```

9. Configure the preemption delay so that a device with higher priority waits for a minimum period before taking over.

```
Device(config-if-vrrp)# preempt delay minimum seconds
```

10. Specify a primary IP address for VRRP.

```
Device(config-if-vrrp)# address ip-address primary
```

Configure a VRF.

1. Configure a VRF routing table instance and enter the VRF configuration mode.

```
Device(config)# vrf definition vrf-number
```

2. Set an address family IPv4 in vrf configuration mode.

```
Device(config-vrf)# address-family ipv4
```

3. Exit from address-family configuration mode

```
Device(config-ipv4)# exit-address-family
```

The following is a sample configuration for configuring the VRRP tracking.

Use the following configuration to add a track to a VRF red.

```
config-transaction
track 1 ip route 10.1.15.13 255.255.255.0 reachability
ip vrf red
```

Use the following configuration to configure interface tracking and decrement the device priority.

```
interface GigabitEthernet 1.101
vrf forwarding 100
ip address 10.1.15.13 255.255.255.0
negotiation auto
vrrp 2 address-family ipv4
vrrpv2
priority 220
track 1 decrement 25
preempt delay minimum 30
address 10.1.15.100 primary
exit
```

Use the following configuration to configure the VRF routing table instance for the configured VRF.


```
vrf definition 100
!
address-family ipv4
exit-address-family
```

Verify VRRP Tracking

Example 1:

The following is a sample output from the **show vrrp details** command that shows the status of the configured VRRP groups on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# show vrrp details
GigabitEthernet1/0/1 - Group 1 - Address-Family IPv4
  State is BACKUP          <----- check states
  State duration 2 mins 13.778 secs
  Virtual IP address is 10.0.0.1
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 1 (Configured 100)    <----- shows current and configured priority
  Track object 121 state DOWN decrement 220 Master Router is 10.1.1.3, priority is 200
<---- track object state
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 2737 msec)
  FLAGS: 0/1
  VRRPv3 Advertisements: sent 27 (errors 0) - rcvd 149
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Adverts received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
    Init to master: 0
    Init to backup: 1 (Last change Wed Feb 17 23:02:04.259)
    Backup to master: 1 (Last change Wed Feb 17 23:02:07.869) <----- check this for flaps
    Master to backup: 1 (Last change Wed Feb 17 23:02:32.008)
    Master to init: 0
    Backup to init: 0
```

Example 2:

The following is a sample output from the **show track** command that displays information about objects that are tracked by the VRRP tracking process.

```
Device# show track 1
Track 1
  IP route 209.165.200.225 209.165.200.236 reachability
  Reachability is Down (no ip route)
  1 change, last change 1w1d
  VPN Routing/Forwarding table "vrrp"
  First-hop interface is unknown
rtr3#
```

Example 3:

The following is a sample output from the **show running-config interface** command that shows the configuration of a Gigabit Ethernet interface that is tracked by the VRRP tracking process.

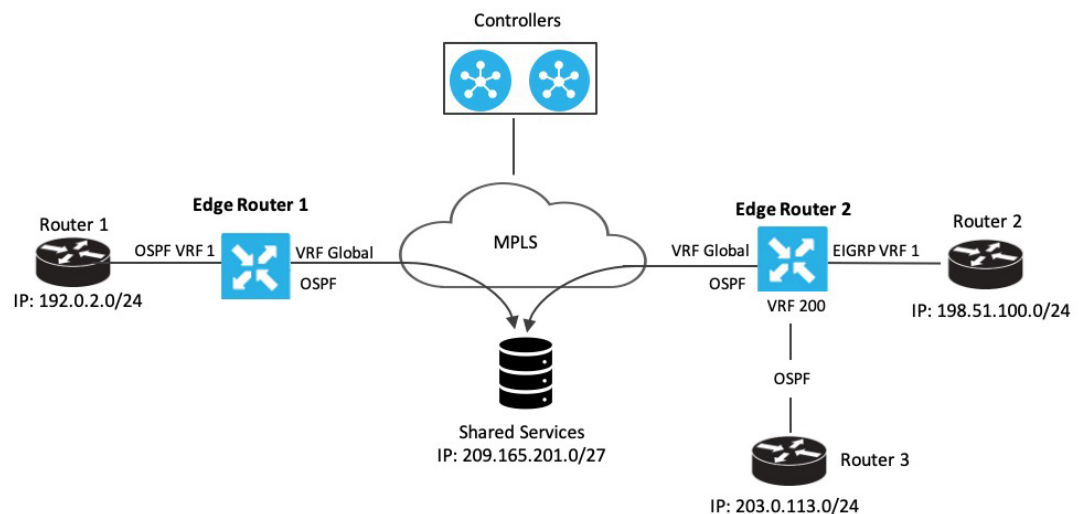
```
Device# show running-config interface GigabitEthernet 4
Building configuration...
Current configuration : 234 bytes
!
interface GigabitEthernet4
ip address 172.16.0.1 255.255.255.0
negotiation auto
vrrp 7 address-family ipv4
  priority 200
  vrrpv2
  track 5 decrement 50-----priority decrement
  address 172.16.0.0 primary
exit-vrrp
no mop enabled
no mop sysid
end
```

Configuration Example for Route Leaking

Route leaking is typically used in scenarios requiring the use of shared services. Configuring route replication allows mutual redistribution between VRFs or VPNs. Route replication allows shared services because routes are replicated or leaked between the global VRF and service VPNs and clients who reside in one VPN can reach matching prefixes that exist in another VPN.

Sample Topology

In this section, we'll use an example topology to show route-leaking configuration. Here, Edge routers 1 and 2 are located in two different sites in the overlay network and are connected to each other through MPLS. Both the edge routers have route leaking configured to be able to access services in the underlay network. Router 1 sits behind Edge Router 1 in the service side. The local network at this site runs OSPF. Router 2 sits behind the Edge Router 2 on network that has EIGRP in VRF 1. Router 3 also sits behind Edge Router 2 and has OSPF running in VRF 200.



Edge Router 1 imports the source IP address of Router 1, 192.0.2.0/24 to the global VRF on Edge Router 1. Thus 192.0.2.0/24 is a route leaked into the global VRF. Edge Router 2 imports the source IP address of Router 2, 198.51.100.0/24 and the source IP address of Edge Router 3, 203.0.113.0/24 to the global VRF on Edge Router 2.

Shared services in the underlay MPLS network are accessed through a loopback address of 209.21.25.18/27. The IP address of the shared services is advertised to the global VRF on Edge Routers 1 and 2 through OSPF. This shared service IP address is then leaked to VRF 1 in Edge Router 1 and VRF 1 and VRF 200 in Edge Router 2. In terms of route-leaking, the leaked routes are imported into the service VRFs on both the edge routers.



Note OMP doesn't advertise any leaked routes from service VPNs into the overlay network to prevent route looping.

Configuration Examples

This example shows the configuration of BGP and OSPF route leaking between the global VRF and VPN 1 on Edge Router 2.

```
vrf definition 1
  rd 1:1
  !
  address-family ipv4
    route-replicate from vrf global unicast ospf 65535
  !
  global-address-family ipv4
    route-replicate from vrf 1 unicast eigrp
  exit-address-family
```

This example shows the configuration of BGP and OSPF route leaking between the global VRF and VPN 200 on Edge Router 2.

```
vrf definition 200
  rd 1:200
  !
  address-family ipv4
    route-replicate from vrf global unicast ospf 65535
  !
  global-address-family ipv4
    route-replicate from vrf 200 unicast eigrp
  exit-address-family
```

