Route Leaking Between VPNs

Table 1: Feature History

Feature Name	Release Information	Description
Route Leaking Between Transport VPN and Service VPNs	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature enables you to leak routes bidirectionally between the transport VPN 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.
Route Manipulation for Leaked Routes with OMP Administrative Distance	Cisco vManage Release 20.6.1 Cisco SD-WAN Release 20.6.1	This feature allows you to configure the following: - OMP administrative distance option to prefer OMP routes over MPLS routes
Route Leaking between Inter-Service VPN	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	With this feature, you can leak routes between the service VPNs at the same edge device.

Supported Protocols

The following protocols are supported for route leaking between the transport VPN and service VPNs.

- Connected

- Static
- BGP
- OSPF

Restrictions for Route Leaking and Redistribution

- Route leaking between the transport VPN and service VPNs is supported for data traffic only. It’s not supported for control traffic.

  Any traffic destined to the router's service-side interface doesn't get a ping response and is dropped. For example: If you ping the IP address of a service-side interface from the global network, it’s dropped at the transport VPN because Cisco vEdge devices consider it as control traffic. However, if you ping the IP address of the host that is connected to the service side, Cisco vEdge devices consider it as transient traffic or data traffic and allows it to pass.
- Route attributes aren’t retained because all routes are leaked as static routes.
- All the leaked routes are displayed as static in the routing table.
- Each service VPN can leak (import and export) a maximum of 1000 routes.
- Each transport VPN can leak (import and export) a maximum of 10,000 routes.
- All supported protocols leaked between the transport VPN and the service VPNs appear as static routes in the Routing Information Base (RIB) with a distance of 240.
- Service-side NAT isn’t supported with route leaking between the transport VPN and service VPNs.
- NAT isn't supported with transport VPN route leaking.
- IPv6 address family isn’t supported for route leaking.
- Only prefix-lists, metrics, and OSPF tags can be matched in route policies to filter leaked routes between the transport VPN and service VPNs.
- Overlay Management Protocol (OMP) routes do not participate in VPN route leaking to prevent overlay looping.
- Route leaking using centralized policy is not supported.

Information About Route Leaking

Route Leaking Between Transport VPN and Service VPNs

The Cisco SD-WAN solution lets you segment the network using VPNs. Route leaking between the transport VPN or VPN 0 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 VPN 0 and the 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 vEdge devices based on the following points:

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

To configure the OMP administrative distance using Cisco vManage, see Configure Basic VPN Parameters and Configure OMP Using vManage Templates.

To configure the OMP administrative distance using the CLI, see the Configure OMP Administrative Distance section in Configure OMP Using CLI.

Inter-Service VPN Route Leaking

Minimum supported release: Cisco SD-WAN Release 20.9.1, Cisco vManage Release 20.9.1.

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

To resolve routing-scalability challenges introduced when you use Cisco vSmart controllers, you can leak routes between the VPNs at the edge device.

To configure the inter-service VPN route leaking feature using Cisco vManage, see Configure Route Leaking Between Service VPNs.

To configure the inter-service VPNs route leaking feature using the CLI, see Configure Route Leaking Between Service VPNs Using the CLI.

Features of Route Leaking

- Routes between the transport and service VPNs can be leaked directly.
- Multiple service VPNs can be leaked to the transport VPN.
- Route leaks of multiple service VPNs into the same service VPN is supported.
- When routes are leaked, the source VPN information is retained.
- You can control leaked routes using policies.
- Route policies can filter routes before leaking them. However, only prefix-lists, metrics, and OSPF tags are matched for filtering routes.
- The feature can be configured using both—Cisco vManage 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 VPNs is used where the VPN traffic goes through a zone-based firewall on the same branch router while being PCI compliant.

How Route Preference is Determined

1. RIB local routes with the same prefix are preferred over leaked routes.
2. If multiple routes learn from the same prefix, the following order of preference is maintained:
   a. Routes with smaller administrative distance are preferred.
   b. ECMP routes are preferred over non-ECMP.
   c. The oldest route is preferred.

Workflow to Configure Route Leaking Using Cisco vManage

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 vManage 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 vManage 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 vManage 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 vManage to the device.

Configure and Enable Route Leaking between Global and Service VPNs

1. From the Cisco vManage 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 **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—65530.

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 transport VPN, 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. Click **Add**.

f. To leak routes from the service VPNs to the transport VPN, 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. 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 static routes to BGP or OSPF protocols, see one of the following:

- Configure BGP
- Configure OSPF

- 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. Perform all operations from Step c of creating a feature template.

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 vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Navigate to the **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 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**, and **BGP** 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. Click **Add**.
11. Click **Save**.

Attach the Service Side VPN Feature Template to the Device Template

1. From the Cisco vManage 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 vManage to the device.

Configure and Verify Route Leaking Using the CLI

Configuration Example: Leak Routes Between Transport VPN and Service VPN

The following examples show how to configure route leaking between a transport VPN and a service VPN.

In this example, VPN 1 represents the service VPN, and in Cisco SD-WAN VPN 0 is the transport VPN.

Import Routes from VPN 0 to VPN 1 and Export Routes from VPN 1 to VPN 0

```
vpn 1
  route-import static
  route-import connected
  route-export static
  route-export connected
```

This example shows that connected and static routes are imported into VPN 1 from the transport VPN. Similarly, the same route-types are exported from VPN 1 to the transport VPN.

Apply Route Policy to Filter Selective Routes between the VPNs for the Protocols Leaked

```
vpn 1
 route-import static route-policy myRoutePolicy
 route-import connected
 route-export static
 route-export connected
```

Verify Configuration

Run the **show ip route vpn** *vpn-id* command to view the routes leaked from the service VPN to the transport VPN.

Note In the outputs, the imported routes are represented by **L** in the status column.

Routes Leaked from Service VPNs to VPN 0

```
Device#  show ip route vpn 1
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
                                          PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP

VPN     PREFIX              PROTOCOL         SUB TYPE  IF NAME     ADDR             VPN
  TLOC IP          COLOR            ENCAP  STATUS
-------------------------------------------------------------------------------------------
3       10.1.16.0/24        static           -         -           -                0
  -                 -                -      F,S,L
3       10.1.18.0/24        omp              -         -           -                -
  172.16.255.11     lte              ipsec  -
3       10.1.18.0/24        static           -         -           -                0
  -                 -                -      F,S,L
```

```
3      172.16.255.112/32   static           -          -          -                0
  -                -                -      F,S,L
3      172.16.255.117/32   omp              -          -          -                -
  172.16.255.11    lte              ipsec
```

Run the **show ip route vpn 0** command to view the routes leaked from the VPN 0 to the service VPN. See the following example.

Routes Leaked from VPN 0 to Service VPNs

```
Device# show ip route vpn 0
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
                                          PROTOCOL   NEXTHOP     NEXTHOP          NEXTHOP

VPN    PREFIX              PROTOCOL         SUB TYPE   IF NAME     ADDR             VPN
  TLOC IP          COLOR            ENCAP   STATUS
0      10.15.15.0/24       static           -          -          -                1
  -                -                       F,S,L
0      10.16.16.0/24       static           -          -          -                2
  -                -                -      F,S,L
0      10.17.17.0/24       ospf             E2         ge0/3      10.0.21.23       -
  -                -                -      F,S
```

Configure Route Leaking Between Service VPNs Using a CLI Template

Minimum supported release: Cisco SD-WAN Release 20.9.1

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 vEdge devices.

- Configure interservice VPN route replication:

```
vpn vpn-id
route-import-service from vpn vpn-id protocol route-policy policy-name
```

Note The redistribute protocol will always be **static** because leaked routes lose their original attributes.

Leaked routes will always be displayed as **static** in the routing table.

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

```
vpn vpn-id
router protocol
redistribute static route-policy policy-name
```

Note Always use the **static** protocol to redistribute the leaked routes.

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

```
vpn 102
 route-import-service from vpn 101 static route-policy VPN101_TO_VPN102
!
policy
 lists
  prefix-list VPN101_TO_VPN102
   ip-prefix 10.0.100.0/24
  !
 !
 route-policy VPN101_TO_VPN102
  sequence 1
   match
    address VPN101_TO_VPN102
   !
   action accept
   !
  !
  default-action reject
 !
!
vpn 102
 router
  ospf
   redistribute static route-policy VPN101_TO_VPN102
 !
!
```

Verify Route-Leaking Configurations Between Service VPNs Using the CLI

Minimum supported release: Cisco SD-WAN Release 20.9.1

The following is a sample output from the **show ip route vpn** command displaying the routes that are replicated for redistribution to VPN 102:

```
vEdge# show ip route vpn 102
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

```
                                          PROTOCOL  NEXTHOP     NEXTHOP   NEXTHOP
VPN    PREFIX              PROTOCOL       SUB TYPE  IF NAME     ADDR      VPN      TLOC IP
COLOR   ENCAP  STATUS
-------------------------------------------------------------------------------------------------
102    10.0.100.0/24       static           -     ge0/4.105    -         101      -
  -       -      F,S,L
102    10.10.25.44/32      static           -         -        -         101      -
  -       -      F,S,L
102    10.10.25.45/32      static           -         -        -         101      -
  -       -      F,S,L
102    192.168.25.0/24     connected        -     ge0/4.102    -         -        -
  -       -      F,S
```

The following is a sample output from the **show ip fib vpn** command that shows the replicated routes' VPNs:

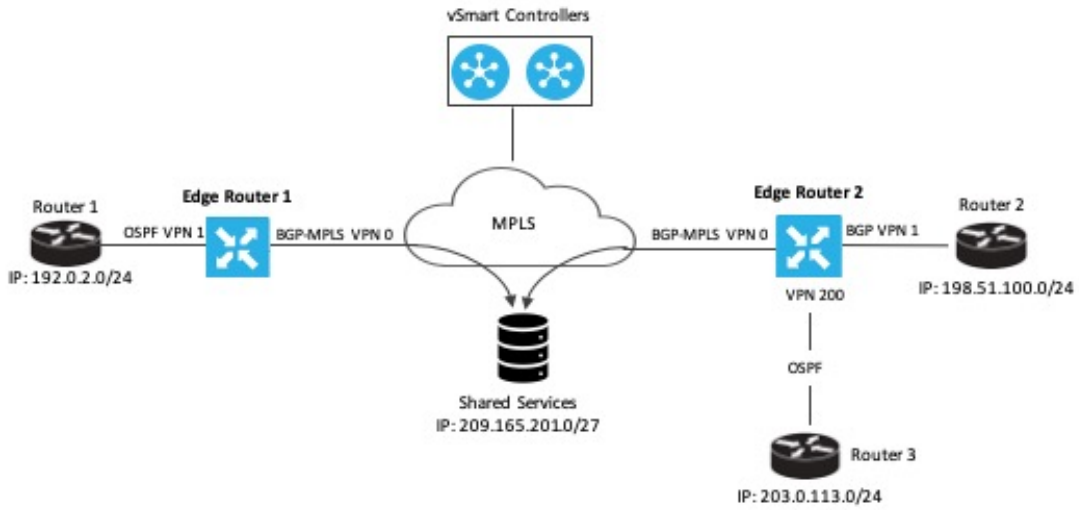
```
vEdge# show ip fib vpn 102
                          NEXTHOP     NEXTHOP   NEXTHOP  NEXTHOP  SA
VPN  PREFIX               IF NAME     ADDR      LABEL    VPN      INDEX    TLOC IP
  COLOR
-------------------------------------------------------------------------------------------------
102  10.0.100.0/24        ge0/4.105   -           -        -        -        -
    -
102  10.51.51.16/32       ge0/4.105   -           -        -        -        -
    -
102  10.61.61.0/24        -           -           -        6        -        -
    -
```

Configuration Example for Route Leaking

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

Topology Example

In this section, we'll take 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 network. 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 sites behind the Edge Router 2 on network that has eBGP in VPN 1. Router 3 also sites behind Edge Router 2 and has OSPF running in VPN 200.



Edge Router 1 imports the source IP address of Router 1, 192.0.2.0/24 to VPN 0 on Edge Router 1. Thus 192.0.2.0/24 is a route leaked into VPN 0. 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 VPN 0 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 are advertised to VPN 0 on Edge Routers 1 and 2 through BGP. This shared service IP address is then leaked to VPN 1 in Edge Router 1 and VPN 1 and VPN 200 in Edge Router 2. In terms of route-leaking, the leaked routes are imported into the service VPNs on both the edge routers.

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

Configure Route Leaking

The following example shows route import and export on Edge Router 1.

```
Edge Router 1(config)# vpn 1
 Edge Router 1(vpn-1)# route-export ospf
 Edge Router 1(vpn-1)# route-import ospf
```

The following example shows import and export of BGP and OSPF routes on Edge Router 2.

```
Edge Router 2(config)# vpn 1
 Edge Router 1(vpn-1)# route-export bgp
 Edge Router 1(vpn-1)# route-import ospf

Edge Router 2(config)# vpn 200
 Edge Router 1(vpn-200)# route-export bgp
 Edge Router 1(vpn-1)# route-import ospf
```

Route Redistribution

OSPF learns routes from other VPNs leaking routes into OSPF. The same is true of BGP. In this example, we'll look at how to have OSPF and BGP redistribute the routes learned from route leaking. The following examples show OSPF redistributing connected, static, and OMP routes; and BGP redistributing OMP and static routes.

```
Edge Router 1# show running-config vpn 1 router
vpn 1
 router
  ospf
   redistribute static
   redistribute connected
   redistribute omp
   area 0
    interface ge0/4
     hello-interval 1
     dead-interval  3
    exit
   exit
  !
 !
!
```

```
Edge Router 2# show running-config vpn 1 router
vpn 1
 router
  bgp 1
   timers
    keepalive 1
    holdtime  3
   !
   address-family ipv4-unicast
    redistribute static
    redistribute omp
   !
   neighbor 198.51.100.1
    no shutdown
    remote-as 2
    timers
     connect-retry          2
     advertisement-interval 1
    !
   !
  !
 !
!
```

Verify Route Leaking Configuration

Use the **show ip routes** command to view the IP addresses that are leaked along with their status. The following output shows the routes leaked into VPN 1 and VPN 200 on Edge Router 2.

Note In the outputs, the imported routes are represented by **L** in the status column.

Routes Leaked from VPNs 1 and 200 on Edge Router 2

```
Device# show ip routes 209.165.201.0/27
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import

                                                PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
```

```
VPN     PREFIX              PROTOCOL          SUB TYPE   IF NAME     ADDR             VPN
  TLOC IP          COLOR             ENCAP   STATUS
-------------------------------------------------------------------------------------------
0       209.165.201.0/27    ospf               IA         ge0/0       10.1.16.13       -
  -              -                 -       F,S
0       209.165.201.0/27    ospf               IA         ge0/3       10.0.21.23       -
  -              -                 -       F,S
1       209.165.201.0/27    static             -          -           -                0
  -              -                 -       F,S,L
200     209.165.201.0/27    static             -          -           -                0
  -              -                 -       F,S,L
```

BGP Routes Leaked to VPN 0 on Edge Router 2

```
Device# show ip routes 198.51.100.0/24
Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import
```

```
                                                PROTOCOL  NEXTHOP     NEXTHOP          NEXTHOP
VPN     PREFIX              PROTOCOL            SUB TYPE  IF NAME     ADDR             VPN
  TLOC IP          COLOR             ENCAP     STATUS
-------------------------------------------------------------------------------------------
0       198.51.100.0/24     static             -         -           -                1
  -              -                 -       F,S,L
1       198.51.100.0/24     bgp                e         ge0/4       10.0.21.22       -
 -               -                 -       F,S
```

See VPN Next Hop Information

Run the **show ip fib** command to view the next hop information for VPNs.

Example of next hop information for VPN 1

```
Device# show ip fib vpn 1
                                                NEXTHOP     NEXTHOP          NEXTHOP  NEXTHOP
  SA
VPN  PREFIX                                     IF NAME     ADDR             LABEL    VPN
  INDEX    TLOC IP          COLOR
-------------------------------------------------------------------------------------------
1    10.0.5.0/24                                -           -                -        0
  -        -                -
1    10.0.6.0/24                                -           -                -        0
  -        -                -
1    10.0.101.3/32                              -           -                -        0
  -        -                -
1    10.0.101.4/32                              -           -                -        0
  -        -                -
1    10.0.111.1/32                              -           -                -        0
  -        -                -
1    209.165.201.0/27                           -           -                -        0
  -        -                -
```

Example of next hop information for VPN 0

```
Device# show ip fib vpn 0
```

```
                                                    NEXTHOP     NEXTHOP          NEXTHOP  NEXTHOP
  SA
VPN  PREFIX                                         IF NAME     ADDR             LABEL    VPN
  INDEX    TLOC IP          COLOR
-------------------------------------------------------------------------------------------------
0    198.51.100.0/24                          -          -               -        1        -
       -               -
```

View Packets and Transmission Statistics

To view the packets received and the transmission statistics for an interface, use the **show app cflows flows** command.

```
Device# show app cflowd flows
```

```
                                                                        TCP
                                                                TIME    EGRESS  INGRESS
                                          SRC    DEST            IP     CNTRL  ICMP
  TOTAL  TOTAL    MIN  MAX                                     TO      INTF    INTF     APP
VPN  SRC IP          DEST IP          PORT   PORT   DSCP  PROTO  BITS   OPCODE  NHOP IP
  PKTS   BYTES    LEN  LEN  START TIME                        EXPIRE  NAME    NAME     ID
-------------------------------------------------------------------------------------------------
1    10.0.5.11       172.16.255.118  0      0      0     1      0      2048    198.51.100.0
  152    14896    98   98   Tue May 26 15:33:13 2020  59      ge0/4   ge0/0    0
1    10.0.26.11      172.16.255.118  0      0      0     1      0      2048    198.51.100.0
  76     7448     98   98   Tue May 26 15:33:15 2020  58      ge0/4   ge0/3    0
1    172.16.255.118  10.0.5.11       0      0      0     1      0      0       10.0.21.23
   152    14896    98   98   Tue May 26 15:33:13 2020  59      ge0/3   ge0/4    0
1    172.16.255.118  10.0.26.11      0      0      0     1      0      0       10.0.21.23
   76     7448     98   98   Tue May 26 15:33:15 2020  58      ge0/3   ge0/4    0
```