Segmentation

Network segmentation has existed for over a decade and has been implemented in multiple forms and shapes. At its most rudimentary level, segmentation provides traffic isolation. The most common forms of network segmentation are virtual LANs, or VLANs, for Layer 2 solutions, and virtual routing and forwarding, or VRF, for Layer 3 solutions.

There are many use cases for segmentation:

Use Cases for Segmentation

- An enterprise wants to keep different lines of business separate (for example, for security or audit reasons).
- The IT department wants to keep authenticated users separate from guest users.
- A retail store wants to separate video surveillance traffic from transactional traffic.
- An enterprise wants to give business partners selective access only to some portions of the network.
- A service or business needs to enforce regulatory compliance, such as compliance with HIPAA, the U.S. Health Insurance Portability and Accountability Act, or with the Payment Card Industry (PCI) security standards.
- A service provider wants to provide VPN services to its medium-sized enterprises.

Limitations of Segmentation

One inherent limitation of segmentation is its scope. Segmentation solutions either are complex or are limited to a single device or pair of devices connected via an interface. As an example, Layer 3 segmentation provides the following:

1. Ability to group prefixes into a unique route table (RIB or FIB).
2. Ability to associate an interface with a route table so that traffic traversing the interface is routed based on prefixes in that route table.

This is a useful functionality, but its scope is limited to a single device. To extend the functionality throughout the network, the segmentation information needs to be carried to the relevant points in the network.

How to Enable Network-Wide Segmentation

There are two approaches to providing this network-wide segmentation:

- Define the grouping policy at every device and on every link in the network (basically, you perform Steps 1 and 2 above on every device).
- Define the grouping policy at the edges of the segment, and then carry the segmentation information in the packets for intermediate nodes to handle.

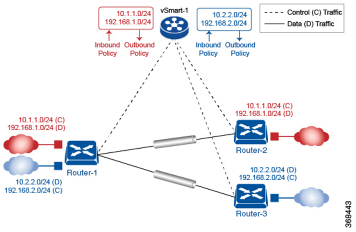
The first approach is useful if every device is an entry or exit point for the segment, which is generally not the case in medium and large networks. The second approach is much more scalable and keeps the transport network free of segments and complexity.

Segmentation in Cisco SD-WAN

In the Cisco SD-WAN overlay network, VRFs divide the network into different segments.

Cisco SD-WAN employs the more prevalent and scalable model of creating segments. Essentially, segmentation is done at the edges of a router, and the segmentation information is carried in the packets in the form of an identifier.

The figure shows the propagation of routing information inside a VRF.



In this figure:

- Router-1 subscribes to two VRFs, red and blue.
  - The red VRF caters to the prefix 10.1.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
  - The blue VRF caters to the prefix 10.2.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-2 subscribes to the red VRF.
  - This VRF caters to the prefix 192.168.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-3 subscribes to the blue VRF.
  - This VRF caters to the prefix 192.168.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).

Because each router has an OMP connection over a TLS tunnel to a vSmart controller, it propagates its routing information to the vSmart controller. On the vSmart controller, the network administrator can enforce policies to drop routes, to change TLOCs (which are overlay next hops) for traffic engineering or service chaining). The network administrator can apply these policies as inbound and outbound policies on the vSmart controller.

All prefixes belonging to a single VRF are kept in a separate route table. This provides the Layer 3 isolation required for the various segments in the network. So, Router-1 has two VRF route tables, and Router-2 and Router-3 each have one route table. In addition, the vSmart controller maintains the VRF context of each prefix.

Separate route tables provide isolation on a single node. So now the question is how to propagate the routing information across the network.

In the Cisco SD-WAN solution, this is done using VRF identifiers, as shown in the figure below. A VRF ID carried in the packet identifies each VRF on a link. When you configure a VRF on a Router, the VRF has a label associated with it. The Router sends the label, along with the VRF ID, to the vSmart controller. The vSmart controller propagates this Router-to- VRF-ID mapping information to the other Routers in the domain. The remote Routers then use this label to send traffic to the appropriate VRF. The local Routers, on receiving the data with the VRF ID label, use the label to demultiplex the data traffic. This is similar to how MPLS labels are used. This design is based on standard RFCs and is compliant with regulatory procedures (such as PCI and HIPAA).

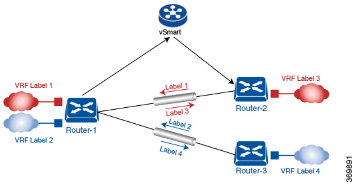


Figure 1:

It is important to point out that the transport network that connects the routers is completely unaware of the VRFs. Only the routers know about VRFs; the rest of the network follows standard IP routing.

VRFs Used in Cisco SD-WAN Segmentation

The Cisco SD-WAN solution involves the use of VRFs to separate traffic.

Global VRF

The global VRF is used for transport. To enforce the inherent separation between services (such as prefixes that belong to the enterprise) and transport (the network that connects the routers), all the transport interfaces (that is, all the TLOCs) are kept in the global VRF. This ensures that the transport network cannot reach the service network by default. Multiple transport interfaces can belong to the same VRF, and packets can be forwarded to and from transport interfaces.

A global VRF contains all interfaces for a device except for the management interface, and all the interfaces are disabled. For the control plane to establish itself so that the overlay network can function, you must configure tunnel interfaces in a global VRF.For each interface in a global VRF, you must set an IP address, and you create a tunnel connection that sets the color and encapsulation for the WAN transport connection. (The encapsulation is used for the transmission of data traffic.) These three parameters—IP address, color, and encapsulation—define a TLOC (transport location) on the router. The OMP session running on each tunnel sends the TLOC to the vSmart controllers so that they can learn the overlay network topology.

Dual Stack Support on Transport VPNs

In the global VRF, Cisco IOS XE SD-WAN devices and vSmart controllers support dual stack. To enable dual stack, configure an IPv4 address and an IPv6 address on the tunnel interface. The router learns from the vSmart controller whether a destination supports IPv4 or IPv6 addresses. When forwarding traffic, the router chooses either the IPv4 or the IPv6 TLOC based on the destination address. But IPv4 is always preferred when configured.

Management VRF

Mgmt-Intf is the management VRF on Cisco IOS XE SD-WAN devices. It is configured and enabled by feault. It carries out-of-band network management traffic among the devices in the overlay network. You can modify this configuration if desired.

Configure VRF Using Cisco vManage Templates

In vManage, use a CLI template to configure VRFs for a device. For each VRF, configure a subinterface and link the subinterface to the VRF. Configure up to 300 VRFs.

When you push a CLI template to a device, Cisco vManage overwrites any existing configuration on the device and loads the configuration defined in the CLI template. Consequently, the template cannot only provide the new content being configured, such as VRFs. The CLI template must include all configuration details required by the device. To display the relevant configuration details on a device, you can use the **show sdwan running-config** command.

For details about creating and applying CLI templates, and for an example of configuring VRFs, see the CLI Templates for Cisco XE SD-WAN Routers chapter of the Systems and Interfaces Configuration Guide.

Supported devices: Cisco ASR1001-HX, ASR1002-HX

Configure VPNs Using vManage Templates

Create a VPN Template

Note Cisco IOS XE SD-WAN devices use VRFs for segmentation and network isolation. However, the following steps still apply if you are configuring segmentation for Cisco IOS XE SD-WAN devices through Cisco vManage. When you complete the configuration, the system automatically converts the VPNs to VRFs for Cisco IOS XE SD-WAN devices.

Step 1 In Cisco vManage, choose **Configuration** > **Templates**.

Step 2 In the Device tab, click **Create Template**.

Step 3 From the Create Template drop-down, select **From Feature Template**.

Step 4 From the **Device Model** drop-down, select the type of device for which you are creating the template.

Step 5 To create a template for VPN 0 or VPN 512:

a. Click the **Transport & Management** VPN tab located directly beneath the Description field, or scroll to the Transport & Management VPN section.

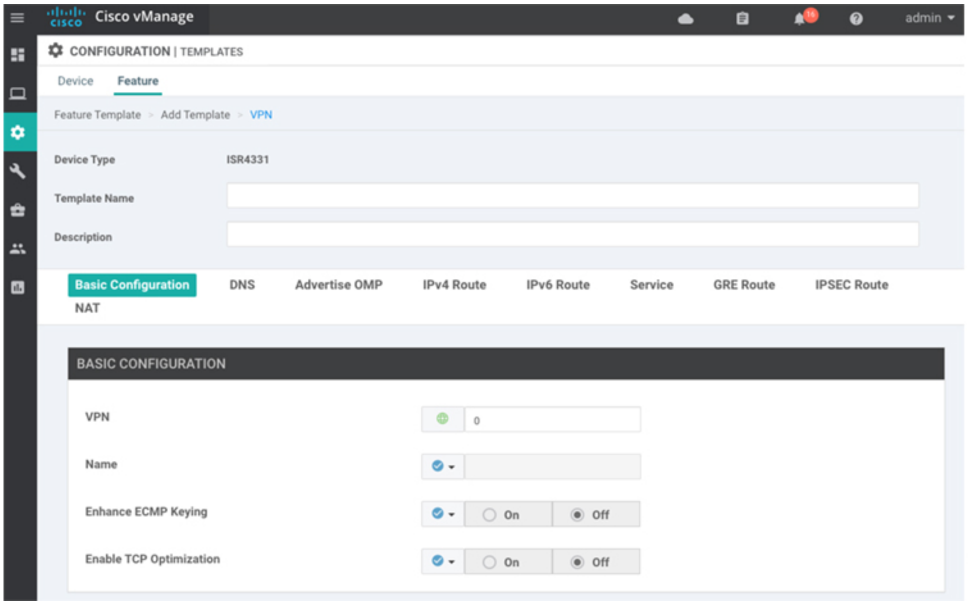
b. From the VPN 0 or VPN 512 drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.

Step 6 To create a template for VPNs 1 through 511, and 513 through 65527:

a. Click the **Service VPN** tab located directly beneath the Description field, or scroll to the Service VPN section.

b. Click the **Service VPN** drop-down.

c. From the VPN drop-down, click **Create Template**. The VPN template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.



Device Type ISR4331

Template Name

Description

VPN 0

Name

Enhance ECMP Keying ○ On ● Off

Enable TCP Optimization ○ On ● Off

Step 7 In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.

Step 8 In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

Configure Basic VPN Parameters

To configure basic VPN parameters, choose the Basic Configuration tab and then configure the following parameters. Parameters marked with an asterisk are required to configure a VPN.

Parameter Name	Description
VPN	Enter the numeric identifier of the VPN. Range for Cisco IOS XE SD-WAN devices: 0 through 65527 Values for Cisco vSmart Controller and Cisco vManage devices: 0, 512

Parameter Name	Description
Name	Enter a name for the VPN. **Note** For Cisco IOS XE SD-WAN devices, you cannot enter a device-specific name for the VPN.

Note To complete the configuration of the transport VPN on a router, you must configure at least one interface in VPN 0.

To save the feature template, click **Save**.

Configure Basic Interface Functionality

To configure basic interface functionality in a VPN, choose the **Basic Configuration** tab and configure the following parameters:

Note Parameters marked with an asterisk are required to configure an interface.

Parameter Name	IPv4 or IPv6	Options	Description
Shutdown*	Click **No** to enable the interface.		
Interface name*	Enter a name for the interface. For Cisco IOS XE SD-WAN devices, you must: • Spell out the interface names completely (for example, GigabitEthernet0/0/0). • Configure all the router's interfaces, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.		
Description	Enter a description for the interface.		
IPv4 / IPv6	Click **IPv4** to configure an IPv4 VPN interface. Click **IPv6** to configure an IPv6 interface.		
Dynamic	Click **Dynamic** to set the interface as a Dynamic Host Configuration Protocol (DHCP) client, so that the interface receives its IP address from a DHCP server.		
	Both	**DHCP Distance**	Optionally, enter an administrative distance value for routes learned from a DHCP server. Default is 1.
	IPv6	**DHCP Rapid Commit**	Optionally, configure the DHCP IPv6 local server to support DHCP Rapid Commit, to enable faster client configuration and confirmation in busy environments. Click **On** to enable DHCP rapid commit Click **Off** to continue using the regular commit process.

Parameter Name	IPv4 or IPv6	Options	Description
Static	Click **Static** to enter an IP address that doesn't change.		
	IPv4	**IPv4 Address**	Enter a static IPv4 address.
	IPv6	**IPv6 Address**	Enter a static IPv6 address.
Secondary IP Address	**IPv4**	Click **Add** to enter up to four secondary IPv4 addresses for a service-side interface.	
IPv6 Address	**IPv6**	Click **Add** to enter up to two secondary IPv6 addresses for a service-side interface.	
DHCP Helper	**Both**	To designate the interface as a DHCP helper on a router, enter up to eight IP addresses, separated by commas, for DHCP servers in the network. A DHCP helper interface forwards BootP (broadcast) DHCP requests that it receives from the specified DHCP servers.	
Block Non-Source IP	**Yes** / **No**	Click **Yes** to have the interface forward traffic only if the source IP address of the traffic matches the interface's IP prefix range. Click **No** to allow other traffic.	

To save the feature template, click **Save**.

Create a Tunnel Interface

On Cisco IOS XE SD-WAN devices, you can configure up to four tunnel interfaces. This means that each Cisco IOS XE SD-WAN device router can have up to four TLOCs. On Cisco vSmart Controllers and Cisco vManage, you can configure one tunnel interface.

For the control plane to establish itself so that the overlay network can function, you must configure WAN transport interfaces in VPN 0. The WAN interface will enable the flow of tunnel traffic to the overlay. You can add other parameters shown in the table below only after you configure the WAN interface as a tunnel interface.

To configure a tunnel interface, select the **Interface Tunnel** tab and configure the following parameters:

Parameter Name	Description
Tunnel Interface	Click **On** to create a tunnel interface.
Color	Select a color for the TLOC.
Port Hop	Click **On** to enable port hopping, or click **Off** to disable it. If port hopping is enabled globally, you can disable it on an individual TLOC (tunnel interface). To control port hopping on a global level, use the System configuration template. Default: Enabled vManage NMS and Cisco vSmart Controller default: Disabled
Allow Service	Select **On** or **Off** for each service to allow or disallow the service on the interface.

To configure additional tunnel interface parameters, click **Advanced Options**:

Parameter Name	Description
Carrier	Select the carrier name or private network identifier to associate with the tunnel. Values: carrier1, carrier2, carrier3, carrier4, carrier5, carrier6, carrier7, carrier8, default Default: default
NAT Refresh Interval	Enter the interval between NAT refresh packets sent on a DTLS or TLS WAN transport connection. Range: 1 through 60 seconds Default: 5 seconds
Hello Interval	Enter the interval between Hello packets sent on a DTLS or TLS WAN transport connection. Range: 100 through 10000 milliseconds Default: 1000 milliseconds (1 second)
Hello Tolerance	Enter the time to wait for a Hello packet on a DTLS or TLS WAN transport connection before declaring that transport tunnel to be down. Range: 12 through 60 seconds Default: 12 seconds

To save the feature template, click **Save**.

Configure DNS and Static Hostname Mapping

To configure DNS addresses and static hostname mapping, click the **DNS** tab and configure the following parameters:

Parameter Name	Options	Description
Primary DNS Address	Select either **IPv4** or **IPv6**, and enter the IP address of the primary DNS server in this VPN.	
New DNS Address	Click **New DNS Address** and enter the IP address of a secondary DNS server in this VPN. This field appears only if you have specified a primary DNS address.	
	Mark as Optional Row	Check **Mark as Optional Row** to mark this configuration as device-specific. To include this configuration for a device, enter the requested variable values when you attach a device template to a device, or create a template variables spreadsheet to apply the variables.
	Hostname	Enter the hostname of the DNS server. The name can be up to 128 characters.
	List of IP Addresses	Enter up to eight IP addresses to associate with the hostname. Separate the entries with commas.
To save the DNS server configuration, click **Add**.		

To save the feature template, click **Save**.

Mapping Host Names to IP Addresses

```
! IP DNS-based host name-to-address translation is enabled
  ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
  ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
  ip domain name cisco.com
```

Configure Segmentation Using CLI

Configure VRFs Using CLI

To segment user networks and user data traffic locally at each site and to interconnect user sites across the overlay network, you create VRFs on Cisco IOS XE SD-WAN devices. To enable the flow of data traffic, you associate interfaces with each VRF, assigning an IP address to each interface. These interfaces connect to local-site networks, not to WAN transport clouds. For each of these VRFs, you can set other interface-specific properties, and you can configure features specific for the user segment, such as BGP and OSPF routing, VRRP, QoS, traffic shaping, and policing.

On Cisco IOS XE SD-WAN devices, a global VRF is used for transport. All Cisco IOS XE SD-WAN devices have Mgmt-intf as the default management VRF.

To configure VRFs on Cisco IOS XE SD-WAN devices, follow these steps.

Note

- Use the **config-transaction** command to open CLI configuration mode. The config terminal command is not supported on Cisco IOS XE SD-WAN devices.
- The VRF ID can be any number between 1 through 511 and 513 through 65535. The numbers 0 and 512 are reserved for Cisco vManage and Cisco vSmart controller.

1. Configure service VRFs.

```
config-transaction
 vrf definition 10
  rd 1:10
  address-family ipv4
   exit-address-family
   exit
 address-family ipv6
  exit-address-family
  exit
exit
```

2. Configure the tunnel interface to be used for overlay connectivity. Each tunnel interface binds to a single WAN interface. For example, if the router interface is Gig0/0/2, the tunnel interface number is 2.

```
config-transaction
 interface Tunnel 2
  no shutdown
  ip unnumbered GigabitEthernet1
  tunnel source GigabitEthernet1
  tunnel mode sdwan
  exit
```

3. If the router is not connected to a DHCP server, configure the IP address of the WAN interface.

```
 interface GigabitEthernet 1
 no shutdown
 ip address dhcp
```

4. Configure tunnel parameters.

```
config-transaction
 sdwan
  interface GigabitEthernet 2
   tunnel-interface
    encapsulation ipsec
    color lte
    end
```

Note If an IP address is manually configured on the router, configure a default route as shown below. The IP address below indicates a next-hop IP address.

```
config-transaction
 ip route 0.0.0.0 0.0.0.0 192.0.2.25
```

5. Enable OMP to advertise VRF segment vroutes.

```
sdwan
omp
 no shutdown
 graceful-restart
 no as-dot-notation
 timers
```

```
    holdtime 15
    graceful-restart-timer 120
    exit
   address-family ipv4
    advertise ospf external
    advertise connected
    advertise static
    exit
   address-family ipv6
    advertise ospf external
    advertise connected
    advertise static
    exit
   address-family ipv4 vrf 1
    advertise bgp
    exit
   exit
```

6. Configure the service VRF interface.

```
config-transaction
 interface GigabitEthernet 2
  no shutdown
  vrf forwarding 10
  ip address 192.0.2.2 255.255.255.0
  exit
```

Verify Configuration

Run the **show ip vrf brief** command to view information about the VRF interface.

```
Device# sh ip vrf brief
  Name                              Default RD            Interfaces
  10                                1:10                  Gi4
  11                                1:11                  Gi3
  30                                1:30
  65528                             <not set>             Lo65528
```

Segmentation (VRFs) Configuration Examples

Some straightforward examples of creating and configuring VRFs to help you understand the configuration procedure for segmenting networks.

Configuration on the vSmart Controller

On the vSmart controller, you configure general system parameters and the two VPNs—VPN 0 for WAN transport and VPN 512 for network management—as you did for the Cisco IOS XE SD-WAN device. Also, you generally create a centralized control policy that controls how the VPN traffic is propagated through the rest of the network. In this particular example, we create a central policy, shown below, to drop unwanted prefixes from propagating through the rest of the network. You can use a single vSmart policy to enforce policies throughout the network.

Here are the steps for creating the control policy on the vSmart controller:

1. Create a list of sites IDs for the sites where you want to drop unwanted prefixes:

   ```
   vSmart(config)# policy lists site-list 20-30 site-id 20
   vSmart(config-site-list-20-30)# site-id 30
   ```

2. Create a prefix list for the prefixes that you do not want to propagate:

   ```
   vSmart(config)# policy lists prefix-list drop-list ip-prefix 10.200.1.0/24
   ```

3. Create the control policy:

   ```
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 match route
   prefix-list drop-list
   vSmart(config-match)# top
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 action reject
   vSmart(config-action)# top
   vSmart(config)# policy control-policy drop-unwanted-routes sequence 10 default-action
   accept
   vSmart(config-default-action)# top
   ```

4. Apply the policy to prefixes inbound to the vSmart controller:

   ```
   vSmart(config)# apply-policy site-list 20-30 control-policy drop-unwanted-routes in
   ```

Here is the full policy configuration on the vSmart controller:

```
apply-policy
 site-list 20-30
  control-policy drop-unwanted-routes in
 !
!
policy
 lists
  site-list 20-30
   site-id 20
   site-id 30
  !
  prefix-list drop-list
   ip-prefix 10.200.1.0/24
  !
 !
 control-policy drop-unwanted-routes
  sequence 10
   match route
    prefix-list drop-list
   !
   action reject
   !
  !
  default-action accept
 !
!
```

Segmentation CLI Reference

CLI commands for monitoring segmentation (VRFs).

- show dhcp
- show ipv6 dhcp
- show ip vrf brief
- show igmp commands
- show ip igmp groups
- show pim commands