THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2022 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1  Read Me First  1

CHAPTER 2  What's New in Cisco IOS XE (SD-WAN)  3

CHAPTER 3  Policy Overview  5
   Policy Architecture  7
      Centralized Control Policy Architecture  7
   Route Types  8
      Default Behavior Without Centralized Control Policy  9
      Behavior Changes with Centralized Control Policy  9
      Examples of Modifying Traffic Flow with Centralized Control Policy  10
      Configure Centralized Policy Based on Prefixes and IP Headers  12
   Cisco vSmart Policy Components  13
      TLOC Attributes Used in Policies  16
      vRoute Attributes Used in Policies  17
   Design Cisco vSmart Controller Policy Processing and Application  18
   Cisco vSmart Policy Operation  19
      Control Policy  20
      Data Policy  22
      VPN Membership Policy Operation  24
   Configure and Execute Cisco vSmart Policies  25

CHAPTER 4  Centralized Policy  27
   Overview of Centralized Policies  27
   Types of Centralized Policies  27
   Configure Centralized Policies Using Cisco vManage  28
CHAPTER 6

Redirect DNS in a Service-Side VPN 91

Information About Redirect DNS in a Service-Side VPN 91
Restrictions for Redirect DNS in a Service-Side VPN 92
Use Cases for Redirect DNS in a Service-Side VPN 92
Configure Redirect DNS in a Service-Side VPN Using Cisco vManage 94
Configure Redirect DNS in a Service-Side VPN Using the CLI 96
Verify Redirect DNS in a Service-Side VPN 98
Configuration Examples for Redirect DNS 98

CHAPTER 7

Default AAR and QoS Policies 101

Information About Default AAR and QoS Policies 101
Benefits of Default AAR and QoS Policies 102
Prerequisites for Default AAR and QoS Policies 102
Restrictions for Default AAR and QoS Policies 103
Supported Devices for Default AAR and QoS Policies 103
Use Cases for Default AAR and QoS Policies 103
Configure Default AAR and QoS Policies Using Cisco vManage 103
Monitor Default AAR and QoS Policies 107

CHAPTER 8

Device Access Policy 109

Device Access Policy Overview 109
Configure Device Access Policy Using Cisco vManage 110
Configure Device Access Policy Using the CLI 111
Examples for ACL Statistics and Counters 111
Verifying ACL Policy on an SNMP Server 113
Verifying ACL Policy on SSH 114

CHAPTER 9

SD-WAN Application Intelligence Engine Flow 117

SD-WAN Application Intelligence Engine Flow Overview 117
Configure SD-WAN Application Intelligence Engine Flow Using Cisco vManage 118
Apply Centralized Policy for SD-WAN Application Intelligence Engine Flow 118
Monitor Running Applications 119
View SAIE Applications 119
CHAPTER 10  
Application-Aware Routing  125

Information About Application-Aware Routing  125
  Application-Aware Routing Support for Multicast Protocols  126
  Restrictions for Multicast Protocols  126
  Components of Application-Aware Routing  127
  SLA Classes  128
  Classification of Tunnels into SLA Classes  131
    Measure Loss, Latency, and Jitter  131
    Calculate Average Loss, Latency, and Jitter  131
    Determine SLA Classification  131
  Per-Class Application-Aware Routing  132
    Per-Class Application-Aware Routing Overview  132
    Application Probe Class  133
    Default DSCP Values  133
  Configure Application-Aware Routing  133
    Configure Application-Aware Routing Policies Using Cisco vManage  134
  Configure Best Tunnel Path  134
    Best Tunnel Path Overview  135
    Recommendation for the Best Tunnel Path  135
    Configure Variance for Best Tunnel Path  135
    Verify Configuration of Variance for Best Tunnel Path  136
  Configure SLA Class  137
  Configure Traffic Rules  138
  Default Action of Application-Aware Routing Policy  142
  Configure Application Probe Class through vManage  142
    Add App-Probe-Class to an SLA Class  143
  Configure Default DSCP on Cisco BFD Template  143
  Apply Policies to Sites and VPNS  144
    How Application-Aware Routing Policy is Applied in Combination with Other Data Policies  145
  Activate an Application-Aware Routing Policy  146
  Monitor Data Plane Tunnel Performance  146
## Contents

<table>
<thead>
<tr>
<th>Chapter 11</th>
<th>Traffic Flow Monitoring with eFlow</th>
<th>155</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Information about Traffic Flow Monitoring</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Traffic Flow Monitoring with Cflowd Overview</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>IPFIX Information Elements for Cisco IOS XE SD-WAN Devices</td>
<td>157</td>
</tr>
<tr>
<td></td>
<td>Flexible Netflow for VPN0 Interface</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>Limitations of Flexible Netflow on VPN0 Interface</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>Configure Traffic Flow Monitoring on Cisco IOS XE SD-WAN Devices</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>Configure Global Flow Visibility</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>Configure Global Application Visibility</td>
<td>163</td>
</tr>
<tr>
<td></td>
<td>Configure Cflowd Monitoring Policy</td>
<td>164</td>
</tr>
<tr>
<td></td>
<td>View Cflowd Information</td>
<td>166</td>
</tr>
<tr>
<td></td>
<td>Configure Cflowd Traffic Flow Monitoring Using the CLI</td>
<td>167</td>
</tr>
<tr>
<td></td>
<td>Configure Flexible Netflow on VPN0 Interface</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>Verify Flexible Netflow Configuration on VPN0 Interface</td>
<td>168</td>
</tr>
<tr>
<td></td>
<td>Apply and Enable Cflowd Policy</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>Cflowd Traffic Flow Monitoring Configuration Example</td>
<td>173</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12</th>
<th>Application Performance Monitor</th>
<th>177</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview of Application Performance Monitor</td>
<td>177</td>
</tr>
<tr>
<td></td>
<td>Limitations and Restrictions</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Configure Application Performance Monitor</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Verify Performance Monitoring Configuration</td>
<td>181</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13</th>
<th>Enhanced Policy Based Routing</th>
<th>193</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overview of ePBR</td>
<td>193</td>
</tr>
<tr>
<td></td>
<td>Configure ePBR</td>
<td>195</td>
</tr>
<tr>
<td></td>
<td>Monitor ePBR</td>
<td>198</td>
</tr>
</tbody>
</table>

| Chapter 14 | Forward Error Correction | 201 |

Enable Application Visibility on Cisco IOS XE SD-WAN Devices 148
Configure Application-Aware Routing Using CLIs 148
Configure Application Probe Class Using CLI 150
Application-Aware Routing Policy Configuration Example 151
Contents

CHAPTER 15
Packet Duplication for Noisy Channels 205
Information about Packet Duplication 205
Configure Packet Duplication 205
Monitor Packet Duplication Per Application 206

CHAPTER 16
Integrate Cisco IOS XE SD-WAN Device with Cisco ACI 209
Guidelines to Integrate with Cisco ACI 210
Verify Cisco ACI Registration 210
SLA Classes 210
Data Prefixes 211
VPNs 211
Map Data Prefix and VPN to SLA 211
Create an App-Route-Policy 211
Map ACI Sites 212
Unmap ACI Sites 213
Delete a Controller 213

CHAPTER 17
Define Custom Applications 215
Overview 215
Define Custom Applications Using Cisco vManage 217
View Custom Applications 219

CHAPTER 18
Service Chaining 221
Configure Service Chaining 224
Service Chaining Configuration Examples 226
Monitor Service Chaining 231

CHAPTER 19
Lawful Intercept 235
Information About Lawful Intercept 235
Prerequisites for Lawful Intercept  238
Install Lawful Intercept using vManage  239
Lawful Intercept MIBs  239
Restrict Access to Trusted Hosts (Without Encryption)  240
Restrict Trusted Mediation Device  240
Configure Lawful Intercept  241
Configure Lawful Intercept Using CLI  241
Encrypt Lawful Intercept Traffic  242
  Configure Encryption in the Device  242
  Configure Lawful Intercept Encryption using CLI  243
Verify Static Tunnel with Media Device Gateway  244
Read Me First

Related References

- Release Notes
- Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations

User Documentation

- Cisco IOS XE (Cisco IOS XE SD-WAN Devices)
- Cisco IOS XE (SD-WAN) Qualified Command Reference
- User Documentation for Cisco IOS XE (SD-WAN) Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.
Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.
What's New in Cisco IOS XE (SD-WAN)

Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

What's New in Cisco IOS XE (SD-WAN) Release 17.x
Policy Overview

Policy influences the flow of data traffic and routing information among Cisco IOS XE SD-WAN devices in the overlay network.

Policy comprises:

- Routing policy—which affects the flow of routing information in the network's control plane.
- Data policy—which affects the flow of data traffic in the network's data plane.

To implement enterprise-specific traffic control requirements, you create basic policies, and deploy advanced features that are activated by means of the policy configuration infrastructure.

Just as the Cisco SD-WAN overlay network architecture clearly separates the control plane from the data plane and control between centralized and localized functions, the Cisco SD-WAN policy is cleanly separated. Policies apply either to control plane or data plane traffic, and they are configured either centrally on Cisco vSmart Controllers or locally on Cisco IOS XE SD-WAN devices. The following figure illustrates the division between control and data policy, and between centralized and local policy.

**Figure 1: Policy Architecture**

Control and Data Policy

Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Centralized and Localized Policy

The Cisco SD-WAN policy design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized Cisco vSmart Controllers in the overlay network, and the localized policy is provisioned on Cisco IOS XE SD-WAN devices, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.
Centralized Policy

Centralized policy refers to policy provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network-wide routing of traffic
- Data policy, which affects the data traffic flow throughout the VPN segments in the network

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco vSmart Controller's route table and that is advertised to the Cisco IOS XE SD-WAN devices. The effects of centralized control policy are seen in how Cisco IOS XE SD-WAN devices direct the overlay network's data traffic to its destination.

Note

The centralized control policy configuration itself remains on the Cisco vSmart Controller and is never pushed to local devices.

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the selected Cisco IOS XE SD-WAN devices.

Localized Policy

Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco IOS XE SD-WAN devices, or through a Cisco vManage device template.

Localized control policy is also called as route policy, which affects (BGP and OSPF) routing behavior on the site-local network.

Localized data policy allows you to provision access lists and apply them to a specific interface or interfaces on the device. Simple access lists permit and restrict access based on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol), in the same way as with centralized data policy. Access lists also allow provisioning of class of service (CoS), policing, which control how data traffic flows out of and in to the device's interfaces and interface queues.

The design of the Cisco SD-WAN policy distinguishes basic and advanced policies. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a Cisco IOS XE SD-WAN device's interfaces, enabling features such as class of service and queuing, and policing.

- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.
- Cflowd, for monitoring traffic flow.

By default, no policy of any kind is configured on Cisco IOS XE SD-WAN devices, either on the centralized Cisco vSmart Controllers or the local Cisco IOS XE SD-WAN devices. When control plane traffic, which distributes route information, is unpolicied:
• All route information that OMP propagates among the Cisco IOS XE SD-WAN devices is shared, unmodified, among all Cisco vSmart Controllers and all Cisco IOS XE SD-WAN devices in the overlay network domain.

• No BGP or OSPF route policies are in place to affect the route information that Cisco IOS XE SD-WAN devices propagate within their local site network.

When data plane traffic is unpolicied, all data traffic is directed towards its destination based solely on the entries in the local Cisco IOS XE SD-WAN device's route table, and all VPNs in the overlay network can exchange data traffic.

• Policy Architecture, on page 7
• Cisco vSmart Policy Components, on page 13
• Design Cisco vSmart Controller Policy Processing and Application, on page 18
• Cisco vSmart Policy Operation, on page 19
• Configure and Execute Cisco vSmart Policies, on page 25

Policy Architecture

This topic offers an orientation about the architecture of the Cisco SD-WAN policy used to implement overlay network-wide policies. These policies are called vSmart policy or centralized policy, because you configure them centrally on a Cisco vSmart Controller. Cisco vSmart policy affects the flow of both control plane traffic (routing updates carried by Overlay Management Protocol (OMP) and used by the Cisco vSmart Controllers to determine the topology and status of the overlay network) and data plane traffic (data traffic that travels between the Cisco IOS XE SD-WAN devices across the overlay network).

With Cisco SD-WAN, you can also create routing policies on the Cisco IOS XE SD-WAN devices. These policies are simply traditional routing policies that are associated with routing protocol (BGP or OSPF) locally on the devices. You use them in the traditional sense for controlling BGP and OSPF, for example, to affect the exchange of route information, to set route attributes, and to influence path selection.

Centralized Control Policy Architecture

In the Cisco IOS XE SD-WAN network architecture, centralized control policy is handled by the Cisco vSmart Controller, which effectively is the routing engine of the network. The Cisco vSmart Controller is the centralized manager of network-wide routes, maintaining a primary route table for these routes. The Cisco vSmart Controller builds its route table based on the route information advertised by the Cisco IOS XE SD-WAN devices in its domain, using these routes to discover the network topology and to determine the best paths to network destinations. The Cisco vSmart Controller distributes route information from its route table to the devices in its domain which in turn use these routes to forward data traffic through the network. The result of this architecture is that networking-wide routing decisions and routing policy are orchestrated by a central authority instead of being implemented hop by hop, by the devices in the network.

Centralized control policy allows you to influence the network routes advertised by the Cisco vSmart Controllers. This type of policy, which is provisioned centrally on the Cisco vSmart Controller, affects both the route information that the Cisco vSmart Controller stores in its primary route table and the route information that it distributes to the devices.

Centralized control policy is provisioned and applied only on the Cisco vSmart Controller. The control policy configuration itself is never pushed to devices in the overlay network. What is pushed to the devices, using the Overlay Management Protocol (OMP), are the results of the control policy, which the devices then install.
in their local route tables and use for forwarding data traffic. This design means that the distribution of network-wide routes is always administered centrally, using policies designed by network administrators. These policies are always implemented by centralized Cisco vSmart Controllers, which are responsible for orchestrating the routing decisions in the Cisco IOS XE SD-WAN overlay network.

Within a network domain, the network topology map on all Cisco vSmart Controllers must be synchronized. To support this, you must configure identical policies on all the Cisco vSmart Controllers in the domain.

*Figure 2: Centralized Control Policy*

All centralized control plane traffic, including route information, is carried by OMP peering sessions that run within the secure, permanent DTLS connections between devices and the Cisco vSmart Controllers in their domain. The end points of an OMP peering session are identified by the system IDs of the devices, and the peering sessions carry the site ID, which identifies the site in which the device is located. A DTLS connection and the OMP session running over it remain active as long as the two peers are operational.

Control policy can be applied both inbound, to the route advertisements that the Cisco vSmart Controller receives from the devices, and outbound, to advertisements that it sends to them. Inbound policy controls which routes and route information are installed in the local routing database on the Cisco vSmart Controller, and whether this information is installed as-is or is modified. Outbound control policy is applied after a route is retrieved from the routing database, but before a Cisco vSmart Controller advertises it, and affects whether the route information is advertised as-is or is modified.

**Route Types**

The Cisco vSmart Controller learns the network topology from OMP routes, which are Cisco IOS XE SD-WAN-specific routes carried by OMP. There are three types of OMP routes:

- **Cisco IOS XE SD-WAN OMP routes**—These routes carry prefix information that the devices learn from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes. OMP advertises OMP routes to the Cisco vSmart Controller by means of an OMP route SAFI (Subsequent Address Family Identifier). These routes are commonly simply called OMP routes.

- **TLOC routes**—These routes carry properties associated with transport locations, which are the physical points at which the devices connect to the WAN or the transport network. Properties that identify a TLOC include the IP address of the WAN interface and a color that identifies a particular traffic flow. OMP advertises TLOC routes using a TLOC SAFI.

- **Service routes**—These routes identify network services, such as firewalls and IDPs, that are available on the local-site network to which the devices are connected. OMP advertises these routes using a service SAFI.

The difference in these three types of routes can be viewed by using the various `show sdwan omp` operational commands when you are logged in to the CLI on a Cisco vSmart Controller or a Cisco IOS XE SD-WAN device. The `show sdwan omp routes` command displays information sorted by prefix, the `show sdwan omp`
services command displays route information sorted by service, and the show sdwan omp tlocs command sorts route information by TLOC.

Default Behavior Without Centralized Control Policy

By default, no centralized control policy is provisioned on the Cisco vSmart Controller. This results in the following route advertisement and redistribution behavior within a domain:

- All Cisco IOS XE SD-WAN devices redistribute all the route-related prefixes that they learn from their site-local network to the Cisco vSmart Controller. This route information is carried by OMP route advertisements that are sent over the DTLS connection between the devices and the Cisco vSmart Controller. If a domain contains multiple Cisco vSmart Controllers, the devices send all OMP route advertisements to all the controllers.

- All the devices send all TLOC routes to the Cisco vSmart Controller or controllers in their domain, using OMP.

- All the devices send all service routes to advertise any network services, such as firewalls and IDPs, that are available at the local site where the device is located. Again, these are carried by OMP.

- The Cisco vSmart Controller accepts all the OMP, TLOC, and service routes that it receives from all the devices in its domain, storing the information in its route table. The Cisco vSmart Controller tracks which OMP routes, TLOCs, and services belong to which VPNs. The Cisco vSmart Controller uses all the routes to develop a topology map of the network and to determine routing paths for data traffic through the overlay network.

- The Cisco vSmart Controller redistributes all information learned from the OMP, TLOC, and service routes in a particular VPN to all the devices in the same VPN.

- The devices regularly send route updates to the Cisco vSmart Controller.

- The Cisco vSmart Controller recalculates routing paths, updates its route table, and advertises new and changed routing information to all the devices.

Behavior Changes with Centralized Control Policy

When you do not want to redistribute all route information to all Cisco IOS XE SD-WAN devices in a domain, or when you want to modify the route information that is stored in the Cisco vSmart Controller's route table or that is advertised by the Cisco vSmart Controller, you design and provision a centralized control policy. To activate the control policy, you apply it to specific sites in the overlay network in either the inbound or the outbound direction. The direction is with respect to the Cisco vSmart Controller. All provisioning of centralized control policy is done on the Cisco vSmart Controller.

Applying a centralized control policy in the inbound direction filters or modifies the routes being advertised by the Cisco IOS XE SD-WAN device before they are placed in the route table on the Cisco vSmart Controller. As the first step in the process, routes are either accepted or rejected. Accepted routes are installed in the route table on the Cisco vSmart Controller either as received or as modified by the control policy. Routes that are rejected by a control policy are silently discarded.

Applying a control policy in outbound direction filters or modifies the routes that the Cisco vSmart Controller redistributes to the Cisco IOS XE SD-WAN devices. As the first step of an outbound policy, routes are either accepted or rejected. For accepted routes, centralized control policy can modify the routes before they are distributed by the Cisco vSmart Controller. Routes that are rejected by an outbound policy are not advertised.
VPN Membership Policy

A second type of centralized data policy is VPN membership policy. It controls whether a Cisco IOS XE SD-WAN device can participate in a particular VPN. VPN membership policy defines which VPNs of a device is allowed and which is not allowed to receive routes from.

VPN membership policy can be centralized, because it affects only the packet headers and has no impact on the choice of interface that a Cisco IOS XE SD-WAN device uses to transmit traffic. What happens instead is that if, because of a VPN membership policy, a device is not allowed to receive routes for a particular VPN, the Cisco vSmart Controller never forwards those routes to that driver.

Examples of Modifying Traffic Flow with Centralized Control Policy

This section provides some basic examples of how you can use centralized control policies to modify the flow of data traffic through the overlay network.

Create an Arbitrary Topology

When data traffic is exchanged between two Cisco IOS XE SD-WAN devices, if you have provisioned no control policy, the two devices establish an IPsec tunnel between them and the data traffic flows directly from one device to the next. For a network with only two devices or with just a small number of devices, establishing connections between each pair of devices is generally not an issue. However, such a solution does not scale. In a network with hundreds or even thousands of branches, establishing a full mesh of IPsec tunnels tax the CPU resources of each device.

Figure 3: Arbitrary Topology

One way to minimize this overhead is to create a hub-and-spoke type of topology in which one of the devices acts as a hub site that receives the data traffic from all the spoke, or branch, devices and then redirects the traffic to the proper destination. This example shows one of the ways to create such a hub-and-spoke topology, which is to create a control policy that changes the address of the TLOC associated with the destination.

The figure illustrates how such a policy might work. The topology has two branch locations, West and East. When no control policy is provisioned, these two devices exchange data traffic with each other directly by creating an IPsec tunnel between them (shown by the red line). Here, the route table on the Device West contains a route to Device East with a destination TLOC of 203.0.113.1, color gold (which we write as the tuple {192.0.2.1, gold}), and Device East route table has a route to the West branch with a destination TLOC of {203.0.113.1, gold}.

To set up a hub-and-spoke-type topology here, we provision a control policy that causes the West and East devices to send all data packets destined for the other device to the hub device. (Remember that because control policy is always centralized, you provision it on the Cisco vSmart Controller.) On the Device West, the policy simply changes the destination TLOC from {203.0.113.1, gold} to {209.165.200.225, gold}, which is the TLOC of the hub device, and on the Device East, the policy changes the destination TLOC from {192.0.2.1, gold} to the hub’s TLOC, {209.165.200.225, gold}. If there were other branch sites on the west
and east sides of the network that exchange data traffic, you could apply these same two control policies to have them redirect all their data traffic through the hub.

**Set Up Traffic Engineering**

Control policy allows you to design and provision traffic engineering. In a simple case, suppose that you have two devices acting as hub devices. If you want data traffic destined to a branch Cisco IOS XE SD-WAN device to always transit through one of the hub devices, set the TLOC preference value to favor the desired hub device.

*Figure 4: Traffic Engineering Topology*

The figure shows that Site ID 100 has two hub devices, one that serves the West side of the network and a second that serves the East side. Data traffic from the Device West must be handled by the Device West hub, and similarly, data traffic from the Device East branch must go through the Device East hub.

To engineer this traffic flow, you provision two control policies, one for Site ID 1, where the Device West device is located, and a second one for Site ID 2. The control policy for Site ID 1 changes the TLOC for traffic destined to the Device East to {209.165.200.225, gold}, and the control policy for Site ID 2 changes the TLOC for traffic destined for Site ID 1 to {198.51.100.1, gold}. One additional effect of this traffic engineering policy is that it load-balances the traffic traveling through the two hub devices.

With such a traffic engineering policy, a route from the source device to the destination device is installed in the local route table, and traffic is sent to the destination regardless of whether the path between the source and destination devices is available. Enabling end-to-end tracking of the path to the ultimate destination allows the Cisco vSmart Controller to monitor the path from the source to the destination, and to inform the source device when that path is not available. The source device can then modify or remove the path from its route table.

*Figure 5: Traffic Engineering 2*

The figure Traffic Engineering 2 illustrates end-to-end path tracking. It shows that traffic from Device-A that is destined for Device-D first goes to an intermediate device, Device-B, perhaps because this intermediate device provides a service, such as a firewall. (You configure this traffic engineering with a centralized control policy that is applied to Device-A, at Site 1.) Then Device-B, which has a direct path to the ultimate destination, forwards the traffic to Device-D. So, in this example, the end-to-end path between Device-A and Device-D comprises two tunnels, one between Device-A and Device-B, and the second between Device-B and Device-D.
The Cisco vSmart Controller tracks this end-to-end path, and it notifies Device-A if the portion of the path between Device-B and Device-D becomes unavailable.

As part of end-to-end path tracking, you can specify how to forwarded traffic from the source to the ultimate destination using an intermediate device. The default method is strict forwarding, where traffic is always sent from Device-A to Device-B, regardless of whether Device-B has a direct path to Device-D or whether the tunnel between Device-B and Device-D is up. More flexible methods forward some or all traffic directly from Device-A to Device-D. You can also set up a second intermediate device to provide a redundant path with the first intermediate device is unreachable and use an ECMP method to forward traffic between the two. The figure Traffic Engineering 3 adds Device-C as a redundant intermediate device.

Centralized control policy, which you configure on Cisco vSmart Controllers, affects routing policy based on information in OMP routes and OMP TLOCs.

In domains with multiple Cisco vSmart Controllers, all the controllers must have the same centralized control policy configuration to ensure that routing within the overlay network remains stable and predictable.

**Configure Centralized Policy Based on Prefixes and IP Headers**

A centralized data policy based on source and destination prefixes and on headers in IP packets consists of a series of numbered (ordered) sequences of match-action pair that are evaluated in order, from lowest sequence number to highest sequence number. When a packet matches one of the match conditions, the associated action is taken and policy evaluation on that packets stops. Keep this in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the sequences in the policy configuration, it is dropped and discarded by default.

**Configuration Components**

The following figure illustrates the configuration components for a centralized data policy:
Cisco vSmart Policy Components

The Cisco vSmart policies that implement overlay network-wide policies are implemented on a Cisco vSmart Controller. Because Cisco vSmart Controllers are centralized devices, you can manage and maintain Cisco vSmart policies centrally, and you can ensure consistency in the enforcement of policies across the overlay network.

The implementation of Cisco vSmart policy is done by configuring the entire policy on the Cisco vSmart Controller. Cisco vSmart policy configuration is accomplished with three building blocks:

- Lists define the targets of policy application or matching.
- Policy definition, or policies, controls aspects of control and forwarding. There are different types of policy, including:
  - app-route-policy (for application-aware routing)
  - cflowd-template (for cflowd flow monitoring)
  - control-policy (for routing and control plane information)
  - data-policy (for data traffic)
  - vpn-membership-policy (for limiting the scope of traffic to specific VPNS)
- Policy application controls what a policy is applied towards. Policy application is site-oriented, and is defined by a specific list called a site-list.

You assemble these three building blocks to Cisco vSmart policy. More specifically, policy is the sum of one or more lists, one policy definition, and at least one policy applications, as shown in the table below.

*Table 1: The Three Building Blocks of Cisco vSmart Policies*

<table>
<thead>
<tr>
<th>Lists</th>
<th>Policy Definition</th>
<th>Policy Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-prefix-list: List of prefixes for use with a data-policy</td>
<td>app-route-policy: Used with sla-classes for application-aware routing</td>
<td>+ apply-policy: Used with a site-list to determine where policies are applied</td>
</tr>
<tr>
<td>prefix-list: List of prefixes for use with any other policy</td>
<td>cflowd-template: Configures the cflowd agents on the Cisco IOS XE SD-WAN devices</td>
<td>+ control-policy: Controls OMP routing control</td>
</tr>
<tr>
<td>site-list: List of site-id:s for use in policy and apply-policy</td>
<td>data-policy: Provides vpn-wide policy-based routing</td>
<td>+ data-policy: Provides vpn-wide policy-based routing</td>
</tr>
<tr>
<td>tloc-list: List of tloc:s for use in policy</td>
<td>vpn-list: List of vpn:s for use in policy</td>
<td>+ vpn-membership-policy: Controls vpn membership across nodes</td>
</tr>
</tbody>
</table>

Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x
Complete policy definition configured on Cisco vSmart and enforced either on Cisco vSmart or on Cisco IOS XE SD-WAN devices.

Lists

Lists are how you group related items so that you can reference them all together. Examples of items you put in lists are prefixes, TLOCs, VPNs, and overlay network sites. In the Cisco vSmart Controller policy, you invoke lists in two places: when you create a policy definition and when you apply a policy. Separating the definition of the related items from the definition of policy means that when you can add or remove items from a lists, you make the changes only in a single place: You do not have to make the changes through the policy definition. So if you add ten sites to your network and you want to apply an existing policy to them, you simply add the site identifiers to the site list. You can also change policy rules without having to manually modify the prefixes, VPNs, or other things that the rules apply to.

Table 2: List Types

<table>
<thead>
<tr>
<th>List type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-prefix-list</td>
<td>Used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.</td>
</tr>
<tr>
<td>prefix-list</td>
<td>Used in control-policy to define prefixes for matching RIB entries.</td>
</tr>
<tr>
<td>site-list</td>
<td>Used in control-policy to match source sites, and in apply-policy to define sites for policy application.</td>
</tr>
<tr>
<td>tloc-list</td>
<td>Used in control-policy to define TLOCs for matching RIB entries and to apply redefined TLOCs to vRoutes.</td>
</tr>
<tr>
<td>vpn-list</td>
<td>Used in control-policy to define prefixes for matching RIB entries, and in data-policy and app-route-policy to define VPNs for policy application.</td>
</tr>
</tbody>
</table>

The following configuration shows the types of Cisco vSmart Controller policy lists:

```
policy
  lists
    data-prefix-list app1
      ip-prefix 209.165.200.225/27 port 100
    prefix-list pfx1
      ip-prefix 209.165.200.225/27
    site-list site1
      site-id 100
    tloc-list site1-tloc
      tloc 209.165.200.225 color mpls
    vpn-list vpn1
      vpn1
  !
```
Policy Definition

The policy definition is where you create the policy rules. You specify match conditions (route-related properties for control policy and data-related fields for data policy) and actions to perform when a match occurs. A policy contains match–action pairings that are numbered and that are examined in sequential order. When a match occurs, the action is performed, and the policy analysis on that route or packet terminates. Some types of policy definitions apply only to specific VPNs.

Table 3: Policy Types

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-type</td>
<td>Can be control-policy, data-policy, or vpn-membership—dictates the type of policy. Each type has a particular syntax and a particular set of match conditions and settable actions.</td>
</tr>
<tr>
<td>vpn-list</td>
<td>Used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.</td>
</tr>
<tr>
<td>sequence</td>
<td>Defines each sequential step of the policy by sequence number.</td>
</tr>
<tr>
<td>match</td>
<td>Decides what entity to match on in the specific policy sequence.</td>
</tr>
<tr>
<td>action</td>
<td>Determines the action that corresponds to the preceding match statement.</td>
</tr>
<tr>
<td>default-action</td>
<td>Action to take for any entity that is not matched in any sequence of the policy. By default, the action is set to reject.</td>
</tr>
</tbody>
</table>

The following configuration shows the components of the Cisco vSmart Controller policy definition. These items are listed in the logical order you should use when designing policy, and this order is also how the items are displayed in the configuration, regardless of the order in which you add them to the configuration.

```plaintext
policy
  policy-type name
  vpn-list vpn-list
  sequence number
  match
    <route | tloc vpn | other>
  !
  action <accept reject drop>
  set attribute value
  !
  default-action <reject accept>
  !
  !
```

Policy Application

The following are the configuration components:
**Component** | **Usage**
--- | ---
**site-list** | Determines the sites to which a given policy is applies. The direction *(in | out)* applies only to control-policy.

**policy-type** | The policy type can be **control-policy**, **data-policy**, or **vpn-membership**—and name refer to an already configured policy to be applied to the sites specified in the site-list for the section.

For a policy definition to take effect, you associate it with sites in the overlay network.

```
apply-policy
  site-list name
  control-policy name <inout>
  site-list name
  data-policy name
  vpn-membership name

Policy Example
```

For a complete policy, which consists of lists, policy definition, and policy application. The example illustrated below creates two lists (a site-list and a tloc-list), defines one policy (a control policy), and applies the policy to the site-list. In the figure, the items are listed as they are presented in the node configuration. In a normal configuration process, you create lists first (group together all the things you want to use), then define the policy itself (define what things you want to do), and finally apply the policy (specify the sites that the configured policy affects).

```
apply-policy
  site-list sitel --------> Apply the defined policy towards the sites in site-list
  control-policy prefer_local out
  policy
    lists
    site-list sitel
      site-id 100
    tloc-list prefer_site1 ---- Define the lists required for apply-policy and for use within
      the policy
      tloc 192.0.2.1 color mols encap ipsec preference 400
      control-policy prefer_local
      sequence 10
      match route
        site-list sitele ------>Lists previously defined used within policy
      !
    action accept
    set
      tloc-list prefer_site
      !
  !
```

**TLOC Attributes Used in Policies**

A transport location, or TLOC, defines a specific interface in the overlay network. Each TLOC consists of a set of attributes that are exchanged in OMP updates among the Cisco SD-WAN devices. Each TLOC is
uniquely identified by a 3-tuple of IP address, color, and encapsulation. Other attributes can be associated with a TLOC.

The TLOC attributes listed below can be matched or set in Cisco vSmart Controller policies.

**Table 4:**

<table>
<thead>
<tr>
<th>TLOC Attribute</th>
<th>Function</th>
<th>Application Point Set By</th>
<th>Application Point Modify By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address (IP address)</td>
<td>system-ip address of the source device on which the interface is located.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Carrier</td>
<td>Identifier of the carrier type. It primarily indicates whether the transport is public or private.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Color</td>
<td>Identifier of the TLOC type.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Identifier of the overlay network domain.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Tunnel encapsulation, either IPsec or GRE.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Originator</td>
<td>system-ip address of originating node.</td>
<td>Configuration on any originator</td>
<td>control-policy</td>
</tr>
<tr>
<td>Preference</td>
<td>OMP path-selection preference. A higher value is a more preferred path.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Site ID</td>
<td>Identification for a give site. A site can have multiple nodes or TLOCs.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Tag</td>
<td>Identifier of TLOC on any arbitrary basis.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
</tbody>
</table>

**vRoute Attributes Used in Policies**

A Cisco SD-WAN route, or vRoute, defines a route in the overlay network. A vRoute, which is similar to a standard IP route, has a number attributes such as TLOC and VPN. The Cisco IOS XE SD-WAN devices exchange vRoutes in OMP updates.

The vRoutes attributes listed below can be matched or set in Cisco vSmart Controller policies.
### Design Cisco vSmart Controller Policy Processing and Application

Understanding how a Cisco vSmart Controller policy is processed and applied allows for proper design of policy and evaluation of how policy is implemented across the overlay network.

Policy is processed as follows:

- A policy definition consists of a numbered, ordered sequence of match–action pairings. Within each policy, the pairings are processed in sequential order, starting with the lowest number and incrementing.
- As soon as a match occurs, the matched entity is subject to the configured action of the sequence and is then no longer subject to continued processing.
- Any entity not matched in a sequence is subject to the default action for the policy. By default, this action is reject.

Cisco vSmart Controller policy is applied on a per-site-list basis, so:

- When applying policy to a site-list, you can apply only one of each type of policy. For example, you can have one control-policy and one data-policy, or one control-policy in and one control-policy out. You cannot have two data policies or two outbound control policies.

### Table 5

<table>
<thead>
<tr>
<th>vRoute Attribute</th>
<th>Function</th>
<th>Application Point Set By</th>
<th>Application Point Modify By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Source of the route, either BGP, OSPF, connected, static.</td>
<td>Source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Originator</td>
<td>Source of the update carrying the route.</td>
<td>Any originator</td>
<td>control-policy</td>
</tr>
<tr>
<td>Preference</td>
<td>OMP path-selection preference. A higher value is a more preferred path.</td>
<td>Configuration on source device or policy</td>
<td>control-policy</td>
</tr>
<tr>
<td>Service</td>
<td>Advertised service associated with the vRoute.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Site ID</td>
<td>Identifier for a give site. A site can have multiple nodes or TLOCs.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>Tag</td>
<td>Identification on any arbitrary basis.</td>
<td>Configuration on source device</td>
<td>control-policy</td>
</tr>
<tr>
<td>TLOC</td>
<td>TLOC used as next hop for the vRoute.</td>
<td>Configuration on source device or policy</td>
<td>control-policy or data-policy</td>
</tr>
<tr>
<td>VPN</td>
<td>VPN to which the vRoute belongs.</td>
<td>Configuration on source device or policy</td>
<td>control-policy or data-policy</td>
</tr>
</tbody>
</table>
• Because a site-list is a grouping of many sites, you should be careful about including a site in more than one site-list. When the site-list includes a range of site identifiers, ensure that there is no overlap. If the same site is part of two site-lists and the same type of policy is applied to both site-lists, the policy behavior is unpredictable and possibly catastrophic.

• Control-policy is unidirectional, being applied either inbound to the vSmart controller or outbound from it. When control-policy is needed in both directions, configure two control policies.

• Data-policy is bidirectional and can be applied either to traffic received from the service side of the Cisco IOS XE SD-WAN device, traffic received from the tunnel side, or all of these combinations.

• VPN membership policy is always applied to traffic outbound from the Cisco vSmart Controller.

• Control-policy remains on the Cisco vSmart Controller and affects routes that the controller sends and receives.

• Data-policy is sent to either the Cisco IOS XE SD-WAN devices in the site-list. The policy is sent in OMP updates, and it affects the data traffic that the devices send and receive.

• When any node in the overlay network makes a routing decision, it uses any and all available routing information. In the overlay network, it is the Cisco vSmart Controller that distributes routing information to the Cisco IOS XE SD-WAN device nodes.

• In a network deployment that has two or more Cisco vSmart Controllers, each controller acts independently to disseminate routing information to other Cisco vSmart Controllers and to Cisco IOS XE SD-WAN devices in the overlay network. So, to ensure that the Cisco vSmart Controller policy has the desired effect in the overlay network, each Cisco vSmart Controller must be configured with the same policy, and the policy must be applied identically. For any given policy, you must configure the identical policy and apply it identically across all the Cisco vSmart Controllers.

---

**Note**  
When you deploy a policy, the deployment status is updated only for 30 minutes, which is the timeout limit for policies. After the timeout period, the deployment task status is not monitored. If you are deploying a bigger policy with more number of lines, and if it takes more than 30 minutes, the task status will not be monitored.

---

**Cisco vSmart Policy Operation**

At a high level, control policy operates on routing information, which in the Cisco IOS XE SD-WAN network is carried in OMP updates. Data policy affects data traffic, and VPN membership controls the distribution of VPN routing tables.

The basic Cisco vSmart policies are:

• Control Policy

• Data Policy

• VPN Membership
Control Policy

Control policy, which is similar to standard routing policy, operates on routes and routing information in the control plane of the overlay network. Centralized control policy, which is provisioned on the Cisco vSmart Controller, is the Cisco SD-WAN technique for customizing network-wide routing decisions that determine or influence routing paths through the overlay network. Local control policy, which is provisioned on a Cisco IOS XE SD-WAN device, allows customization of routing decisions made by BGP and OSPF on site-local branch or enterprise networks.

The routing information that forms the basis of centralized control policy is carried in Cisco IOS XE SD-WAN route advertisements, which are transmitted on the DTLS or TLS control connections between Cisco vSmart Controllers and Cisco IOS XE SD-WAN devices. Centralized control policy determines which routes and route information are placed into the centralized route table on the Cisco vSmart Controller and which routes and route information are advertised to the Cisco IOS XE SD-WAN devices in the overlay network. Basic centralized control policy establish traffic engineering, to set the path that traffic takes through the network. Advanced control policy supports a number of features, which allows Cisco IOS XE SD-WAN devices in the overlay network to share network services, such as firewalls and load balancers.

Centralized control policy affects the OMP routes that are distributed by the Cisco vSmart Controller throughout the overlay network. The Cisco vSmart Controller learns the overlay network topology from OMP routes that are advertised by the Cisco IOS XE SD-WAN devices over the OMP sessions inside the DTLS or TLS connections between the Cisco vSmart Controller and the devices.

Three types of OMP routes carry the information that the Cisco vSmart Controller uses to determine the network topology:

- Cisco SD-WAN OMP routes, which are similar to IP route advertisements, advertise routing information that the devices have learned from their local site and the local routing protocols (BGP and OSPF) to the Cisco vSmart Controller. These routes are also referred to as OMP routes or vRoutes.

- TLOC routes carry overlay network–specific locator properties, including the IP address of the interface that connects to the transport network, a link color, which identifies a traffic flow, and the encapsulation type. (A TLOC, or transport location, is the physical location where a Cisco IOS XE SD-WAN device connects to a transport network. It is identified primarily by IP address, link color, and encapsulation, but a number of other properties are associated with a TLOC.)

- Service routes advertise the network services, such as firewalls, available to VPN members at the local site.

By default, no centralized control policy is provisioned. In this bare, unpolicied network, all OMP routes are placed in the Cisco vSmart Controller’s route table as is, and the Cisco vSmart Controller advertises all OMP routes, as is, to all the devices in the same VPN in the network domain.

By provisioning centralized control policy, you can affect which OMP routes are placed in the Cisco vSmart Controller's route table, what route information is advertised to the devices, and whether the OMP routes are modified before being put into the route table or before being advertised.
Cisco IOS XE SD-WAN devices place all the route information learned from the Cisco vSmart Controllers, as is, into their local route tables, for use when forwarding data traffic. Because the Cisco vSmart Controller’s role is to be the centralized routing system in the network, Cisco IOS XE SD-WAN devices can never modify the OMP route information that they learn from the Cisco vSmart Controllers.

The Cisco vSmart Controller regularly receives OMP route advertisements from the devices and, after recalculating and updating the routing paths through the overlay network, it advertises new routing information to the devices.

The centralized control policy that you provision on the Cisco vSmart Controller remains on the Cisco vSmart Controller and is never downloaded to the devices. However, the routing decisions that result from centralized control policy are passed to the devices in the form of route advertisements, and so the affect of the control policy is reflected in how the devices direct data traffic to its destination.

Localized control policy, which is provisioned locally on the devices, is called route policy. This policy is similar to the routing policies that you configure on a regular driver, allowing you to modify the BGP and OSPF routing behavior on the site-local network. Whereas centralized control policy affects the routing behavior across the entire overlay network, route policy applies only to routing at the local branch.

The Cisco IOS XE SD-WAN devices periodically exchange OMP updates, which carry routing information pertaining to the overlay network. Two of the things that these updates contain are vRoute attributes and Transport Locations (TLOC) attributes.

The Cisco vSmart Controller uses these attributes from the OMP updates to determine the topology and status of the overlay network, and installs routing information about the overlay network into its route table. The controller then advertises the overlay topology to the Cisco IOS XE SD-WAN devices in the network by sending OMP updates to them.

Control policy examines the vRoute and TLOC attributes carried in OMP updates and can modify attributes that match the policy. Any changes that results from control policy are applied directionally, either inbound or outbound.

The figure shows a control-policy named prefer_local that is configured on a Cisco vSmart Controller and that is applied to Site 1 (via site-list list1) and to Site 2 (via site-list list2).

Figure 8: Control Policy Topology

The upper left arrow shows that the policy is applied to Site 1—more specifically, to site-list list1, which contains an entry for Site 1. The command control-policy prefer_local in is used to apply the policy to OMP updates that are coming in to the Cisco vSmart Controller from the Cisco IOS XE SD-WAN device, which is inbound from the perspective of the controller. The in keyword indicates an inbound policy. So, for all OMP updates that the Site 1 devices send to the Cisco vSmart Controller, the "prefer_local" control policy is
applied before the updates reach the route table on the Cisco vSmart Controller. If any vRoute or TLOC attributes in an OMP update match the policy, any changes that result from the policy actions occur before the Cisco vSmart Controller installs the OMP update information into its route table.

The route table on the Cisco vSmart Controller is used to determine the topology of the overlay network. The Cisco vSmart Controller then distributes this topology information, again via OMP updates, to all the devices in the network. Because applying policy in the inbound direction influences the information available to the Cisco vSmart Controller. It determines the network topology and network reachability, modifying vRoute and TLOC attributes before they are placed in the controller’s route table.

```
apPLY-POLICY
Site-list list2
Control-Policy prefer_local out
```

On the right side of the figure above, the "prefer_local" policy is applied to Site 2 via the control-policy prefer_local out command. The out keyword in the command indicates an outbound policy, which means that the policy is applied to OMP updates that the Cisco vSmart Controller is sending to the devices at Site 2. Any changes that result from the policy occur, after the information from the Cisco vSmart Controller's route table is placed in to an OMP update and before the devices receive the update. Again, note that the direction is outbound from the perspective of the Cisco vSmart Controller.

In contrast to an inbound policy, which affects the centralized route table on the Cisco vSmart Controller and has a broad effect on the route attributes advertised to all the devices in the overlay network. A control policy applied in the outbound direction influences only the route tables on the individual devices included in the site-list.

The same control policy (the prefer_local policy) is applied to both the inbound and outbound OMP updates. However, the effects of applying the same policy to inbound and outbound are different. The usage shown in the figure illustrates the flexibility of the Cisco IOS XE SD-WAN control policy design architecture and configuration.

**Data Policy**

Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between Cisco IOS XE SD-WAN devices, shown in purple in the adjacent figure.

The Cisco IOS XE SD-WAN architecture implements two types of data policy:

- Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the Cisco vSmart controller, and they affect traffic flow across the entire network.

- Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a Cisco IOS XE SD-WAN device. This type of data policy is provisioned locally using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.
By default, no centralized data policy is provisioned. The result is that all prefixes within a VPN are reachable from anywhere in the VPN. Provisioning centralized data policy allows you to apply a 6-tuple filter that controls access between sources and destinations.

As with centralized control policy, you provision a centralized data policy on the Cisco vSmart Controller, and that configuration remains on the Cisco vSmart Controller. The effects of data policy are reflected in how the Cisco IOS XE SD-WAN devices direct data traffic to its destination. Unlike control policy, however, centralized data polices are pushed to the devices in a read-only fashion. They are not added to the router's configuration file, but you can view them from the CLI on the router.

With no access lists provisioned on a Cisco IOS XE SD-WAN device, all data traffic is transmitted at line rate and with equal importance, using one of the interface's queues. Using access lists, you can provision class of service, which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. You can provision policing.

Data policy examines fields in the headers of data packets, looking at the source and destination addresses and ports, and the protocol and DSCP values, and for matching packets, it can modify the next hop in a variety of ways or apply a policer to the packets. Data policy is configured and applied on the Cisco vSmart Controller, and then it is carried in OMP updates to the Cisco IOS XE SD-WAN devices in the site-list that the policy is applied to. The match operation and any resultant actions are performed on the devices as it transmits or receives data traffic.

In the Data Policy Topology figure, a data policy named “change_next_hop” is applied to a list of sites that includes Site 3. The OMP update that the vSmart controller sends to the devices at Site 3 includes this policy definition. When the device sends or receives data traffic that matches the policy, it changes the next hop to the specified TLOC. Nonmatching traffic is forwarded to the original next-hop TLOC.
In the **apply-policy** command for a data policy, specify a direction from the perspective of the device. The "all" direction in the figure applies the policy to incoming and outgoing data traffic transiting the tunnel interface. You can limit the span of the policy to only incoming traffic with a **data-policy change_next_hop from-tunnel** command or to only outgoing traffic with a **data-policy change_next_hop from-service** command.

### VPN Membership Policy Operation

VPN membership policy, as the name implies, affects the VPN route tables that are distributed to particular Cisco IOS XE SD-WAN devices. In an overlay network with no VPN membership policy, the Cisco vSmart Controller pushes the routes for all VPNs to all the devices. If your business usage model restricts participation of specific devices in particular VPNs, a VPN membership policy is used to enforce this restriction.

The figure VPN Membership Topology illustrates how VPN membership policy works. This topology has three Cisco IOS XE SD-WAN devices:

- The Cisco IOS XE SD-WAN devices at Sites 1 and 2 service only VPN 2.
- The Cisco IOS XE SD-WAN devices at Site 3 service both VPN 1 and VPN 2.

In the figure, the device at Site 3 receives all route updates from the Cisco vSmart Controller, because these updates are for both VPN 1 and VPN 2. However, because the other Cisco IOS XE SD-WAN devices service only VPN 2, it can filter the route updates sent to them, remove the routes associated with VPN 1 and sends only the ones that apply to VPN 2.
Notice that here, direction is not set when applying VPN membership policy. The Cisco vSmart Controller always applies this type of policy to the OMP updates that it sends outside to the Cisco IOS XE SD-WAN devices.

Configure and Execute Cisco vSmart Policies

All Cisco vSmart Controller policies are configured on the Cisco IOS XE SD-WAN devices, using a combination of policy definition and lists. All Cisco vSmart Controller policies are also applied on the Cisco IOS XE SD-WAN devices, with a combination of apply-policy and lists. However, where the actual Cisco vSmart Controller policy executes depends on the type of policy, as shown in this figure:

For control policy and VPN membership policy, the entire policy configuration remains on the Cisco vSmart Controller, and the actions taken as a result of routes or VPNs that match a policy are performed on the Cisco vSmart Controller.

For the other three policy types—application-aware routing, cflowd templates, and data policy—the policies are transmitted in OMP updates to the Cisco IOS XE SD-WAN devices, and any actions taken as a result of the policies are performed on the devices.
Centralized Policy

The topics in this section provide overview information about the different types of centralized policies, the components of centralized policies, and how to configure centralized policies using Cisco vManage or the CLI.

• Overview of Centralized Policies, on page 27
• Configure Centralized Policies Using Cisco vManage, on page 28
• Configure Centralized Policies Using the CLI, on page 58
• Centralized Policies Configuration Examples, on page 61

Overview of Centralized Policies

Centralized policies refer to policies that are provisioned on Cisco vSmart Controllers, which are the centralized controllers in the Cisco SD-WAN overlay network.

Types of Centralized Policies

Centralized Control Policy

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the Cisco vSmart Controller's route table and that is advertised to the Cisco IOS XE SD-WAN devices. The effects of centralized control policy are seen in how Cisco IOS XE SD-WAN devices direct the overlay network's data traffic to its destination.

Note The centralized control policy configuration itself remains on the Cisco vSmart Controller and is never pushed to local devices.

Centralized Data Policy

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the selected Cisco IOS XE SD-WAN devices.
Centralized Data Policy Based on Packet Header Fields

Policy decisions affecting data traffic can be based on the packet header fields, specifically, on the source and destination IP prefixes, the source and destination IP ports, the protocol, and the DSCP.

This type of policy is often used to modify traffic flow in the network. Here are some examples of the types of control that can be effected with a centralized data policy:

- Which set of sources are allowed to send traffic to any destination outside the local site. For example, local sources that are rejected by such a data policy can communicate only with hosts on the local network.
- Which set of sources are allowed to send traffic to a specific set of destinations outside the local site. For example, local sources that match this type of data policy can send voice traffic over one path and data traffic over another.
- Which source addresses and source ports are allowed to send traffic to any destination outside the local site or to a specific port at a specific destination.

Configure Centralized Policies Using Cisco vManage

To configure a centralized policy, use the Cisco vManage policy configuration wizard. The wizard consists of the following operations that guide you through the process of creating and editing policy components:

- Create Groups of Interest: Create lists that group together related items and that you call in the match or action components of a policy.
- Configure Topology and VPN Membership: Create the network structure to which the policy applies.
- Configure Traffic Rules: Create the match and action conditions of a policy.
- Apply Policies to Sites and VPNs: Associate the policy with sites and VPNs in the overlay network.
- Activate the centralized policy.

For a centralized policy to take effect, you must activate the policy.

To configure centralized policies using Cisco vManage, use the steps identified in the procedures that follow this section.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Centralized Policy.
3. Click Add Policy.

The policy configuration wizard appears, and the Create Groups of Interest window is displayed.

Configure Groups of Interest for Centralized Policy

In Create Groups of Interest, create new groups of list types as described in the following sections to use in a centralized policy:
**Configure Application**

1. In the groups of interest list, click **Application** list type.

2. Click **New Application List**.

3. Enter a name for the list.

4. Choose either **Application** or **Application Family**.

   **Application** can be the names of one or more applications, such as **Third Party Control**, **ABC News**, **Microsoft Teams** and so on. The Cisco IOS XE SD-WAN devices support about 2300 different applications. To list the supported applications, use the `?` in the CLI.


5. In the **Select** drop-down, in the 'Search' filter, select the required applications or application families.

6. Click **Add**.

A few application lists are preconfigured. You cannot edit or delete these lists.

- Microsoft Apps—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.

- Google Apps—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.

**Configure Color**

1. In the groups of interest list, click **Color**.

2. Click **New Color List**.

3. Enter a name for the list.

4. From the **Select Color** drop-down, in the 'Search' filter select the required colors.

   Colors can be: 3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver.

5. Click **Add**.

To configure multiple colors in a single list, you can select multiple colors from the drop-down.
Configure Community

**Table 6: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to Match and Set Communities</td>
<td>Cisco SD-WAN Release 20.5.1</td>
<td>This feature lets you match and set communities using a control policy. Control policies are defined and applied on Cisco IOS XE SD-WAN device devices to manipulate communities. With this feature, you can match and assign single or multiple BGP community tags to your prefixes based on which routing policies can be manipulated.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 17.5.1a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.5.1</td>
<td></td>
</tr>
</tbody>
</table>

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. Choose either **Standard** or **Expanded**.
   - Standard community lists are used to specify communities and community numbers.
   - Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes.
5. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - **aa:nn**: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices.
   - **local-as**: Routes in this community are not advertised outside the local AS number.
   - **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
   - **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
6. Click **Add**.

**Configure Data Prefix**

1. In the **Groups of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
5. In the **Add Data Prefix** field, enter one or more data prefixes separated by commas.
6. Click **Add**.

**Configure Policer**
1. In the groups of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. Define the policing parameters:
   a. In the **Burst** field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.
   b. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. It can be **drop**, which sets the packet loss priority (PLP) to **low**.
      You can use the **remark** action to set the packet loss priority (PLP) to **high**.
   c. In the **Rate** field, enter the maximum traffic rate, a value from 0 through $2^{64} - 1$ bits per second (bps).
5. Click **Add**.

**Configure Prefix**
1. In the groups of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Add Prefix** field, enter one or more data prefixes separated by commas.
5. Click **Add**.

**Configure Site**
1. In the groups of interest list, click **Site**.
2. Click **New Site List**.
3. Enter a name for the list.
4. In the **Add Site** field, enter one or more site IDs separated by commas.
   For example, 100 or 200 separated by commas or in the range, 1- 4294967295.
5. Click **Add**.
Configure App Probe Class

1. In the groups of interest list, click **App Probe Class**.
2. Click **New App Probe Class**.
3. Enter the probe class name in the **Probe Class Name** field.
4. Select the required forwarding class from the **Forwarding Class** drop-down list.
5. In the **Entries** pane, select the appropriate color from the **Color** drop-down list and enter the **DSCP** value.
   You can add more entries if needed by clicking on **+** symbol.
6. Click **Save**.

Configure SLA Class

1. In the groups of interest list, click **SLA Class**.
2. Click **New SLA Class List**.
3. Enter a name for the list.
4. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Select the required app probe class from the **App Probe Class** drop-down list.
5. (Optional) Select the **Fallback Best Tunnel** checkbox to enable the best tunnel criteria.
   This optional file is available from Cisco IOS XE Release 17.5.1a to pick the best path or color from the available colors when SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and, jitter values.
6. Select the **Criteria** from the drop-down list. The available criteria are:
   - Latency
   - Loss
   - Jitter
   - Latency, Loss
   - Latency, Jitter
   - Loss, Latency
   - Loss, Jitter
   - Jitter, Latency
• Jitter, Loss
• Latency, Loss, Jitter
• Latency, Jitter, Loss
• Loss, Latency, Jitter
• Loss, Jitter, Latency
• Jitter, Latency, Loss
• Jitter, Loss, Latency

7. Enter the Loss Variance (%), Latency Variance (ms), and the Jitter Variance (ms) for the selected criteria.

8. Click Add.

**Configure TLOC**

1. In the groups of interest list, click TLOC.
2. Click New TLOC List. The TLOC List popup displays.
3. Enter a name for the list.
4. In the TLOC IP field, enter the system IP address for the TLOC.
5. In the Color field, select the TLOC's color.
6. In the Encap field, select the encapsulation type.
7. In the Preference field, optionally select a preference to associate with the TLOC.
   The range is 0 to 4294967295.
8. Click Add TLOC to add another TLOC to the list.
9. Click Save.

**Note**

To use the set tloc and set tloc-list commands, you must use the set-vpn command.

For each TLOC, specify its address, color, and encapsulation. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

**Configure VPN**

1. In the groups of interest list, click VPN.
2. Click New VPN List.
3. Enter a name for the list.
4. In the **Add VPN** field, enter one or more VPN IDs separated by commas. For example, 100 or 200 separated by commas or in the range, 1-65530.

5. Click **Add**.

**Configure Region**

Minimum release: Cisco vManage Release 20.7.1

To configure a list of regions for Hierarchical SD-WAN, ensure that Hierarchical SD-WAN is enabled in **Administration > Settings**.

1. In the groups of interest list, click **Region**.

2. Click **New Region List**.

3. In the **Region List Name** field, enter a name for the region list.

4. In the **Add Region** field, enter one or more regions, separated by commas, or enter a range.
   For example, specify regions 1, 3 with commas, or a range 1-4.

5. Click **Add**.

Click **Next** to move to **Configure Topology and VPN Membership** in the wizard.

**Configure Topology and VPN Membership**

When you first open the **Configure Topology and VPN Membership** window, the **Topology** window is displayed by default.

To configure topology and VPN membership:

**Hub-and-Spoke**

1. In the **Add Topology** drop-down, select **Hub-and-Spoke**.

2. Enter a name for the hub-and-spoke policy.

3. Enter a description for the policy.

4. In the **VPN List** field, select the VPN list for the policy.

5. In the left pane, click **Add Hub-and-Spoke**. A hub-and-spoke policy component containing the text string **My Hub-and-Spoke** is added in the left pane.

6. Double-click the **My Hub-and-Spoke** text string, and enter a name for the policy component.

7. In the right pane, add hub sites to the network topology:
   a. Click **Add Hub Sites**.
   b. In the **Site List** field, select a site list for the policy component.
   c. Click **Add**.
   d. Repeat these steps to add more hub sites to the policy component.

8. In the right pane, add spoke sites to the network topology:
a. Click Add Spoke Sites.
b. In the Site List Field, select a site list for the policy component.
c. Click Add.
d. Repeat these steps to add more spoke sites to the policy component.

9. Repeat steps as needed to add more components to the hub-and-spoke policy.
10. Click Save Hub-and-Spoke Policy.

Mesh
1. In the Add Topology drop-down, select Mesh.
2. Enter a name for the mesh region policy component.
3. Enter a description for the mesh region policy component.
4. In the VPN List field, select the VPN list for the policy.
5. Click New Mesh Region.
6. In the Mesh Region Name field, enter a name for the individual mesh region.
7. In the Site List field, select one or more sites to include in the mesh region.
8. Click Add.
9. Repeat these steps to add more mesh regions to the policy.
10. Click Save Mesh Topology.

Custom Control (Route & TLOC): Centralized route control policy (for matching OMP routes)
1. In the Add Topology drop-down, select Custom Control (Route & TLOC).
2. Enter a name for the control policy.
3. Enter a description for the policy.
4. In the left pane, click Sequence Type. The Add Custom Control Policy popup displays.
5. Select Route. A policy component containing the text string Route is added in the left pane.
6. Double-click the Route text string, and enter a name for the policy component.
7. In the right pane, click Sequence Rule. The Match/Actions box opens, and Match is selected by default.
8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired.
9. Click Actions. The Reject option is selected by default. To configure actions to perform on accepted packets, click the Accept option. Then select the action or enter a value for the action.
10. Click Save Match and Actions.
11. Click Sequence Rule to configure more sequence rules, as desired. Drag and drop to re-order them.
12. Click Sequence Type to configure more sequences, as desired. Drag and drop to re-order them.
13. Click Save Control Policy.

**Custom Control (Route & TLOC):** Centralized TLOC control policy (for matching TLOC routes)

1. In the Add Topology drop-down, select Custom Control (Route & TLOC).
2. Enter a name for the control policy.
3. Enter a description for the policy.
4. In the left pane, click Sequence Type. The Add Custom Control Policy popup displays.
5. Select TLOC. A policy component containing the text string TLOC is added in the left pane.
6. Double-click the TLOC text string, and enter a name for the policy component.
7. In the right pane, click Sequence Rule. The Match/Actions box opens, and Match is selected by default.
8. From the boxes under the Match box, select the desired policy match type. Then select or enter the value for that match condition. Configure additional match conditions for the sequence rule, as desired.
9. Click Actions. The Reject option is selected by default. To configure actions to perform on accepted packets, click the Accept option. Then select the action or enter a value for the action.
10. Click Save Match and Actions.
11. Click Sequence Rule to configure more sequence rules, as desired. Drag and drop to re-order them.
12. Click Sequence Type to configure more sequences, as desired. Drag and drop to re-order them.
13. Click Save Control Policy.

A centralized control policy contains sequences of match–action pairs. The sequences are numbered to set the order in which a route or TLOC is analyzed by the match–action pairs in the policy.

---

**Note**

Sequence can have either **match app-list** or **dns-app-list** configured for a policy, but not both. Configuring both **match app-list** and **dns-app-list** for a policy is not supported.

---

Each sequence in a centralized control policy can contain one match condition (either for a route or for a TLOC) and one action condition.

**Default Action**

If a selected route or TLOC does not match any of the match conditions in a centralized control policy, a default action is applied to it. By default, the route or TLOC is rejected.

If a selected data packet does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

---

**Import Existing Topology**

1. In the Add Topology drop-down, click **Import Existing Topology**. The **Import Existing Topology** popup appears.
2. Select the type of topology.
3. For **Policy Type**, choose the name of the topology you want to import.

4. In the **Policy** drop-down, select a policy to import.

   **Note** The policy configuration wizard does not let you import an already configured policy as in other instances of centralized policies (data, control, or application-aware routing). The policy must be configured in its entirety.

5. Click **Import**.

Click Next to move to **Configure Traffic Rules** in the wizard.

**Create a VPN Membership Policy**

1. In the **Specify your network topology** area, click **VPN Membership**.

2. Click **Add VPN Membership Policy**.

   **Note** You can add only one VPN membership at a time, therefore all site lists and VPN lists must be included in a single policy.

   The **Add VPN Membership Policy** popup displays.

3. Enter a name and description for the VPN membership policy.

4. In the **Site List** field, select the site list.

5. In the **VPN Lists** field, select the VPN list.

6. Click **Add List** to add another VPN to the VPN membership.

7. Click **Save**.

8. Click Next to move to **Configure Traffic Rules** in the wizard.

**Configure Traffic Rules**

*Table 7: Feature History*

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Matching with ICMP Message</td>
<td>Cisco IOS XE Release 17.4.1</td>
<td>This feature provides support for a new match condition that you can use to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.4.1</td>
<td></td>
</tr>
</tbody>
</table>

When you first open the **Configure Traffic Rules** window, **Application-Aware Routing** is selected by default.
You can also view already created AAR routing policies listed in the page. It provides various information related to the policies such as the Name of the policy, Type, Mode, Description, Update By, and Last Updated details.

---

**Note**

You can refer to Mode column for the security status details of the policy. The status helps to differentiate whether the policy is used in unified security or not.

For more information on configuring traffic rules for the SD-WAN Application Intelligence Engine (SAIE) flow, see [SD-WAN Application Intelligence Engine Flow](#).

---

**Note**

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

To configure traffic rules for a centralized data policy:

1. Click **Traffic Data**.
2. Click the **Add Policy** drop-down.
3. Click **Create New**. The **Add Data Policy** window displays.
4. Enter a name and a description for the data policy.
5. In the right pane, click **Sequence Type**. The **Add Data Policy** popup opens.
6. Select the type of data policy you want to create, **Application Firewall**, **QoS**, **Traffic Engineering**, or **Custom**.

---

**Note**

If you want to configure multiple types of data policies for the same match condition, you need to configure a custom policy.

7. A policy sequence containing the text string **Application, Firewall, QoS, Traffic Engineering**, or **Custom** is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.
9. In the right pane, click **Sequence Rule**. The **Match/Action** box opens, and **Match** is selected by default. The available policy match conditions are listed below the box.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all packets)</td>
<td>Do not specify any match conditions.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Procedure</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Applications/Application Family List    | a. In the Match conditions, click **Applications/Application Family List**.  
b. In the drop-down, select the application family.  
c. To create an application list:  
  1. Click **New Application List**.  
  2. Enter a name for the list.  
  3. Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications.  
  4. In the **Select Application** drop-down, select the desired applications or application families.  
  5. Click **Save**.  |
| Destination Data Prefix                 | a. In the Match conditions, click **Destination Data Prefix**.  
b. To match a list of destination prefixes, select the list from the drop-down.  
c. To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.  |
| Destination Port                       | a. In the Match conditions, click **Destination Port**.  
b. In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).  |
| DNS Application List                   | Add an application list to enable split DNS.  
a. In the Match conditions, click **DNS Application List**.  
b. In the drop-down, select the application family.  |
| DNS                                    | Add an application list to process split DNS.  
a. In the Match conditions, click **DNS**.  
b. In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications.  |
| DSCP                                   | a. In the Match conditions, click **DSCP**.  
b. In the **DSCP** field, type the DSCP value, a number from 0 through 63.  |
| Packet Length                          | a. In the Match conditions, click **Packet Length**.  
b. In the **Packet Length** field, type the length, a value from 0 through 65535.  |
**Match Condition** | **Procedure**
--- | ---
**PLP** | a. In the **Match** conditions, click **PLP** to set the **Packet Loss Priority**.  
  b. In the **PLP** drop-down, select **Low** or **High**. To set the PLP to **High**, apply a policer that includes the **exceed remark** option.

**Protocol** | a. In the **Match** conditions, click **Protocol**.  
  b. In the **Protocol** field, type the Internet Protocol number, a number from 0 through 255.

**ICMP Message** | To match ICMP messages, in the **Protocol** field, set the Internet Protocol Number to 1, or 58, or both.

  **Note** This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.

**Source Data Prefix** | a. In the **Match** conditions, click **Source Data Prefix**.  
  b. To match a list of source prefixes, select the list from the drop-down.  
  c. To match an individual source prefix, enter the prefix in the **Source** field.

**Source Port** | a. In the **Match** conditions, click **Source Port**.  
  b. In the **Source** field, enter the port number. Specify as a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with numbers separated with a hyphen [-]).

**TCP** | a. In the **Match** conditions, click **TCP**.  
  b. In the **TCP** field, **syn** is the only option available.

10. For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy to IPv4 and IPv6 address families.

11. To select one or more **Match** conditions, click its box and set the values as described.

  **Note** Not all match conditions are available for all policy sequence types.

12. To select actions to take on matching data traffic, click the **Actions** box.

13. To drop matching traffic, click **Drop**. The available policy actions are listed in the right side.

14. To accept matching traffic, click **Accept**. The available policy actions are listed in the right side.

15. Set the policy action as described.
Not all actions are available for all match conditions.

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Counter          | Count matching data packets. | a. In the **Action** conditions, click **Counter**.  
|                  |             | b. In the **Counter Name** field, enter the name of the file in which to store packet counters. |
| DSCP             | Assign a DSCP value to matching data packets. | a. In the **Action** conditions, click **DSCP**.  
|                  |             | b. In the **DSCP** field, type the DSCP value, a number from 0 through 63. |
| Forwarding Class | Assign a forwarding class to matching data packets. | a. In the **Match** conditions, click **Forwarding Class**.  
|                  |             | b. In the **Forwarding Class** field, type the class value, which can be up to 32 characters long. |
| Log              | Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active. | a. In the **Action** conditions, click **Log** to enable logging. |
| Policer          | Apply a policer to matching data packets. | a. In the **Match** conditions, click **Policer**.  
|                  |             | b. In the **Policer** drop-down field, select the name of a policer. |
| Loss Correction  | Apply loss correction to matching data packets. | a. In the **Match** conditions, click **Loss Correction**.  
|                  | Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data. | b. In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**.  
|                  | FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels. | |
|                  | • **FEC Adaptive** – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. | |
|                  | • **FEC Always** – Corresponding packets are always subjected to FEC. | |
|                  | • **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters. | |
16. Create additional sequence rules as desired. Drag and drop to re-arrange them.

17. Click Save Data Policy.

18. Click Next to move to Apply Policies to Sites and VPNs in the wizard.

**Match Parameters - Control Policy**

For OMP and TLOC routes, you can match the following attributes:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Color List</td>
<td>One or more colors. The available colors are: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver.</td>
</tr>
</tbody>
</table>
| Community List  | List of one or more BGP communities. In the Community List field, you can specify:  
  • *aa:nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535.  
  • *internet*: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices.  
  • *local-as*: Routes in this community are not advertised outside the local AS.  
  • *no-advertise*: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.  
  • *no-export*: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one community in each option. |
<p>| Types           | Specifies the community type. Choose Standard to specify communities and community numbers or, Expanded to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes. |</p>
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria OR</td>
<td>Compares each regex string in the community list against the community string of the route. The OR condition is applicable across multiple community lists and is valid for all devices. Starting from Cisco IOS XE Release 17.5.1a, the Community Types and Criteria fields are available.</td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Tag value associated with the route or prefix in the routing database on the device. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Origin</td>
<td>Protocol from which the route was learned.</td>
</tr>
<tr>
<td>Originator</td>
<td>IP address from which the route was learned.</td>
</tr>
</tbody>
</table>
| Path Type       | In a Hierarchical SD-WAN architecture, match a route by its path type, which can be one of the following:  
  - **Hierarchical Path**: A route that includes hops from an access region to a border router, through region 0, to another border router, then to an edge router in a different access region  
  - **Direct Path**: A direct path route from one edge router to another edge router.  
  - **Transport Gateway Path**: A route that is re-originated by a router that has transport gateway functionality enabled.  
  **Note**: This option is available beginning with Cisco vManage Release 20.8.1. |
| Preference      | How preferred a prefix is. This is the preference value that the route or prefix has in the local site, that is, in the routing database on the device. A higher preference value is more preferred. The range is 0 through 255. |
| Prefix List     | One or more prefixes. Specifies the name of a prefix list. One or more overlay network site identifiers. |
| Not available in Cisco vManage. | Individual site identifier. The range is 0 through 4294967295. |

**Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x**
### Match Condition | Description
--- | ---
**Region** | Region defined for Hierarchical SD-WAN. The range is 1 to 63.  
*Note* This option is available beginning with Cisco vManage Release 20.7.1.

**Role** | In a Hierarchical SD-WAN architecture, match by the device type, which can be **Border Router** or **Edge Router**.  
*Note* This option is available beginning with Cisco vManage Release 20.8.1.

**TLOC** | Individual TLOC address.  
*Note* To use the `set tloc` and `set tloc-list` commands, you must use the `set-vpn` command.

**VPN** | Individual VPN identifier. The range is 0 through 65535.

**Carrier** | Carrier for the control traffic. Values are: default, carrier1 through carrier8.

**Domain ID** | Domain identifier associated with a TLOC. The range is 0 through 4294967295.

**OMP Tag** | Tag value associated with the TLOC route in the route table on the device. The range is 0 through 4294967295.

**Site** | Individual site contributor or more overlay network site identifiers. The range is 0 through 4294967295.

In the CLI, you configure the OMP route attributes to match with the `policy control-policy sequence match route` command, and you configure the TLOC attributes to match with the `policy control-policy sequence match tloc` command.

## Match Parameters - Data Policy

A centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

Each sequence in a policy can contain one match condition.
**Table 8:**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omit</td>
<td>Match all packets.</td>
</tr>
<tr>
<td>Applications/Application Family List</td>
<td>Applications or application families.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>Group of destination prefixes, IP prefix and prefix length. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>DNS Application List</td>
<td>Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an app-list list. This list specifies the applications whose DNS requests are processed.</td>
</tr>
<tr>
<td>DNS</td>
<td>Specify the direction in which to process DNS packets. To process DNS requests sent by the applications (for outbound DNS queries), specify dns request. To process DNS responses returned from DNS servers to the applications, specify dns response.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the DSCP value.</td>
</tr>
<tr>
<td>Packet length</td>
<td>Specifies the packet length. The range is 0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>Packet Loss Priority (PLP)</td>
<td>Specifies the packet loss priority. By default, packets have a PLP value of low. To set the PLP value to high, apply a policer that includes the exceed remark option.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies Internet protocol number. The range is 0 through 255.</td>
</tr>
<tr>
<td>ICMP Message</td>
<td>For Protocol IPv4 when you enter a Protocol value as 1, the ICMP Message field displays where you can select an ICMP message to apply to the data policy. Likewise, the ICMP Message field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the ICMP Message or ICMPv6 Message field displays. <strong>Note</strong> This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1.</td>
</tr>
<tr>
<td>Source Data Prefix</td>
<td>Specifies the group of source prefixes or an individual source prefix.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specifies the source port number. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>TCP Flag</td>
<td>Specifies the TCP flag, syn.</td>
</tr>
<tr>
<td>Traffic To</td>
<td>In a Hierarchical SD-WAN architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. <strong>Note</strong> Minimum release: Cisco vManage Release 20.8.1</td>
</tr>
</tbody>
</table>
### Table 9: ICMP Message Types/Codes and Corresponding Enumeration Values

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Enumeration</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>echo-reply</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>unreachable</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>net-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>host-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>protocol-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>port-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>packet-too-big</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>source-route-failed</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>network-unknown</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>host-unknown</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>host-isolated</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>dod-net-prohibited</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>dod-host-prohibited</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>net-tos-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>host-tos-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>administratively-prohibited</td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td>hostprecedence-unreachable</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>precedence-unreachable</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>redirect</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>net-redirect</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>host-redirect</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>net-tos-redirect</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>host-tos-redirect</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>echo</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>router-advertisement</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>router-solicitation</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>time-exceeded</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>ttl-exceeded</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>reassembly-timeout</td>
</tr>
<tr>
<td>Type</td>
<td>Code</td>
<td>Enumeration</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>unreachable</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>no-route</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>beyond-scope</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>destination-unreachable</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>port-unreachable</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>source-policy</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>reject-route</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>source-route-header</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>packet-too-big</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>time-exceeded</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>reassembly-timeout</td>
</tr>
</tbody>
</table>

Table 10: ICMPv6 Message Types/Codes and Corresponding Enumeration Values
<table>
<thead>
<tr>
<th>Index</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>parameter-problem</td>
</tr>
<tr>
<td>0</td>
<td>Header</td>
</tr>
<tr>
<td>1</td>
<td>next-header</td>
</tr>
<tr>
<td>2</td>
<td>parameter-option</td>
</tr>
<tr>
<td>128</td>
<td>echo-request</td>
</tr>
<tr>
<td>129</td>
<td>echo-reply</td>
</tr>
<tr>
<td>130</td>
<td>mld-query</td>
</tr>
<tr>
<td>131</td>
<td>mld-report</td>
</tr>
<tr>
<td>132</td>
<td>mld-reduction</td>
</tr>
<tr>
<td>133</td>
<td>router-solicitation</td>
</tr>
<tr>
<td>134</td>
<td>router-advertisement</td>
</tr>
<tr>
<td>135</td>
<td>nd-ns</td>
</tr>
<tr>
<td>136</td>
<td>nd-na</td>
</tr>
<tr>
<td>137</td>
<td>redirect</td>
</tr>
<tr>
<td>138</td>
<td>router-renumbering</td>
</tr>
<tr>
<td>0</td>
<td>renum-command</td>
</tr>
<tr>
<td>1</td>
<td>renum-result</td>
</tr>
<tr>
<td>255</td>
<td>renum-seq-number</td>
</tr>
<tr>
<td>139</td>
<td>ni-query</td>
</tr>
<tr>
<td>0</td>
<td>ni-query-v6-address</td>
</tr>
<tr>
<td>1</td>
<td>ni-query-name</td>
</tr>
<tr>
<td>2</td>
<td>ni-query-v4-address</td>
</tr>
<tr>
<td>140</td>
<td>ni-response</td>
</tr>
<tr>
<td>0</td>
<td>ni-response-success</td>
</tr>
<tr>
<td>1</td>
<td>ni-response-refuse</td>
</tr>
<tr>
<td>2</td>
<td>ni-response-qtype-unknown</td>
</tr>
<tr>
<td>141</td>
<td>ind-solicitation</td>
</tr>
<tr>
<td>142</td>
<td>ind-advertisement</td>
</tr>
<tr>
<td>143</td>
<td>mldv2-report</td>
</tr>
<tr>
<td>144</td>
<td>dhaad-request</td>
</tr>
<tr>
<td>145</td>
<td>dhaad-reply</td>
</tr>
<tr>
<td>146</td>
<td>mpd-solicitation</td>
</tr>
<tr>
<td>147</td>
<td>mpd-advertisement</td>
</tr>
</tbody>
</table>
**Action Parameters - Control Policy**

For each match condition, you configure a corresponding action to take if the route or TLOC matches for a control policy.

In the CLI, you configure actions with the `policy control-policy action` command.

Each sequence in a centralized control policy can contain one action condition.

In the action, you first specify whether to accept or reject a matching route or TLOC:

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco vManage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the route. An accepted route is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click <em>Accept</em>.</td>
</tr>
<tr>
<td>Discard the packet.</td>
<td>Click <em>Reject</em>.</td>
</tr>
</tbody>
</table>

Then, for a route or TLOC that is accepted, you can configure the following actions:

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export To</td>
<td>Export the route the the specified VPN or list of VPNs (for a <em>match route</em> match condition only). The range is 0 through 65535 or list name.</td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Change the tag string in the route, prefix, or TLOC. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Preference</td>
<td>Change the preference value in the route, prefix, or TLOC to the specified value. A higher preference value is more preferred. The range is 0 through 255.</td>
</tr>
</tbody>
</table>
### Action Parameters - Data Policy

#### Service
Specify a service to redirect traffic to before delivering the traffic to its destination.

The TLOC address or list of TLOCs identifies the TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.

The VPN identifier is where the service is located.

Standard services: FW, IDS, IDP Custom services: netsvc1, netsvc2, netsvc3, netsvc4

Configure the services themselves on the Cisco IOS XE SD-WAN devices that are collocated with the service devices, using the **vpn service** configuration command.

#### TLOC
Change the TLOC address, color, and encapsulation to the specified address and color.

For each TLOC, specify its address, color, and encapsulation. **address** is the system IP address. **color** can be one of 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver. **encapsulation** can be gre or ipsec. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an **action accept** condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

Set the TLOC action option to enable the Cisco vSmart Controller to perform end-to-end tracking of the path to the ultimate destination device.

#### TLOC Action
Direct matching routes or TLOCs using the mechanism specified by **action**, and enable end-to-end tracking of whether the ultimate destination is reachable.

Setting the TLOC action option enables the Cisco vSmart Controller to perform end-to-end tracking of the path to the ultimate destination device.

---

**Note**

The **preference** command controls the preference for directing inbound and outbound traffic to a tunnel. The preference can be a value from 0 through 4294967295 (232 – 1), and the default value is 0. A higher value is preferred over a lower value.

When a Cisco vEdge device has two or more tunnels, if all the TLOCs have the same preference and no policy is applied that affects traffic flow, all the TLOCs are advertised into OMP. When the router transmits or receives traffic, it distributes traffic flows evenly among the tunnels, using ECMP.

---

### Action Parameters - Data Policy

#### Table 12: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Preference Support for Cisco IOS XE SD-WAN Devices</td>
<td>Cisco IOS XE Release 17.2.1r</td>
<td>This feature extends to Cisco IOS XE SD-WAN devices, support for selecting one or more local transport locators (TLOCs) for a policy action.</td>
</tr>
</tbody>
</table>
With this feature, while creating a data policy, you can define an application list along with other match criteria and redirect the application traffic to a Secure Internet Gateway (SIG).

Next Hop Action Enhancement in Data Policies

This feature enhances match action conditions in a centralized data policy for parity with the features configured on Cisco IOS XE SD-WAN devices. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.

Traffic Redirection to SIG Using Data Policy: Fallback to Routing

With this feature, you can configure internet-bound traffic to be routed through the Cisco SD-WAN overlay, as a fallback mechanism, when all SIG tunnels are down.

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped. Then, you can associate parameters with accepted packets.

In the CLI, you configure the action parameters with the `policy data-policy vpn-list sequence action` command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Accept</td>
<td>Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
</tr>
<tr>
<td>Cflowd</td>
<td>Enables cflowd traffic monitoring.</td>
</tr>
<tr>
<td>Counter</td>
<td>Counts the accepted or dropped packets. Specifies the name of a counter. Use the <code>show policy access-lists counters</code> command on the Cisco IOS XE SD-WAN device.</td>
</tr>
<tr>
<td>Click Drop</td>
<td>Discards the packet. This is the default action.</td>
</tr>
<tr>
<td>Log</td>
<td>Logs the packet. Packets are placed into the messages and syslog system logging (syslog) files. To view the packet logs, use the <code>show app log flows</code> and <code>show log</code> commands.</td>
</tr>
<tr>
<td>Action Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Redirect DNS</td>
<td>Redirects DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions. For an inbound policy, <code>redirect-dns host</code> allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server. <strong>Note</strong> When you upgrade to releases later than Cisco IOS XE Release 17.7.1a, you must configure redirect DNS through <code>nat use-vpn 0</code> to redirect DNS to Direct Internet Interface (DIA). <strong>Note</strong> You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC.</td>
</tr>
<tr>
<td>TCP Optimization</td>
<td>Fine-tune TCP to decrease round-trip latency and improve throughout for matching TCP traffic.</td>
</tr>
</tbody>
</table>
| Secure Internet Gateway | Redirect application traffic to a SIG  
**Note** Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see [Automatic Tunnels](#). For more information on configuring Manual SIG tunnels, see [Manual Tunnels](#).  
Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down. This option is introduced in Cisco IOS XE Release 17.8.1, Cisco vManage Release 20.8.1. |

---

**Note** On Cisco IOS XE SD-WAN devices, all the ongoing optimized flows are dropped when the TCP Optimization is removed.

Then, for a packet that is accepted, the following parameters can be configured:

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cflowd</td>
<td>Enables cflowd traffic monitoring.</td>
</tr>
<tr>
<td>NAT Pool or NAT VPN</td>
<td>Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination.</td>
</tr>
<tr>
<td>DSCP</td>
<td>DSCP value. The range is 0 through 63.</td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>Name of the forwarding class.</td>
</tr>
<tr>
<td>Action Condition</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Local TLOC</strong></td>
<td>Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: <strong>ipsec</strong> and <strong>gre</strong>. By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the <strong>restrict</strong> option. By default, encapsulation is <strong>ipsec</strong>.</td>
</tr>
<tr>
<td><strong>Next Hop</strong></td>
<td>Sets the next hop IP address to which the packet should be forwarded. <strong>Note</strong>: Starting from Cisco IOS XE Release 17.5.1a and Cisco vManage Release 20.5.1, the <strong>Use Default Route when Next Hop is not available</strong> field is available next to the <strong>Next Hop</strong> action parameter. This option is available only when the sequence type is <strong>Traffic Engineering</strong> or <strong>Custom</strong>, and the protocol is either <strong>IPv4</strong> or <strong>IPv6</strong>, but not both.</td>
</tr>
<tr>
<td><strong>Policer</strong></td>
<td>Applies a policer. Specifies the name of policer configured with the <strong>policy policer</strong> command.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>Specifies a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Standard services: <strong>FW</strong>, <strong>IDS</strong>, <strong>IDP</strong> Custom services: <strong>netsvc1</strong>, <strong>netsvc2</strong>, <strong>netsvc3</strong>, <strong>netsvc4</strong> TLOC list is configured with a <strong>policy lists tloc-list</strong> list. Configure the services themselves on the Cisco IOS XE SD-WAN devices that are collocated with the service devices, using the <strong>vpn service</strong> command.</td>
</tr>
<tr>
<td><strong>TLOC</strong></td>
<td>Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic. Click <strong>Accept</strong>, then action <strong>VPN</strong>.</td>
</tr>
<tr>
<td></td>
<td>Set the VPN that the packet is part of. The range is 0 through 65530.</td>
</tr>
</tbody>
</table>
Data policies are applicable on locally generated packets, including routing protocol packets, when the match conditions are generic.

Example configuration:

```plaintext
sequence 21
match
  source-ip 10.0.0.0/8
action accept
```

In such situations, it may be necessary to add a sequence in the data policy to escape the routing protocol packets. For example to skip OSPF, use the following configuration:

```plaintext
sequence 20
match
  source-ip 10.0.0.0/8
  protocol 89
action accept
sequence 21
match
  source-ip 10.0.0.0/8
action accept
```

The following table describes the IPv4 and IPv6 actions.

### Table 13:

<table>
<thead>
<tr>
<th>IPv4 Actions</th>
<th>IPv6 Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)</td>
<td>N/A</td>
</tr>
<tr>
<td>App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL) App-route SLA (only), App-route preferred color, app-route sla strict</td>
</tr>
<tr>
<td>policer (DataPolicy), tcp-optimization, fecalways,</td>
<td>policer (DataPolicy)</td>
</tr>
<tr>
<td>tloc, tloc-list (set tloc, set tloc-list)</td>
<td>tloc, tloc-list (set tloc, set tloc-list)</td>
</tr>
<tr>
<td>App-Route backup-preferred color, local-tloc, local-tloc-list</td>
<td>App-Route backup-preferred color, local-tloc, local-tloc-list</td>
</tr>
</tbody>
</table>

**Apply Policies to Sites and VPNs**

In the **Apply Policies to Sites and VPNs** page, apply a policy to sites and VPNs:
1. In the **Policy Name** field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. In the **Policy Description** field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

3. Associate the policy with VPNs and sites. The choice of VPNs and sites depends on the type of policy block:
   a. For a **Topology** policy block, click **New Site List**, **Inbound Site List**, **Outbound Site List**, or **VPN List**. Some topology blocks might have no **Add** buttons. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   b. For an **Application-Aware Routing** policy block, click **New Site List** and **VPN list**. Choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   c. For a **Traffic Data** policy block, click **New Site List and VPN List**. Choose the direction for applying the policy (**From Service, From Tunnel**, or **All**), choose one or more site lists, and choose one or more VPN lists. Click **Add**.
   d. For a cflowd policy block, click **New Site List**. Choose one or more site lists, and click **Add**.

4. Click **Preview** to view the configured policy. The policy appears in CLI format.

5. Click **Save Policy**. The **Configuration > Policies** page appears, and the policies table includes the newly created policy.

---

### NAT Fallback on Cisco IOS XE SD-WAN Devices

<table>
<thead>
<tr>
<th>NAT Fallback on Cisco IOS XE SD-WAN Devices</th>
<th>Release Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 17.3.2</td>
<td></td>
</tr>
<tr>
<td>Cisco vManage Release 20.3.2</td>
<td></td>
</tr>
</tbody>
</table>

Cisco IOS XE SD-WAN devices support the NAT fallback feature for Direct Internet Access (DIA). The NAT fallback feature provides a routing-based mechanism for all traffic that is sent to the DIA route to use an alternative route when required. With this release, fallback is supported on the service and tunnel side.

---

**Note**

To use Cisco vManage to configure NAT DIA fallback, Cisco vManage must manage your Cisco vSmart Controller.

To enable NAT fallback using Cisco vManage, create and configure a data policy by doing the following:

1. From the Cisco vManage menu, choose **Configuration > Policies**.
2. From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Policy**.

---

**Release Information**

- **Cisco IOS XE SD-WAN Devices**: Cisco IOS XE SD-WAN devices support the NAT fallback feature for Direct Internet Access (DIA). The NAT fallback feature provides a routing-based mechanism for all traffic that is sent to the DIA route to use an alternative route when required. With this release, fallback is supported on the service and tunnel side.

---

**Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x**
3. Click Traffic Data.
4. From the Add Policy drop-down, click Create New.
5. Click Sequence Type and select Custom.
6. Click (+) Sequence Rule to create a new sequence rule.
7. After adding match conditions, click Actions and click Accept.
8. Click NAT VPN and select the Fallback checkbox.
9. Click Save and Match Actions.
10. Click Save Data Policy.

Edit your existing centralized policy and import the policy:
1. Click Centralized Policy and for the required centralized policy, click ... and select Edit.
2. Click Traffic Rules and select Traffic Data.
3. From the Add Policy drop-down, select Import Existing.
4. Select the NAT policy that you created from the Policy drop-down.
5. Click Policy Application and select Traffic Data.
6. Click + New Site List and VPN List.
7. Select the direction, VPN, and site as required.
8. Click Add.
9. Click Save Policy Changes.
10. Click to select VPN, and Site from the drop-down.

Note

The following NAT fallback actions/commands are now supported:

- **Action**: nat fallback
- **When applying a policy**: direction from-tunnel

### Activate a Centralized Policy

Activating a centralized policy sends that policy to all connected Cisco vSmart Controllers. To activate a centralized policy:

1. From the Cisco vManage menu, choose Configuration > Policies. Centralized Policy is selected and displayed by default.
2. For the required policy, click ... and select Activate. The Activate Policy popup appears. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy must be applied.
3. Click Activate.
View Centralized Policies

To view centralized policies:

1. From the Centralized Policy, select a policy.
2. For a policy created using the UI policy builder or using the CLI, click ... and select View. The policy created using the UI policy builder is displayed in graphical format while the policy created using the CLI method is displayed in text format.
3. For a policy created using Cisco vManage policy configuration wizard, click ... and select Preview. This policy is displayed in text format.

Copy, Edit, and Delete Policies

To copy a policy:

1. From the Centralized Policy, select a policy.
2. For the desired policy, click ... and select Copy.
3. In the Policy Copy popup window, enter the policy name and a description of the policy.

Note: Starting with the Cisco IOS XE Release 17.2, 127 characters are supported for policy names for the following policy types:

- Central route policy
- Local route policy
- Local Access Control lOst (ACL)
- Local IPv6 ACL
- Central data policy
- Central app route policy
- QoS map
- Rewrite rule

All other policy names support 32 characters.

4. Click Copy.

To edit policies created using the Cisco vManage policy configuration wizard:

1. For the desired policy, click ... and select Edit.
2. Edit the policy as needed.
3. Click Save Policy Changes.

To edit policies created using the CLI method:

1. In the Custom Options drop-down, click CLI Policy.
2. For the desired policy, click ... and select Edit.
3. Edit the policy as needed.
4. Click Update.

To delete policies:
1. From the Centralized Policy, select a policy.
2. For the desired policy, click ... and select Delete.
3. Click OK to confirm deletion of the policy.

Configure Centralized Policies Using the CLI

To configure a centralized control policy using the CLI:

1. Create a list of overlay network sites to which the centralized control policy is to be applied (in the apply-policy command):

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

   The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (-). Create additional site lists, as needed.

2. Create lists of IP prefixes, TLOCs, and VPNs as needed:

   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   vSmart(config)# policy lists
   vSmart(config-lists)# tloc-list list-name
   vSmart(config-lists-list-name)# tloc address
   vSmart(config-lists-list-name)# color color
   vSmart(config-lists-list-name)# encapsulation
   [preference value]
   ```

   ```
   vSmart(config)# policy lists data-ipv6-prefix-list dest_ip_prefix_list
   vSmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# ipv6-prefix 2001:DB8::/32
   vSmart(config-data-ipv6-prefix-list-dest_ip_prefix_list)# commit
   Commit complete.
   ```

   ```
   vSmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
   vSmart (config-sequence-100)# match destination-data-ipv6-prefix-list dest_ip_prefix_list
   vSmart (config-match)# commit
   vSmart(config)# exit
   vSmart(config)# match source-data-ipv6-prefix-list dest_ip_prefix_list
   vSmart(config-match)# commit
   Commit complete.
   vSmart(config)# end
   ```

   ```
   vSmart(config)# policy
   vSmart(config-policy)# data-policy data_policy_1
   ```
vsmart(config-data-policy-data_policy_1)# vpn-list vpn_1
vsmart(config-vpn-list-vpn_1)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8::/32
vsmart(config-match)# exit
vsmart(config-sequence-101)# match destination-ipv6 2001:DB8::/32
vsmart(config-match)#

3. Create a control policy instance:

vSmart(config)# policy control-policy policy-name
vSmart(config-control-policy-policy-name)#

4. Create a series of match–action pair sequences:

vSmart(config-control-policy-policy-name)# sequence number
vSmart(config-sequence-number)#

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

5. Define match parameters for routes and for TLOCs:

vSmart(config-sequence-number)# match route route-parameter
vSmart(config-sequence-number)# match tloc tloc-parameter

6. Define actions to take when a match occurs:

vSmart(config-sequence-number)# action reject
vSmart(config-sequence-number)# action accept export-to (vpn vpn-id | vpn-list list-name)
vSmart(config-sequence-number)# action accept set omp-tag number
vSmart(config-sequence-number)# action accept set preference value
vSmart(config-sequence-number)# action accept set service service-name (tloc ip-address | tloc-list list-name) [vpn vpn-id]

7. Create additional numbered sequences of match–action pairs within the control policy, as needed.

8. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching routes to be accepted, configure the default action for the policy:

vSmart(config-policy-name)# default-action accept

9. Apply the policy to one or more sites in the Cisco SD-WAN overlay network:

vSmart(config)# apply-policy site-list list-name
control-policy policy-name (in | out)
If the action you are configuring is a service, configure the required services on the Cisco IOS XE SD-WAN devices so that the Cisco vSmart Controller knows how to reach the services:

```
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
vsmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8::/32
```

Specify the VPN in which the service is located and one to four IP addresses to reach the service device or devices. If multiple devices provide the same service, the device load-balances the traffic among them. Note that the Cisco IOS XE SD-WAN device keeps track of the services, advertising them to the Cisco vSmart Controller only if the address (or one of the addresses) can be resolved locally, that is, at the device's local site, and not learned through OMP. If a previously advertised service becomes unavailable, the Cisco IOS XE SD-WAN device withdraws the service advertisement.

Following are the high-level steps for configuring a VPN membership data policy:

1. Create a list of overlay network sites to which the VPN membership policy is to be applied (in the `apply-policy` command):

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

The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (`-`). Create additional site lists, as needed.

2. Create lists of IP prefixes and VPNs, as needed:

```
vSmart(config)# policy lists
vSmart(config-lists)# data-prefix-list list-name
vSmart(config-lists-list-name)# ip-prefix prefix/length
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists-list-name)# vpn vpn-id
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match destination-data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-match)# commit
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-match)# commit
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# match source-data-ipv6-prefix-list dest_ip_prefix_list
vsmart(config-match)# exit
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-100)# sequence 101
vsmart(config-sequence-101)# match source-ipv6 2001:DB8:19::1
vsmart(config-match)# exit
vsmart(config)# policy data-policy data_policy_1 vpn-list vpn_1
vsmart (config-sequence-101)# match destination-ipv6 2001:DB8:19::1
vsmart(config-match)#
```

Commit complete.

3. Create lists of TLOCs, as needed.

```
vSmart(config)# policy
vSmart(config-policy)# lists tloc-list list-name
```
Centralized Policies Configuration Examples

This topic provides some examples of configuring a centralized data policy to influence traffic flow across the Cisco IOS XE SD-WAN domain and to configure a Cisco IOS XE SD-WAN device to be an internet exit point.

vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation | preference number

4. Define policing parameters, as needed:
   vSmart(config-policy)# policer policer-name
   vSmart(config-policer)# rate bandwidth
   vSmart(config-policer)# burst bytes
   vSmart(config-policer)# exceed action

5. Create a data policy instance and associate it with a list of VPNs:
   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name

6. Create a series of match–pair sequences:
   vSmart(config-vpn-list)# sequence number
   vSmart(config-sequence-number)#

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

7. Define match parameters for packets:
   vSmart(config-sequence-number)# match parameters

8. Define actions to take when a match occurs:
   vSmart(config-sequence-number)# action (accept | drop) [count counter-name] [log]
   vSmart(config-sequence-number)# action accept nat [pool number] [use-vpn 0]
   vSmart(config-sequence-number)# action accept redirect-dns (host | ip-address)
   vSmart(config-sequence-number)# action accept set parameters

   vSmart(config)# policy data-policy data_policy_1 vpn-list vpn_1 sequence 100
   vSmart(config-sequence-100)# action accept set next-hop-ipv6 2001:DB8:19::1
   vSmart(config-set)#

9. Create additional numbered sequences of match–action pairs within the data policy, as needed.

10. If a route does not match any of the conditions in one of the sequences, it is rejected by default. To accept nonmatching prefixed, configure the default action for the policy:
    vSmart(config-policy-name)# default-action accept

11. Apply the policy to one or more sites in the overlay network:
    vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
General Centralized Policy Example

This section shows a general example of a centralized data policy to illustrate that you configure centralized data policy on a Cisco vSmart Controller and that after you commit the configuration, the policy itself is pushed to the required Cisco IOS XE SD-WAN device.

Here we configure a simple data policy on the Cisco vSmart Controller vm9:

```bash
vm9# show running-config policy
data-policy test-data-policy
  vpn-list test-vpn-list
  sequence 10
  match
  destination-ip 209.165.201.0/27
  !
  action drop
  count test-counter
  !
  !
  default-action drop
  !

lists
  vpn-list test-vpn-list
  vpn 1
  site-list test-site-list
  site-id 500
  !

Then, apply this policy to the site list named test-site-list, which includes site 500:

```bash
vm9# show sdwan running-config apply-policy
apply-policy
  site-list test-site-list
  data-policy test-data-policy
  !
```

Immediately after you activate the configuration on the Cisco vSmart Controller, it pushes the policy configuration to the Cisco IOS XE SD-WAN devices in site 500. One of these devices is vm5, where you can see that the policy has been received:

```bash
vm5# show sdwan policy from-vsmart
policy-from-vsmart
  data-policy test-data-policy
  vpn-list test-vpn-list
  sequence 10
  match
  destination-ip 209.165.201.0/27
  !
  action drop
  count test-counter
  !
  !
  default-action drop
  !

lists
  vpn-list test-vpn-list
  vpn 1
```
Control Access

This example shows a data policy that limits the type of packets that a source can send to a specific destination. Here, the host at source address 192.0.2.1 in site 100 and VPN 100 can send only TCP traffic to the destination host at 203.0.113.1. This policy also specifies the next hop for the TCP traffic sent by 192.0.2.1, setting it to be TLOC 209.165.200.225, color gold. All other traffic is accepted as a result of the default-action statement.

```
policy
  lists
    site-list north
    site-id 100
    vpn-list vpn-north
    vpn 100
  !
  data-policy tcp-only
  vpn-list vpn-north
  sequence 10
  match
    source-ip 192.0.2.1/32
    destination-ip 198.51.100.1/32
    protocol tcp
  action accept
  set tloc 203.0.113.1 gold
  !
  default-action accept
  !
apply-policy
  site north data-policy tcp-only
```

Restrict Traffic

This example illustrates how to disallow certain types of data traffic from being sent from between VPNs. This policy drops data traffic on port 25, which carries SMTP mail traffic, that originates in 209.165.201.0/27. However, the policy accepts all other data traffic, including non-HTTP traffic from 209.165.201.0/27.

```
policy
  lists
    data-prefix-list north-ones
    ip-prefix 209.165.201.0/27
    port 25
    vpn-list all-vpns
    vpn 1
    vpn 2
    site-list north
    site-id 100
  !
  data-policy no-mail
  vpn-list all-vpns
  sequence 10
  match
    source-data-prefix-list north-ones
  action drop
  !
  default-action accept
  !
apply-policy
  site north data-policy no-mail
```
**Traffic Engineering**

This example of traffic engineering forces all traffic to come to a Cisco IOS XE SD-WAN device using a device hub instead of directly.

One common way to design a domain in a Cisco IOS XE SD-WAN overlay network is to route all traffic destined for branches through a hub router, which is typically located in a data center, rather than sending the traffic directly from one Cisco IOS XE SD-WAN device to another. You can think of this as a hub-and-spoke design, where one device is acting as a hub and the devices are the spokes. With such a design, traffic between local branches travels over the IPsec connections that are established between the spoke routers and the hub routers when the devices are booted up. Using established connections means that the devices do not need to expend time and CPU cycles to establish IPsec connections with each other. If you were to imagine that this were a large network with many devices, having a full mesh of connections between each pair of routers would require a large amount of CPU from the routers. Another attribute of this design is that, from an administrative point of view, it can be simpler to institute coordinated traffic flow policies on the hub routers, both because there are fewer of them in the overlay network and because they are located in a centralized data center.

One way to direct all the device spoke router traffic to a Cisco hub router is to create a policy that changes the TLOC associated with the routes in the local network. Let’s consider the topology in the figure here:

![Topology Diagram](image)

This topology has two devices in different branches:

- The Device West in site ID 1. The TLOC for this device is defined by its IP address (192.0.2.1), a color (gold), and an encapsulation (here, IPsec). We write the full TLOC address as {192.0.2.1, gold, ipsec}. The color is simply a way to identify a flow of traffic and to separate it from other flows.

- The Device East in site ID 2 has a TLOC address of {203.0.113.1, gold, ipsec}.

The devices West and East learn each other’s TLOC addresses from the OMP routes distributed to them by the Cisco vSmart Controller. In this example, the Device East advertises the prefix 209.165.201.0/27 as being reachable at TLOC {203.0.113.1, gold, }. In the absence of any policy, the Device West could route traffic destined for 209.165.201.0/27 to TLOC {203.0.113.1, gold, ipsec}, which means that the Device West would be sending traffic directly to the Device East.

However, our design requires that all traffic from West to East be routed through the hub router, whose TLOC address is {209.165.200.225, gold, ipsec}, before going to the Device East. To effect this traffic flow, you define a policy that changes the route's TLOC. So, for the prefix 209.165.201.0/27, you create a policy that changes the TLOC associated with the prefix 209.165.201.0/27 from {203.0.113.1, gold, ipsec}, which is the TLOC address of the Device East, to {209.165.200.225, gold, ipsec}, which is the TLOC address of the hub router. The result is that the OMP route for the prefix 209.165.201.0/27 that the Cisco vSmart Controller advertises to the Device West that contains the TLOC address of the hub router instead of the TLOC address of the Device East. From a traffic flow point of view, the Device West then sends all traffic destined for 209.165.201.0/27 to the hub router.
The device also learns the TLOC addresses of the West and East devices from the OMP routes advertised by the Cisco vSmart Controller. Because, devices must use these two TLOC addresses, no policy is required to control how the hub directs traffic to the devices.

Here is a policy configuration on the Cisco vSmart Controller that directs the Device West (and any other devices in the network domain) to send traffic destined to prefix 209.165.201.0/27 to TLOC 209.165.200.225, gold, which is the device:

```
policy
lists
  prefix-list east-prefixes
    ip-prefix 209.165.201.0/27
  site-list west-sites
    site-id 1
control-policy change-tloc
  sequence 10
match route
  prefix-list east-prefixes
    site-id 2
action accept
set tloc 209.165.200.225 color gold encap ipsec
apply-policy
  site west-sites control-policy change-tloc out
```

A rough English translation of this policy is:

Create a list named “east-prefixes” that contains the IP prefix “209.165.201.0/27”
Create a list named “west-sites” that contains the site-id “1”
Define a control policy named “change-tloc”
Create a policy sequence element that:
  Matches a prefix from list “east-prefixes”, that is, matches “209.165.201.0/27”
  AND matches a route from site-id “2”
If a match occurs:
  Accept the route
  AND change the route’s TLOC to “209.165.200.225” with a color of “gold” and an
  encapsulation of “ipsec”
Apply the control policy “change-tloc” to OMP routes sent by the vSmart
  controller to “west-sites”, that is, to site ID 1

This control policy is configured on the Cisco vSmart Controller as an outbound policy, as indicated by the
  out option in the apply-policy site command. This option means the Cisco vSmart Controller applies the
  TLOC change to the OMP route after it distributes the route from its route table. The OMP route for prefix
  209.165.201.0/27 that the Cisco vSmart Controller distributes to the Device West associates 209.165.201.0/27
  with TLOC 209.165.200.225, gold. This is the OMP route that the Device West installs it in its route table.
  The end results are that when the Device West sends traffic to 209.165.201.0/27, the traffic is directed to the
  hub; and the Device West does not establish a DTLS tunnel directly with the Device East.

If the West side of the network had many sites instead of just one and each site had its own device, it would
be straightforward to apply this same policy to all the sites. To do this, you simply add the site IDs of all the
  sites in the site-list west-sites list. This is the only change you need to make in the policy to have all the
  West-side sites send traffic bound for the prefix 209.165.201.0/27 through the device. For example:

```
policy
lists
  prefix-list east-prefixes
    ip-prefix 209.165.201.0/27
  site-list west-sites
    site-id 1
    site-id 11
    site-id 12
    site-id 13
control-policy change-tloc
```
Creating Arbitrary Topologies

To provide redundancy in the hub-and-spoke-style topology discussed in the previous example, you can add a second Cisco hub to create a dual-homed hub site. The following figure shows that site ID 100 now has two Device hubs. We still want all inter-branch traffic to be routed through a device hub. However, because we now have dual-homed hubs, we want to share the data traffic between the two hub routers.

• Device Hub West, with TLOC 209.165.200.225, gold. We want all data traffic from branches on the West side of the overlay network to pass through and be processed by this device.

• Device Hub East, with TLOC 198.51.100.1, gold. Similarly, we all East-side data traffic to pass through the Device Hub East.

Here is a policy configuration on the Cisco vSmart Controller that would send West-side data traffic through the Cisco hub, and West and East-side traffic through the Device Hub East:

```
policy
  lists
    site-list west-sites
      site-id 1
    site-list east-sites
      site-id 2
  tloc-list west-hub-tlocs
    tloc-id 209.165.200.225 gold
  tloc-list east-hub-tlocs
    tloc-id 198.51.100.1 gold
  control-policy prefer-west-hub
    sequence 10
      match tloc
        tloc-list west-hub-tlocs
      action accept
        set preference 50
  control-policy prefer-east-hub
    sequence 10
      match tloc
        tloc-list east-hub-tlocs
      action accept
        set preference 50
  apply-policy
    site west-sites control-policy prefer-west-hub out
    site east-sites control-policy prefer-east-hub out
```
Here is an explanation of this policy configuration:

Create the site lists that are required for the **apply-policy** configuration command:

- **site-list west-sites** lists all the site IDs for all the devices in the West portion of the overlay network.
- **site-list east-sites** lists the site IDs for the devices in the East portion of the network.

Create the TLOC lists that are required for the match condition in the control policy:

- **west-hub-tlocs** lists the TLOC for the Device West Hub, which we want to service traffic from the West-side device.
- **east-hub-tlocs** lists the TLOC for the Device East Hub, to service traffic from the East devices.

Define two control policies:

- **prefer-west-hub** affects OMP routes destined to TLOC 209.165.200.225, gold, which is the TLOC address of the Device West hub router. This policy modifies the preference value in the OMP route to a value of 50, which is large enough that it is likely that no other OMP routes will have a larger preference. So setting a high preference value directs traffic destined for site 100 to the Device West Hub router.

- Similarly, **prefer-east-hub** sets the preference to 50 for OMP routes destined TLOC 198.51.100.1, gold, which is the TLOC address of the Device East hub router, thus directing traffic destined for site 100 site to the Device East hub 198.51.100.1 router.

Apply the control policies:

- The first line in the **apply-policy** configuration has the Cisco vSmart Controller apply the **prefer-west-hub** control policy to the sites listed in the **west-sites** list, which here is only site ID 1, so that the preference in their OMP routes destined to TLOC 209.165.200.225 is changed to 50 and traffic sent from the Device West to the hub site goes through the Device West Hub router.

- The Cisco vSmart Controller applies the **prefer-east-hub** control policy to the OMP routes that it advertises to the devices in the **east-sites** list, which changes the preference to 50 for OMP routes destined to TLOC 198.51.100.1, so that traffic from the Device East goes to the Device East hub router.

**Community Example**

This example displays the configuration for centralized control policy for community lists.

```
policy
  lists
    expanded-community-list test
      community 0:110* 100:[7-9]+ 
      community 0:110* 11:* 
    community-list test-com
      community 0:1
      community 0:2

  control-policy test
    sequence 10
    match route
      expanded-community-list test

    action accept
    set
```
This example displays the configuration for standard community lists.

**Standard Community list**

route : 0:1234 0:11 0:12

```community-list
  community 0:100
  community 0:1234
  community 0:101
*MATCH*
```

route : 0:1234 0:11 0:12

```community-list
  community 0:100
  community 0:5678
  community 0:101
*NO MATCH*
```

This example displays the configuration for expanded community lists. OR match compares each regex string in the community list against the route’s community string.

**Expanded Community list**

route - 0:1234 0:5678

```expanded-community-list:
  community 0:110* 11:
 社区 0:110* 100:([7-9]+)
  community 0:12[3-7]+
*MATCH*
```

route - 0:1234 0:5678

```expanded-community-list:
  community 0:111*
  community 0:110* 11:*  
*NO MATCH*
```

EXACT match input strings need to have communities in sorted order. Sorts it by byte value and add the meta characters for start and end of string.

route - 0:1234 0:5678

```expanded-community-list:
  community ^0:1234 0:5678$
*MATCH*
```

AND match input strings need to have communities in sorted order. Add ‘.+’ to blindly match between the sorted communities.

route - 0:0 0:1234 0:5678 0:9789 0:9800 0:9900 0:9999 1:10

```expanded-community-list:
  community 0:1234 .+ 0:9900 .+$
*MATCH*
```

**SIG Data Policy Fallback**

From Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1, you can use the `sig-action fallback-to-routing` command to configure internet-bound traffic to be routed through the Cisco SD-WAN overlay when all SIG tunnels are down. The following example shows the configuration of this fallback mechanism.
data-policy _VPN10_SIG_Fall_Back
vpn-list VPN10
  sequence 1
    match
      app-list Google_Apps
      source-ip 0.0.0.0/0
    !
    action accept
    sig
      sig-action fallback-to-routing
    !
  !
default-action drop
Localized Policy

The topics in this section provide overview information about the different types of localized policies, the components of localized policies, and how to configure localized policies using Cisco vManage or the CLI.

- Overview of Localized Policies, on page 71
- Configure Localized Policy Using Cisco vManage, on page 72
- Configure Localized Policy for IPv4 Using the CLI, on page 87
- Configure Localized Policy for IPv6 Using the CLI, on page 89
- Localized Data Policy Configuration Examples, on page 90

Overview of Localized Policies

Localized policy refers to a policy that is provisioned locally through the CLI on the Cisco IOS XE SD-WAN devices, or through a Cisco vManage device template.

Types of Localized Policies

Localized Control Policy

Control policy operates on the control plane traffic in the Cisco IOS XE SD-WAN overlay network, influencing the determination of routing paths through the overlay network. Localized control policy is policy that is configured on a Cisco IOS XE SD-WAN device (hence, it is local) and affects BGP and OSPF routing decisions on the site-local network that the device is part of.

In addition to participating in the overlay network, a Cisco IOS XE SD-WAN device participates in the network at its local site, where it appears to the other network devices to be simply a regular router. As such, you can provision routing protocols, such as BGP and OSPF, on the Cisco IOS XE SD-WAN device so that it can exchange route information with the local-site routers. To control and modify the routing behavior on the local network, you configure a type of control policy called route policy on the devices. Route policy applies only to routing performed at the local branch, and it affects only the route table entries in the local device's route table.

Localized control policy, which you configure on the devices, lets you affect routing policy on the network at the local site where the device is located. This type of control policy is called route policy. This policy is similar to the routing policies that you configure on a regular driver, allowing you to modify the BGP and OSPF routing behavior on the site-local network. Whereas, centralized control policy affects the routing behavior across the entire overlay network, route policy applies only to routing at the local branch.
Localized Data Policy

Data policy operates on the data plane in the Cisco IOS XE SD-WAN overlay network and affects how data traffic is sent among the Cisco IOS XE SD-WAN devices in the network. The Cisco SD-WAN architecture defines two types of data policy, centralized data policy, which controls the flow of data traffic based on the IP header fields in the data packets and based on network segmentation, and localized data policy, which controls the flow of data traffic into and out of interfaces and interface queues on a Cisco IOS XE SD-WAN device.

Localized data policy, so called because it is provisioned on the local Cisco IOS XE SD-WAN device, is applied on a specific router interface and affects how a specific interface handles the data traffic that it is transmitting and receiving. Localized data policy is also referred to as access lists (ACLs). With access lists, you can provision class of service (CoS), classifying data packets and prioritizing the transmission properties for different classes. You can configure policing and provision packet mirroring.

For IPv4, you can configure QoS actions.

You can apply IPv4 access lists in any VPN on the router, and you can create access lists that act on unicast and multicast traffic. You can apply IPv6 access lists only to tunnel interfaces in the transport VPN (VPN 0).

You can apply access lists either in the outbound or inbound direction on the interface. Applying an IPv4 ACL in the outbound direction affects data packets traveling from the local service-side network into the IPsec tunnel toward the remote service-side network. Applying an IPv4 ACL in the inbound direction affects data packets exiting from the IPsec tunnel and being received by the local Cisco IOS XE SD-WAN device. For IPv6, an outbound ACL is applied to traffic being transmitted by the router, and an inbound ACL is applied to received traffic.

Explicit and Implicit Access Lists

Access lists that you configure using localized data policy are called explicit ACLs. You can apply explicit ACLs in any VPN on the router.

Router tunnel interfaces also have implicit ACLs, which are also referred to as services. Some of these are present by default on the tunnel interface, and they are in effect unless you disable them. Through configuration, you can also enable other implicit ACLs. On Cisco IOS XE SD-WAN devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

Perform QoS Actions

With access lists, you can provision quality of service (QoS) which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. See Forwarding and QoS Overview.

Mirror Data Packets

Once packets are classified, you can configure access lists to send a copy of data packets seen on a Cisco vEdge device to a specified destination on another network device. The Cisco IOS XE SD-WAN devices support 1:1 mirroring; that is, a copy of every packet is sent to the alternate destination.

Configure Localized Policy Using Cisco vManage

To configure localized policies, use the Cisco vManage policy configuration wizard. The wizard is a UI policy builder that consists of five windows to configure and modify the following localized policy components:
• Groups of interest, also called lists
• Forwarding classes to use for QoS
• Access control lists (ACLs)
• Route policies
• Policy settings

You configure some or all these components depending on the specific policy you are creating. To skip a component, click Next at the bottom of the window. To return to a component, click Back at the bottom of the window.

To configure localized policies using Cisco vManage, use the steps identified in the procedures that follow this section.

Start the Policy Configuration Wizard

To start the policy configuration wizard:
1. From the Cisco vManage menu, choose Configuration > Policies.
2. Select Localized Policy.
3. Click Add Policy.

The Create Groups of Interest page is displayed.

Configure Groups of Interest for Localized Policy

In Create Groups of Interest, create lists of groups to use in a localized policy:

In Create Groups of Interest, create new groups of list types as described in the following sections to use in a localized policy:

Configure As Path

1. In the group of interest list, click AS Path.
2. Click New AS Path List.
3. Enter a name for the list.
4. Enter the AS path, separating AS numbers with a comma.
5. Click Add.

AS Path list specifies one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list separated by commas. To configure multiple AS paths in a single list, include multiple as-path options, specifying one AS path in each option.
Configure Community

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click Community.
2. Click New Community List.
3. Enter a name for the community list.
4. In the Add Community field, enter one or more data prefixes separated by commas in any of the following formats:
   • aa:nn: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   • internet: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices.
   • local-as: Routes in this community are not advertised outside the local AS number.
   • no-advertise:attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
   • no-export:attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one community in each option.
5. Click Add.

Configure Data Prefix

1. In the Group of Interest list, click Data Prefix.
2. Click New Data Prefix List.
3. Enter a name for the list.
4. Enter one or more IP prefixes.
5. Click Add.

A data prefix list specifies one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple ip-prefix options, specifying one prefix in each option.

Configure Extended Community

1. In the group of interest list, click Extended Community.
2. Click New Extended Community List.
3. Enter a name for the list.
4. Enter the BGP extended community in the following formats:
• **rt (aa:nn | ip-address)**: Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.

• **soo (aa:nn | ip-address)**: Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.

5. Click **Add**.

**Configure Class Map**

1. In the group of interest list, click **Class Map**.
2. Click **New Class List**.
3. Enter a name for the class.
4. Select a required queue from the **Queue** drop-down list.
5. Click **Save**.

**Configure Mirror**

1. In the group of interest list, click **Mirror**.
2. Click **New Mirror List**. The Mirror List popup displays.
3. Enter a name for the list.
4. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
5. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
6. Click **Add**.

To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

**Configure Policer**

1. In the group of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. In the **Burst (bps)** field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.
5. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high.
6. In the **Rate (bps)** field, enter the maximum traffic rate. It can be a value from 8 through $2^{64}$ bps (8 through 100000000000).

7. Click **Add**.

**Configure Prefix**

1. In the group of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Internet Protocol** field, click either **IPv4** or **IPv6**.
5. Under **Add Prefix**, enter the prefix for the list. (An example is displayed.) Optionally, click the green **Import** link on the right-hand side to import a prefix list.
6. Click **Add**.

Click **Next** to move to **Configure Forwarding Classes/QoS** in the wizard.

---

**Configure Forwarding Classes/QoS**

When you first open the **Forwarding Classes/QoS** page, **QoS Map** is selected by default:

**QoS Map**

To create a new QoS mapping:

1. In **QoS**, click the **Add QoS Map** drop-down.
2. Select **Create New**.
3. Enter a name and description for the QoS mapping.
4. Click **Add Queue**. The **Add Queue** popup appears.
5. Select the queue number from the **Queue** drop-down.
6. Select the maximum bandwidth and buffer percentages, and the scheduling and drop types.
7. Enter the **Forwarding Class**.
8. Click **Save Queue**.

To import an existing QoS mapping:

1. In **QoS**, click the **Add QoS Map** drop-down.
2. Select **Import Existing**. The **Import Existing Application QoS Map Policy** popup displays.
3. Select a **QoS Map** policy.
4. Click **Import**.

To view or copy a QoS mapping or to remove the mapping from the localized policy, click ... and select the desired action.
For hardware, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for low-latency queuing (LLQ), so any class that is mapped to queue 0 must be configured to use LLQ. The default scheduling method for all is weighted round-robin (WRR).

For Cisco IOS XE SD-WAN devices, each interface has eight queues, numbered from 0 through 7. Queue 0 is reserved for control traffic, and queues 1, 2, 3, 4, 5, 6 and 7 are available for data traffic. The scheduling method for all eight queues is WRR. LLQ is not supported.

To configure QoS parameters on a Cisco IOS XE SD-WAN device, you must enable QoS scheduling and shaping. To enable QoS parameters for traffic that the Cisco IOS XE SD-WAN device receives from transport-side interfaces:

To enable QoS parameters for traffic that the Cisco IOS XE SD-WAN device receives from service-side interfaces:

Policy Rewrite

To configure policy rewrite rules for the QoS mapping:

1. In Policy Rewrite, click the Add Rewrite Policy drop-down.
2. Select Create New.
3. Enter a name and description for the rewrite rule.
5. Select a class from the Class drop-down.
6. Select the priority (Low or High) from the Priority drop-down.
   - Low priority is supported only for Cisco IOS XE SD-WAN devices.
7. Enter the DSCP value (0 through 63) in the DSCP field.
8. Enter the class of service (CoS) value (0 through 7) in the Layer 2 Class of Service field.
9. Click Save Rule.

To import an existing rewrite rule:

1. In QoS, click the Add Rewrite Policy drop-down.
2. Select Import Existing. The Import Existing Policy Rewrite popup appears.
3. Select a rewrite rule policy.
4. Click Import.

Click Next to move to Configure Access Lists page.

Configure ACLs

1. In the Configure Access Control Lists page, configure ACLs.
2. To create a new ACL, click the Add Access Control List Policy drop-down. Select one from the following options:
• **Add IPv6 ACL Policy**: Configure IPv6 ACL policy.

• **Import Existing**: Import existing ACL policy.

3. If you click Add IPv4 ACL Policy, the Add IPv4 ACL Policy page appears.
   or
   If you click Add IPv6 ACL Policy, the Add IPv6 ACL Policy page appears.

4. Enter a name and description for the ACL in the ACL Policy page.

5. In the left pane, click Add ACL Sequence. An Access Control List box is displayed in the left pane.

6. Double-click the Access Control List box, and type a name for the ACL.

7. In the right pane, click Add Sequence Rule to create a single sequence in the ACL. **Match** is selected by default.

8. Click a match condition.

9. On the left, enter the values for the match condition.
   a. On the right enter the action or actions to take if the policy matches.

10. Repeat Steps 6 through 8 to add match–action pairs to the ACL.

11. To rearrange match–action pairs in the ACL, in the right pane drag them to the desired position.

12. To remove a match–action pair from the ACL, click the X in the upper right of the condition.

13. Click **Save Match and Actions** to save a sequence rule.

14. To rearrange sequence rules in an ACL, in the left pane drag the rules to the desired position.

15. To copy, delete, or rename an ACL sequence rule, in the left pane, click ... next to the rule's name and select the desired option.

**Default Action**

If a packet being evaluated does not match any of the match conditions in a access list, a default action is applied to this packet. By default, the packet is dropped. To change the default action:

1. Click **Default Action** in the left pane.

2. Click the **Pencil** icon.

3. Change the default action to **Accept**.

4. Click **Save Match and Actions**.

5. Click **Save Access Control List Policy**.

To configure **Device Access Policy**, see **Device Access Policy**.

Click **Next** to move to Configure Route Policy page.
Explicit and Implicit Access Lists

Access lists that you configure through localized data policy using the `policy access-list` command are called **explicit ACLs**. You can apply explicit ACLs to any interface in any VPN on the device.

The device's tunnel interfaces in VPN 0 also have **implicit ACLs**, which are also referred to as **services**. Some services are enabled by default on the tunnel interface, and are in effect unless you disable them. Through configuration, you can also enable other services. You configure and modify implicit ACLs with the `allow-service` command:

```
Device(config)# vpn 0
Device(config-vpn)# interface interface-name
Device(config-interface)# tunnel-interface
Device(config-tunnel-interface)# allow-service service-name
Device(config-tunnel-interface)# no allow-service service-name
```

On Cisco IOS XE SD-WAN devices, the following services are enabled by default: DHCP (for DHCPv4 and DHCPv6), DNS, and ICMP. These three services allow the tunnel interface to accept DHCP, DNS, and ICMP packets. You can also enable services for BGP, Netconf, NTP, OSPF, SSHD, and STUN.

---

**Note**

If a connection is initiated from a device, and if NAT is enabled on the device (for example, Direct Internet Access (DIA) is configured), return traffic is allowed by the NAT entry even if the implicit ACL has been configured as `no allow-service`. You can still block this traffic with an explicit ACL.

Do not confuse an explicit ACL with a Cisco IOS XE ACL. A Cisco IOS XE ACL does not interact with a Cisco SD-WAN explicit and an implicit ACL and cannot override an implicit ACL or explicit ACL. Cisco IOS XE ACLs are executed later in the order of traffic processing operations.

When data traffic matches both an explicit ACL and an implicit ACL, how the packets are handled depends on the ACL configuration. Specifically, it depends on:

- Whether the implicit ACL is configured as allow (`allow-service service-name`) or deny (`no allow-service service-name`). Allowing a service in an implicit ACL is the same as specifying the `accept` action in an explicit ACL, and a service that is not allowed in an implicit ACL is the same as specifying the `drop` action in an explicit ACL.

- Whether, in an explicit ACL, the `accept` or `deny` action is configured in a policy sequence or in the default action.

The following table explains how traffic matching both an implicit and an explicit ACL is handled:

<table>
<thead>
<tr>
<th>Implicit ACL</th>
<th>Explicit ACL: Sequence</th>
<th>Explicit ACL: Default</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
<td>—</td>
<td>Deny (drop)</td>
</tr>
<tr>
<td>Allow (accept)</td>
<td>—</td>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>Allow (accept)</td>
<td>—</td>
<td>Allow (accept)</td>
</tr>
<tr>
<td>Implicit ACL</td>
<td>Explicit ACL: Sequence</td>
<td>Explicit ACL: Default</td>
<td>Result</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Deny (drop)</td>
<td>—</td>
<td>Allow (accept)</td>
<td>Deny (drop)</td>
</tr>
</tbody>
</table>

**Configure Route Policies**

In **Configure Route Policies**, configure the routing policies:

1. In **Add Route Policy**, select **Create New**.
2. Enter a name and description for the route policy.
3. In the left pane, click **Add Sequence Type**. A **Route** box is displayed in the left pane.
4. Double-click the **Route** box, and type a name for the route policy.
5. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. **Match** is selected by default.
6. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.
7. Click a match condition.
8. On the left, enter the values for the match condition.
9. On the right enter the action or actions to take if the policy matches.
10. Repeat Steps 6 through 8 to add match–action pairs to the route policy.
11. To rearrange match–action pairs in the route policy, in the right pane drag them to the desired position.
12. To remove a match–action pair from the route policy, click the X in the upper right of the condition.
13. Click **Save Match and Actions** to save a sequence rule.
14. To rearrange sequence rules in an route policy, in the left pane drag the rules to the desired position.
15. To copy, delete, or rename the route policy sequence rule, in the left pane, click ... next to the rule's name and select the desired option.
16. 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**.
17. Click **Save Route Policy**.
18. Click **Next** to move to **Policy Overview** page.
Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the `policy access-list sequence match` command.

Each sequence in an access-list must contain one match condition.

For access lists, you can match these parameters:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Name of a class defined with a <code>policy class-map</code> command.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>Name of a data-prefix-list list.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the DSCP value. The range is 0 through 63.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the internet protocol number. The range is 0 through 255.</td>
</tr>
<tr>
<td>ICMP Message</td>
<td>When you select a Protocol value as 1 the <code>ICMP Message</code> field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the <code>ICMP Message</code> field displays where you can select an ICMP message to apply to the data policy. <strong>Note</strong> This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For <code>icmp-msg</code> and <code>icmp6-msg</code> message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table in the Centralized chapter.</td>
</tr>
<tr>
<td>Packet Length</td>
<td>Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>Source Data Prefix</td>
<td>Specifies the name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td>PLP</td>
<td>Specifies the Packet Loss Priority (PLP) (high</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.</td>
</tr>
<tr>
<td>TCP</td>
<td>syn</td>
</tr>
</tbody>
</table>
### Route Policy Parameters

For route policies, you can match these parameters:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Specifies the name of a Prefix-List list.</td>
</tr>
<tr>
<td><strong>AS Path List</strong></td>
<td>Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (&quot; &quot;). To configure multiple AS numbers in a single list, include multiple AS Path options, specifying one AS path in each option.</td>
</tr>
</tbody>
</table>
| **Community List**| List of one of more BGP communities. In Community List, you can specify:  
  - *aa:nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535.  
  - *internet*: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices.  
  - *local-as*: Routes in this community are not advertised outside the local AS.  
  - *no-advertise*: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.  
  - *no-export*: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple community options, specifying one community in each option. |
| **Extended Community List**| Specifies the list of one or more BGP extended communities. In community, you can specify:  
  - *rt (aa:nn | ip-address)*: Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.  
  - *soo (aa:nn | ip-address)*: Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple community options, specifying one community in each option. |
| **BGP Local Preference**| Specifies the BGP local preference number. The range is 0 through 4294967295. |
| **Metric** | Specifies the route metric value. The range is 0 through 4294967295. |
| **Next Hop** | Specifies the name of an IP prefix list. |
| **OMP Tag** | Specifies the OMP tag number. The range is 0 through 4294967295. |
| **Origin** | Specifies the BGP origin code. The options are: EGP (default), IGP, Incomplete. |
| **OSPF Tag** | Specifies the OSPF tag number. The range is 0 through 4294967295. |
| **Peer** | Specifies the peer IP address. |
Action Parameters

Access List Parameters

When a packet matches the conditions in the match portion of an access list, the packet can be accepted or dropped, and it can be counted. Then, you can classify, mirror, or police accepted packets.

In the CLI, you configure the action parameters with the `policy access-list sequence action` command.

Each sequence in an access list can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Action Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the access list.</td>
</tr>
<tr>
<td>Counter</td>
<td>Name of a counter. To display counter information, use the <code>show policy access-lists counters</code> command on the Cisco IOS XE SD-WAN device.</td>
</tr>
<tr>
<td>Drop</td>
<td>Discards the packet. This is the default action.</td>
</tr>
<tr>
<td>Log</td>
<td>Logs the packet headers into the messages and syslog system logging (syslog) files.</td>
</tr>
<tr>
<td></td>
<td>In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
</tr>
<tr>
<td></td>
<td>To display logging information, use the <code>show app log flow-all</code>, <code>show app log flows</code>, and <code>show log</code> commands on the Cisco IOS XE SD-WAN device.</td>
</tr>
</tbody>
</table>

For a packet that is accepted, the following actions can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Specifies the name of a QoS class. It can also be defined with a <code>policy class-map</code> command.</td>
</tr>
<tr>
<td>Mirror List</td>
<td>Specifies the name of mirror. It is defined with a <code>policy mirror</code> command.</td>
</tr>
<tr>
<td>Policer</td>
<td>Specifies the name of a policer defined with a <code>policy policer</code> command.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the packet's DSCP value. The range is 0 through 63.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Specifies the IPv4 address. It sets the next hop IP address to which the packet should be forwarded.</td>
</tr>
</tbody>
</table>

**Note**: Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Release 17.5.1a, Use **Default Route when Next Hop is not available** field is available next to Next Hop action parameter.

Route Policy Parameters

Each sequence in a localized control policy can contain one action condition.

When a route matches the conditions in the match portion of a route policy, the route can be accepted or rejected:
For a packet that is accepted, the following actions can be configured:

<table>
<thead>
<tr>
<th>Description</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregator</td>
<td>Set the AS number in which a BGP route aggregator is located and the IP address of the route aggregator. The range is 1 through 65535.</td>
</tr>
<tr>
<td>As Path</td>
<td>Sets an AS number or a series of AS numbers to exclude from the AS path or to prepend to the AS path. The range is 1 through 65535.</td>
</tr>
<tr>
<td>Atomic Aggregate</td>
<td>Sets the BGP atomic aggregate attribute.</td>
</tr>
<tr>
<td>Community</td>
<td>Sets the BGP community value. Starting from Cisco IOS XE Release 17.5.1a, the Community Additive option field is available. Additive option appends the communities to the existing communities of the route.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>Sets the BGP local preference. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Metric</td>
<td>Sets the metric value. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Sets the metric type. The options are type1 or type2.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>Sets the IPv4 address. It sets the next hop IP address to which the packet should be forwarded. <strong>Note</strong> Starting from Cisco vManage Release 20.5.1 and Cisco IOS XE Release 17.5.1a, Use <strong>Default Route when Next Hop is not available</strong> field is available next to Next Hop action parameter.</td>
</tr>
<tr>
<td>OMP Tag</td>
<td>Sets the OMP tag for OSPF to use. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Origin</td>
<td>Sets the BGP origin code. The options are: EGP (default), IGP, Incomplete.</td>
</tr>
<tr>
<td>Originator</td>
<td>Sets the IP address from which the route was learned.</td>
</tr>
<tr>
<td>OSPF Tag</td>
<td>Sets the OSPF tag value. The range is 0 through 4294967295.</td>
</tr>
<tr>
<td>Weight</td>
<td>Sets the BGP weight. The range is 0 through 4294967295.</td>
</tr>
</tbody>
</table>

**Configure Policy Settings**

In **Policy Overview**, configure the policy settings:

1. In the **Enter name and description for your localized master policy** pane, enter name and description for the policy.
2. In the **Policy Settings** pane, select the policy application checkboxes that you want to configure. The options are:
   - **Netflow**: Perform traffic flow monitoring on IPv4 traffic.
   - **Netflow IPv6**: Perform traffic flow monitoring on IPv6 traffic.
   - **Application**: Track and monitor IPv4 applications.
   - **Application IPv6**: Track and monitor IPv6 applications.
- **Cloud QoS**: Enable QoS scheduling.
- **Cloud QoS Service Side**: Enable QoS scheduling on the service side.
- **Implicit ACL Logging**: Log the headers of all the packets that are dropped because they do not match a service perform traffic flow monitoring.

3. To configure how often packets flows are logged, click **Log Frequency**.
Packet flows are those that match an access list (ACL), a cflowd flow, or an application-aware routing flow.

4. Click **Preview** to view the full policy in CLI format.

5. Click **Save Policy**.

### Apply Localized Policy in a Device Template

1. From the Cisco vManage menu, choose **Configuration > Templates**.

2. If you are creating a new device template:
   a. Click **Device Templates**.

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

   b. From the **Create Template** drop-down, select **From Feature Template**.
   c. From the **Device Model** drop-down, select one of the Cisco IOS XE SD-WAN devices.
   d. In the **Template Name** field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
   e. In the **Description** field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
   f. Continue with Step 4.

3. If you are editing an existing device template:
   a. Click **Device Templates**, and for the desired template, click ... and select **Edit**.

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

   b. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.
   c. From the **Policy** drop-down, select the name of a policy that you have configured.

4. Click **Additional Templates** located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.
5. From the **Policy** drop-down, select the name of the policy you configured in the above procedure.
6. Click **Create** (for a new template) or **Update** (for an existing template).

**Activate a Localized Policy**

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click ... and select **Activate**.
3. In the **Activate Policy** popup, click **Activate** to push the policy to all reachable Cisco vSmart Controllers in the network.
4. Click **OK** to confirm activation of the policy on all Cisco vSmart Controllers.
5. To deactivate the localized policy, select =, and then select a policy.
6. For the desired policy, click ... and select **Deactivate**.
7. In the **Deactivate Policy** popup, click **Deactivate** to confirm that you want to remove the policy from all reachable Cisco vSmart Controllers.

**View Localized Policies**

To view localized policies:

1. Click **Localized Policy**, and select a policy.
2. For a policy created using the UI policy builder or using the CLI, click ... and select **View**. The policy created using the UI policy builder is displayed in graphical format while the policy created using the CLI method is displayed in text format.
3. For a policy created using the Cisco vManage policy configuration wizard, click ... and select **Preview**. This policy is displayed in text format.

**Copy, Edit, and Delete Policies**

To copy a policy:

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click ... and select **Copy**.
3. In the **Policy Copy** popup window, enter the policy name and a description of the policy.
Starting with the Cisco IOS XE Release 17.2, 127 characters are supported for policy names for the following policy types:

- Central route policy
- Local route policy
- Local Access Control List (ACL)
- Local IPv6 ACL
- Central data policy
- Central app route policy
- QoS map
- Rewrite rule

All other policy names support 32 characters.

4. Click **Copy**.

To edit policies created using the Cisco vManage policy configuration wizard:

1. For the desired policy, click ... and select **Edit**.
2. Edit the policy as needed.
3. Click **Save Policy Changes**.

To edit policies created using the CLI method:

1. From the **Custom Options** drop-down, under Localized Policy, select **CLI Policy**.
2. For the desired policy, click ... and select **Edit**.
3. Edit the policy as needed.
4. Click **Update**.

To delete policies:

1. Click **Localized Policy**, and select a policy.
2. For the desired policy, click ... and select **Delete**.
3. Click **OK** to confirm deletion of the policy.

**Configure Localized Policy for IPv4 Using the CLI**

Following are the high-level steps for configuring an access list using the CLI on Cisco IOS XE SD-WAN devices:

1. Create lists of IP prefixes as needed:
Device(config)# **policy lists data-prefix-list ipv4_prefix_list**
Device(config-data-prefix-list-ipv4_prefix_list)# ip-prefix 192.168.0.3/24

2. For QoS, configure the **class-map ios**:

Device(config)# **class-map match-any class1**
Device(config)# **match qos-group 1**
class-map match-any class6
match qos-group 6
class-map match-any class7
match qos-group 7
class-map match-any class4
match qos-group 4
class-map match-any class5
match qos-group 5
class-map match-any class2
match qos-group 2
class-map match-any class3
match qos-group 3
class-map match-any class1
match qos-group 1
end

Note  queue2 is optional here since we are using **class-default**.

3. For QoS, define rewrite rules to overwrite the DSCP field of a packet's outer IP header, if desired:

Device(config)# **policy rewrite-rule rule1**
Device(config-rewrite-rule-rule1)# **class class1** low dscp 3
Device(config-rewrite-rule-rule1)# **class class2** high dscp 4
Will be a table to map class-id → QoS-Group, QID, DSCP, Discard-Class

4. For QoS, map each forwarding class to an output queue, configure a QoS scheduler for each forwarding class, and group the QoS schedulers into a QoS map:

Device(config)# **policy class-map class class1 queue 1**
<0..7>[1]

5. For QoS map configuration, merge with interface shaping configuration, if shaping is configured.
If shaping is not configured, you can apply the **policy-map** generated for the **qos-map**.

Device(config)# **policy-map qos_map_for_data_policy**
<name:string>
Device(config-pmap)# **class class1** name:string
Device(config-pmap-c)# bandwidth percentage
Device(config-pmap-c)# random-detect

6. Configure a WAN interface without a shaping configuration:

Device(config)# **policy-map qos_map_for_data_policy name:string**
Device(config-pmap)# **class class1** name:string
Device(config-pmap-c)# bandwidth percentage
Device(config-pmap-c)# random-detect

7. Configure a WAN interface with a shaping configuration:

Device(config)# **policy-map shaping_interface**
Device(config-pmap)# **class class-default**
Device(config-pmap-c)# shape average 100000000(rate-in-bps)
Device(config-pmap-c)# service-policy qos_map_for_data_policy
8. Associate a service-policy to a Cisco IOS XE SD-WAN device:

   Device(config)# sdwan interface GigabitEthernet 1
   Device(config-if)# rewrite-rule rule1
   Device(config-if)# service-policy output qos_map_for_data_policy

9. Define policing parameters:

   Device(config)# policy policer policer_On_gige
   Device(config-policer-policer_On_gige)# rate ?
   Description: Bandwidth for 1g interfaces: <8..1000000000>bps; for 10g interfaces: <8..10000000000>bps
   Possible completions: <0..2^64-1>
   Device(config-policer-policer_On_gige)# burst
   Description: Burst rate, in bytes
   Possible completions: <15000..10000000>
   Device(config-policer-policer_On_gige)# exceed drop

10. Associate an access list set to policer:

    Device(config)# policy access-list ipv4_acl
    Device(config-access-list-ipv4_acl)# sequence 100
    Device(config-sequence-100)# match dscp 10
    Device(config-sequence-100)# action accept
    Device(config-sequence-100)# action count dscp_10_count
    Device(config-sequence-100)# action drop
    Device(config-sequence-100)# exit

11. Associate an access list to a LAN or a WAN interface:

    Device(config)# sdwan interface GigabitEthernet5
    Device(config-interface-GigabitEthernet5)# access-list ipv4_acl
    Device(config-interface-GigabitEthernet5)# commit

---

Configure Localized Policy for IPv6 Using the CLI

Following are the high-level steps for configuring an access list using the CLI:

1. Define policing parameters:

   Device(config)# policy policer policer_On_gige
   Device(config-policer-policer_On_gige)# rate ?
   Description: Bandwidth for 1g interfaces: <8..1000000000>bps; for 10g interfaces: <8..10000000000>bps
   Possible completions: <0..2^64-1>
   Device(config-policer-policer_On_gige)# burst
   Description: Burst rate, in bytes
   Possible completions: <15000..10000000>
   Device(config-policer-policer_On_gige)# exceed drop

2. Create an access list instance:

   Device (config)# policy ipv6 access-list ipv6_access_list

3. Create a series of match–action pair sequences:

   Device(config-access-list-ipv6_access_list)# sequence 100

   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).
4. Define match parameters for packets:

```bash
Device(config-sequence-100)# match traffic-class 10
Device(config-match)# exit
```

5. Define actions to take when a match occurs:

```bash
Device(config-sequence-100)# action accept count traffic_class10_count
Device(config-sequence-100)# action drop
Device(config-sequence-100)# action accept class class1
Device(config-sequence-100)# action accept policer policer_On_gige
```

6. Create additional numbered sequences of match-action pairs within the access list, as needed.

7. If a packet does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching packets to be accepted, configure the default action for the access list:

8. Apply the access list to an interface:

```bash
Device(config)# sdwan interface GigabitEthernet5
Device(config-interface-GigabitEthernet5)# ipv6 access-list ipv6_access_list in
Device(config-interface-GigabitEthernet5)# commit
```

Applying the access list in the inbound direction (in) affects packets being received on the interface. Applying it in the outbound direction (out) affects packets being transmitted on the interface.

---

**Localized Data Policy Configuration Examples**

This topic provides some straightforward examples of configuring localized data policy to help you get an idea of how to use policy to influence traffic flow across the Cisco SD-WAN domain. Localized data policy, also known as access lists, is configured directly on the local Cisco vEdge devices.

**QoS**

You can configure quality of service (QoS) to classify data packets and control how traffic flows out of and in to the interfaces on a Cisco vEdge device and on the interface queues. For examples of how to configure a QoS policy, see Forwarding and QoS Configuration Examples.

**ICMP Message Example**

This example displays the configuration for localized data policy for ICMP messages.

```
policy
access-list acl_1
sequence 100
match
  protocol 1
  icmp-msg administratively-prohibited
!
action accept
  count administratively-prohibited
!
```
CHAPTER 6

Redirect DNS in a Service-Side VPN

Table 15: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect DNS in a Service-Side VPN</td>
<td>Cisco IOS XE Release 17.8.1a</td>
<td>This feature allows you to configure a Cisco IOS XE SD-WAN device to respond to Domain Name System (DNS) queries using proxy servers. This feature adds support for DNS proxy for service-side VPN hosts and DNS redirects inside the service VPNs.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.8.1</td>
<td></td>
</tr>
</tbody>
</table>

- Information About Redirect DNS in a Service-Side VPN, on page 91
- Restrictions for Redirect DNS in a Service-Side VPN, on page 92
- Use Cases for Redirect DNS in a Service-Side VPN, on page 92
- Configure Redirect DNS in a Service-Side VPN Using Cisco vManage, on page 94
- Configure Redirect DNS in a Service-Side VPN Using the CLI, on page 96
- Verify Redirect DNS in a Service-Side VPN, on page 98
- Configuration Examples for Redirect DNS, on page 98

Information About Redirect DNS in a Service-Side VPN

The Redirect DNS feature enables Cisco IOS XE SD-WAN devices to respond to DNS queries using a specific configuration and associated host table cache that are selected based on certain characteristics of the queries. In a redirect DNS environment, multiple DNS databases can be configured on the device. The Cisco SD-WAN software can be configured to choose one of the DNS name server configurations whenever the device responds to a DNS query, by forwarding or resolving the query. Prior to Cisco IOS XE Release 17.8.1a, redirect DNS is supported only through NAT Direct Internet Access (DIA) path.

When an application-aware routing policy allows a Cisco IOS XE SD-WAN device to send application traffic to a service VPN and receive application traffic from a service VPN, the device performs a DNS lookup to determine the path to reach the application server. If the router does not have a connection to the internet, it sends DNS queries to an edge device that has such a connection, and that device determines how to reach a server for that application.
Note
In a network in which the device that is connected to the internet is in a geographically distant data center, the resolved DNS address points to a server that is also geographically distant from the site where the service VPN is located.

Because you can configure a Cisco IOS XE SD-WAN device to be an internet exit point, it is possible for any router to reach the internet directly to perform DNS lookups.

You can configure redirect DNS with either a centralized data policy or, if you want to apply SLA criteria to the data traffic, you can use application-aware routing policy.

Restrictions for Redirect DNS in a Service-Side VPN

- A redirect DNS request is not accepted without NAT configuration if the request is from the same VPN with the same port from a different host.
- If you configure DNS server IP address using NAT, it cannot be changed through the data policy.
- DNS fragmented packets and self-generated DNS are not supported.
- DNS requests from the overlay tunnel are not supported.
- Redirect DNS is supported only on IPv4 traffic, and not on IPv6 traffic.
- DNS requests through User Datagram Protocol (UDP) are supported. However, requests from Transmission Control Protocol (TCP) are not supported.

Use Cases for Redirect DNS in a Service-Side VPN

Unconditional Redirect DNS

In unconditional redirect DNS (scenario A), a host sends all the DNS requests to a local edge router, and the local edge router redirects the DNS request to an enterprise DNS server in the data center (which is available only using a service-side VPN) and acts as a DNS forwarder. A use case for this feature redirects statically configured IP addresses for printers to an enterprise DNS server in a data center. In this use case, all the legacy printers are statically configured with an IP address of a local router as DNS server, which acts as DNS forwarder to forward all the DNS requests from printers.
In conditional redirect DNS (scenario B), a host uses a service provider (SP) or managed service provider (MSP) DNS by default. For known applications that use an SD-WAN Application Intelligence Engine (SAIE) or custom applications, for example, *.google.com, the DNS request is forwarded to the enterprise DNS server using a Cisco SD-WAN overlay network. All the other DNS requests are sent to the SP or MSP DNS server.

Note

In Cisco vManage Release 20.7.x and earlier releases, SAIE is called deep packet inspection (DPI).
Configure Redirect DNS in a Service-Side VPN Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration > Policies**.
2. From the **Custom Options** drop-down list, choose **Traffic Policy** from the **Centralized Policy** menu.
3. Click **Traffic Data** to create a traffic data policy.
4. From the **Add Policy** drop-down list, choose **Create New**.
5. In the **Name** and **Description**, enter a name and a description for the data policy.
6. Click **Sequence Type**.
   The **Add Data Policy** dialog box is displayed.
7. Choose the type of data policy that you want to create—**Application Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom**.
   A policy sequence containing the selected type of data policy is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence.
   The name you type is displayed both in the **Sequence Type** list in the left pane and in the right pane.
9. Click **Sequence Rule**. The **Match/Action** dialog box is displayed, where **Match** is selected by default.
   The available policy match conditions are listed in the menu.
10. From the **Protocol** drop-down list, choose **IPv4** to apply the policy only to IPv4 address families.
11. To choose one or more Match conditions, click the fields and set the values as described.

Note: Not all match conditions are available for all policy sequence types.

12. To select the actions to take on matching data traffic, click the Actions menu.
13. To drop matching traffic, click Drop. The available policy actions are listed on the right side.
14. To accept matching traffic, click Accept. The available policy actions are listed on the right side.
15. In the Actions menu, choose Redirect DNS to configure redirect DNS.
16. In the Redirect DNS condition field, enter the IP Address and click Save Match and Actions.
17. Click Save Data Policy.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all the packets)</td>
<td>Do not specify any match conditions.</td>
</tr>
<tr>
<td>Applications/Application Family List / Custom Applications</td>
<td></td>
</tr>
<tr>
<td>1. In the Match conditions menu, click Applications/Application Family List.</td>
<td></td>
</tr>
<tr>
<td>2. From the drop-down list, choose the application family.</td>
<td></td>
</tr>
<tr>
<td>3. To create an application list:</td>
<td></td>
</tr>
<tr>
<td>a. Click New Application List.</td>
<td></td>
</tr>
<tr>
<td>b. Enter a name for the list.</td>
<td></td>
</tr>
<tr>
<td>c. Click Application to create a list of individual applications. Click Application Family to create a list of related applications.</td>
<td></td>
</tr>
<tr>
<td>d. From the Select Application drop-down list, choose the corresponding applications or application families.</td>
<td></td>
</tr>
<tr>
<td>e. Click Save.</td>
<td></td>
</tr>
<tr>
<td>DNS Application List</td>
<td>Add an application list to enable split DNS:</td>
</tr>
<tr>
<td>1. In the Match conditions menu, click DNS Application List.</td>
<td></td>
</tr>
<tr>
<td>2. From the drop-down list, choose the application family.</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>Add an application list to process split DNS:</td>
</tr>
<tr>
<td>1. In the Match conditions menu, click DNS.</td>
<td></td>
</tr>
<tr>
<td>2. From the drop-down list, choose Request to process DNS requests for the DNS applications.</td>
<td></td>
</tr>
<tr>
<td>Match Condition</td>
<td>Procedure</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Destination Data Prefix** | 1. In the **Match** conditions menu, click **Destination Data Prefix**.  
2. To match a list of destination prefixes, from the **Data Prefix** drop-down list, choose a list.  
3. To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field. |
| **Destination Port**     | 1. In the **Match** conditions menu, click **Destination Port**.  
2. In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with two numbers separated with a hyphen [-]). |
| **DSCP**                 | 1. In the **Match** conditions menu, click **DSCP**.  
2. In the **DSCP** field, enter the DSCP value—a number from 0 through 63. |
| **Packet Length**        | 1. In the **Match** conditions menu, click **Packet Length**.  
2. In the **Packet Length** field, enter the length—a value from 0 through 65535. |
| **PLP**                  | 1. In the **Match** conditions menu, click **PLP** to set the **Packet Loss Priority**.  
2. From the **PLP** drop-down list, choose **Low** or **High**. |
| **Protocol**             | 1. In the **Match** conditions menu, click **Protocol**.  
2. In the **Protocol** field, enter the Internet Protocol number—a number from 0 through 255. |
| **Source Data Prefix**   | 1. In the **Match** conditions menu, click **Source Data Prefix**.  
2. To match a list of source prefixes, from the **Source Data Prefix List** drop-down list, choose a data prefix list.  
3. To match an individual source prefix, enter the prefix in the **Source** field. |
| **Source Port**          | 1. In the **Match** conditions menu, click **Source Port**.  
2. In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). |

Configure Redirect DNS in a Service-Side VPN Using the CLI

The following steps show the minimum policy components required to enable redirect DNS with a centralized data policy:

1. Create a list of overlay network sites to which the centralized control policy is to be applied:
vsmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id

The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with an end dash (–). Create additional site lists, as needed.

2. Create lists of applications or application families for which you want to enable redirect DNS. Refer to these lists in the match section of the data policy.

vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name | app-family family-name

3. Create list VPNs to which the redirect DNS policy is to be applied:

vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists)# vpn vpn-id

4. Create a data policy instance and associate it with a list of VPNs:

vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# vpn-list list-name

5. Create a series of match–action pair sequences:

vSmart(config-vpn-list)# sequence number

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or, if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

6. Process the DNS server resolution for the applications or application families contained in an application list. For the list-name argument, specify the list name.

vSmart(config-sequence)# match dns-app-list list-name

7. Configure the match–action pair sequence to process DNS requests (for outbound data traffic) or responses (for inbound data traffic):

vSmart(config-sequence)# match dns (request | response)

8. By default, the DNS servers configured in the VPN in which the policy is applied are used to process DNS lookups for the applications. You can direct the DNS requests to a particular DNS server. For a data policy condition that applies to outbound traffic (from the service network), configure the IP address of the DNS server:

vSmart(config-sequence)# action accept redirect-dns ip-address

For a data policy condition that applies to inbound traffic (from the tunnel), include the following action so that the DNS response can be correctly forwarded back to the service VPN:

vSmart(config-sequence)# action accept redirect-dns host

9. Apply the policy to one or more sites in the Cisco SD-WAN overlay network:

vSmart(config)# apply-policy site-list list-name
data-policy policy-name [all | from-service]
Verify Redirect DNS in a Service-Side VPN

The following is a sample output from the show sdwan policy from-vsmart command that shows how to verify the redirect DNS configuration:

```
vSmart# show sdwan policy from-vsmart
from-vsmart data-policy vpn1_dns-redirect-prefer-lte
direction from-service
vpn-list vpn1
sequence 1
match
  source-ip 10.0.0.0/0
dns  request
action accept
  count  gdns2_-396115821
redirect-dns 10.255.255.254
default-action accept
from-vsmart lists vpn-list vpn1
vpn 1
```

Configuration Examples for Redirect DNS

Unconditional DNS Redirect

The following example shows how to configure an unconditional DNS redirect, where all the DNS requests are matched:

```
policy
data-policy rdns
vpn-list vpn10
sequence 10
match
  source-ip 0.0.0.0/0
dns request
!
action
  redirect-dns 209.165.200.225
!
default-action accept
!
!
apply-policy
site-list siteA
data-policy rdns from-service
```

Conditional DNS Redirect

The following example shows how to configure a conditional DNS redirect, where a selective DNS request is defined using an app list:

```
policy
data-policy rdns
vpn-list vpn10
sequence 10
```
match
  source-ip 10.0.0.0/8
  dns  request
  dns-app-list YouTube
!
action
  redirect-dns 209.165.200.225
  !
  default-action accept
  !
  !
apply-policy
  site-list siteA
  data-policy rdns from-service
Default AAR and QoS Policies

Table 16: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Default AAR and QoS Policies</td>
<td>Cisco IOS XE Release 17.7.1a</td>
<td>This feature enables you to efficiently configure default application-aware routing (AAR), data, and quality of service (QoS) policies for Cisco IOS XE SD-WAN devices. The feature provides a step-by-step workflow for categorizing the business relevance, path preference, and other parameters for network applications, and applying those preferences as traffic policy.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.7.1</td>
<td></td>
</tr>
</tbody>
</table>

• Information About Default AAR and QoS Policies, on page 101
• Prerequisites for Default AAR and QoS Policies, on page 102
• Restrictions for Default AAR and QoS Policies, on page 103
• Supported Devices for Default AAR and QoS Policies, on page 103
• Use Cases for Default AAR and QoS Policies, on page 103
• Configure Default AAR and QoS Policies Using Cisco vManage, on page 103
• Monitor Default AAR and QoS Policies, on page 107

Information About Default AAR and QoS Policies

It is often helpful to create an AAR policy, a data policy, and a QoS policy for devices in a network. These policies route and prioritize traffic for best performance. When creating these policies, it is helpful to distinguish among the applications producing network traffic, based on the likely business relevance of the applications, and to give higher priority to business-relevant applications.

Cisco vManage provides an efficient workflow to help you create a default set of AAR, data, and QoS policies to apply to devices in the network. The workflow presents a set of more than 1000 applications that can be identified by network-based application recognition (NBAR), an application recognition technology built into Cisco IOS XE SD-WAN devices. The workflow groups the applications into one of three business-relevance categories:

• Business-relevant: Likely to be important for business operations, for example, Webex software.
• Business-irrelevant: Unlikely to be important for business operations, for example, gaming software.
• Default: No determination of relevance to business operations.

Within each of the business-relevance categories, the workflow groups the applications into application lists, such as broadcast video, multimedia conferencing, VoIP telephony, and so on.

Using the workflow, you can accept the predefined categorization of each application's business relevance or you can customize the categorization of specific applications by moving them from one of the business-relevance categories to another. For example, if, by default, the workflow predefines a specific application as business-irrelevant, but that application is important for your business operations, then you can recategorize the application as Business-relevant.

The workflow provides a step-by-step procedure for configuring the business relevance, path preference, and service level agreement (SLA) category.

After you complete the workflow, Cisco vManage produces a default set of the following:

• AAR policy
• QoS policy
• Data policy

After you attach these policies to a centralized policy, you can apply these default policies to Cisco IOS XE SD-WAN devices in the network.

**Background Information About NBAR**

NBAR is an application recognition technology included in Cisco IOS XE SD-WAN devices. NBAR uses a set of application definitions called protocols to identify and categorize traffic. One of the categories that it assigns to traffic is the business-relevance attribute. The values of this attribute are Business-relevant, Business-irrelevant, and Default. In developing protocols to identify applications, Cisco estimates whether an application is likely to be important for typical business operations, and assigns a business-relevance value to the application. The default AAR and QoS policy feature uses the business-relevance categorization provided by NBAR.

**Benefits of Default AAR and QoS Policies**

• Manage and customize bandwidth allocations.
• Prioritize applications based on their relevance to your business.

**Prerequisites for Default AAR and QoS Policies**

• Knowledge about the relevant applications.
• Familiarity with the SLAs and QoS markings to prioritize traffic.
Restrictions for Default AAR and QoS Policies

- When you customize a business-relevant application group, you cannot move all the applications from that group to another section. Application groups of business-relevant section need to have at least one application in them.
- Default AAR and QoS policies do not support IPv6 addressing.

Supported Devices for Default AAR and QoS Policies

- Cisco 1000 Series Integrated Services Routers (ISR1100-4G and ISR1100-6G)
- Cisco 4000 Series Integrated Services Routers (ISR44xx)
- Cisco Catalyst 8000V Edge Software
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms

Use Cases for Default AAR and QoS Policies

If you are setting up a Cisco SD-WAN network and want to apply an AAR and a QoS policy to all the devices in a network, use this feature to create and deploy these policies quickly.

Configure Default AAR and QoS Policies Using Cisco vManage

Follow these steps to configure default AAR, data, and QoS policies using Cisco vManage:

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Add Default AAR & QoS.
   The Process Overview page is displayed.
3. Click Next.
   The Recommended Settings based on your selection page is displayed.
4. Based on the requirements of your network, move the applications between the Business Relevant, Default, and Business Irrelevant groups.

   Note
   When customizing the categorization of applications as Business-relevant, Business-irrelevant, or Default, you can only move individual applications from one category to another. You cannot move an entire group from one category to another.

5. Click Next.
On the **Path Preferences (optional)** page, choose the **Preferred** and **Preferred Backup** transports for each traffic class.

6. Click **Next**.

The **App Route Policy Service Level Agreement (SLA) Class** page is displayed.

This page shows the default settings for **Loss**, **Latency**, and **Jitter** values for each traffic class. If necessary, customize **Loss**, **Latency**, and **Jitter** values for each traffic class.

7. Click **Next**.

The **Enterprise to Service Provider Class Mapping** page is displayed.

a. Select a service provider class option, based on how you want to customize bandwidth for different queues. For further details on QoS queues, refer to the section **Mapping of Application Lists to Queues**

b. If necessary, customize the bandwidth percentage values for each queues.

8. Click **Next**.

The **Define prefixes for the default policies and applications lists** page is displayed.

For each policy, enter a prefix name and description.

9. Click **Next**.

The **Summary** page is displayed. On this page, you can view the details for each configuration.

You can click **Edit** to edit the options that appeared earlier in the workflow. Clicking edit returns you to the relevant page.

10. Click **Configure**.

Cisco vManage creates the AAR, data, and QoS policies and indicates when the process is complete.

The following table describes the workflow steps or actions and their respective effects:

<table>
<thead>
<tr>
<th>Workflow Step</th>
<th>Affects the Following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended Settings based on your selection</td>
<td>AAR and data policies</td>
</tr>
<tr>
<td>Path Preferences (optional)</td>
<td>AAR policies</td>
</tr>
<tr>
<td>App Route Policy Service Level Agreement (SLA) Class:</td>
<td>AAR policies</td>
</tr>
<tr>
<td>• Loss</td>
<td></td>
</tr>
<tr>
<td>• Latency</td>
<td></td>
</tr>
<tr>
<td>• Jitter</td>
<td></td>
</tr>
<tr>
<td>Enterprise to Service Provider Class Mapping</td>
<td>Data and QoS policies</td>
</tr>
<tr>
<td>Define prefixes for the default policies and applications</td>
<td>AAR, data, QoS policies, forwarding classes, application lists, SLA class lists</td>
</tr>
</tbody>
</table>
To view the policy, click **View Your Created Policy**.

**Note**
To apply the default AAR and QoS policies to the devices in the network, create a centralized policy that attaches the AAR and data policies to the required site lists. To apply the QoS policy to the Cisco IOS XE SD-WAN devices, attach it to a localized policy through device templates.

**Mapping of Application Lists to Queues**

The following lists show each service provider class option, the queues in each option, and the application lists included in each queue. The application lists are named here as they appear on the Path Preferences page in this workflow.

4 QoS class
- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data
- Default
  - Best effort
  - Scavenger

5 QoS class
- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
• Broadcast video
• Multimedia conferencing
• Real-Time interactive
• Multimedia streaming

• Business data
  • Signaling
  • Transactional data
  • Network management
  • Bulk data

• General data
  • Scavenger

• Default
  • Best effort

6 QoS class
• Voice
  • Internetwork control
  • VoIP telephony

• Video
  • Broadcast video
  • Multimedia conferencing
  • Real-Time interactive

• Mission Critical
  • Multimedia streaming

• Business data
  • Signaling
  • Transactional data
  • Network management
  • Bulk data

• General data
  • Scavenger
Monitor Default AAR and QoS Policies

Monitor Default AAR Policies

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Custom Options.
3. Choose Traffic Policy from Centralized Policy.

4. Click Application Aware Routing.
   A list of AAR policies is displayed.

5. Click Traffic Data.
   A list of traffic data policies is displayed.

**Monitor QoS Policies**

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Custom Options.
3. Choose Forwarding Class/QoS from Localized Policy.
4. Click QoS Map.
   A list of QoS policies is displayed.

---

**Note** To verify QoS policies, refer to Verify QoS Policy.
Device Access Policy

Table 18: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Access Policy on SNMP and SSH</td>
<td>Cisco IOS XE Release 17.2.1r</td>
<td>This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. The control plane of a Cisco IOS XE SD-WAN device processes the data traffic for local services (like SSH and SNMP) from a set of sources. Routing packets are required to form the overlay.</td>
</tr>
</tbody>
</table>

- Device Access Policy Overview, on page 109
- Configure Device Access Policy Using Cisco vManage, on page 110
- Configure Device Access Policy Using the CLI, on page 111
- Examples for ACL Statistics and Counters, on page 111
- Verifying ACL Policy on an SNMP Server, on page 113
- Verifying ACL Policy on SSH, on page 114

Device Access Policy Overview

Starting from Cisco IOS XE SD-WAN Release 17.2.1r, the Cisco vManage user interface is enhanced to configure device access policy on all the Cisco IOS XE SD-WAN devices.

The control plane of Cisco IOS XE SD-WAN devices process the data traffic for local services like, SSH and SNMP, from a set of sources. It is important to protect the CPU from device access traffic by applying the filter to avoid malicious traffic.

Access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies, in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol used, the source and destination IP address or network, and optionally, the users and user groups. Each incoming packet at an interface is analyzed to determine if it must be forwarded or dropped based on criteria you specify. If you define access rules for the outgoing traffic, packets are also analyzed before they are allowed to leave an interface. Access policies are applied in order. That is, when the device compares a packet to the rules, it searches from top to bottom in the access policies list, and applies the policy.
for the first matched rule, ignoring all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure the specific rules are not skipped.

## Configure Device Access Policy Using Cisco vManage

Cisco IOS XE SD-WAN devices support device access policy configuration to handle SNMP and SSH traffic directed towards the control plane. Use Cisco vManage to configure destination ports based on the device access policy.

**Note**

In order to allow connections to devices from **Tools > SSH Terminal** in Cisco vManage, create a rule to accept **Device Access Protocol** as SSH and **Source Data Prefix** as 192.168.1.5/32.

To configure localized device access control policies, use the Cisco vManage policy configuration wizard. Configure specific or all components depending on the specific policy you are creating. To skip a component, click the **Next** button. To return to a component, click the **Back** button at the bottom of the screen.

To configure a device access policy:

1. From the Cisco vManage menu, choose **Configuration > Policies**.
2. Click **Localized Policy** and from the **Custom Options** drop-down, under **Localized Policy**, select **Access Control Lists**.
3. From the **Add Device Access Policy** drop-down list, select **Add IPv4 Device Access Policy** or **Add IPv6 Device Access Policy** option to add a device.
4. Select **Add IPv4 Device Access Policy** from the drop-down list to add an **IPv4 ACL Policy**. The edit **Device IPv4 ACL Policy** page appears.
5. Enter the name and the description for the new policy.
6. Click **Add ACL Sequence** to add a sequence. The **Device Access Control List** page is displayed.
7. Click **Sequence Rule. Match** and **Actions** options are displayed.
8. Click **Match**, select and configure the following conditions for your ACL policy:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Access Protocol</strong> (required)</td>
<td>Select a carrier from the drop-down list. For example SNMP, SSH.</td>
</tr>
<tr>
<td><strong>Source Data Prefix</strong></td>
<td>Enter the source IP address. For example, 10.0.0.0/12.</td>
</tr>
<tr>
<td><strong>Source Port</strong></td>
<td>Enter the list of source ports. The range is 0-65535.</td>
</tr>
<tr>
<td><strong>Destination Data Prefix</strong></td>
<td>Enter the destination IP address. For example, 10.0.0.0/12.</td>
</tr>
<tr>
<td><strong>VPN</strong></td>
<td>Enter the VPN ID. The range is 0-65536.</td>
</tr>
</tbody>
</table>

9. Click **Actions**, configure the following conditions for your ACL policy:
Configure Device Access Policy Using the CLI

Configuration:

```
ip access-list standard snmp-acl
  1 permit 10.0.1.12 255.255.255.0
  11 deny any
!
snmp-server community private view v2 ro snmp-acl

ip access-list extended ssh-acl
  1 permit tcp host 10.0.1.12 any eq 22
  11 deny tcp any any eq 22
!
line vty 0 4
  access-class ssh-acl in vrf-also
!```

Note IPv6 prefix match is not supported on Cisco IOS XE SD-WAN devices.

Examples for ACL Statistics and Counters

To configure ACL statistics and counters using yang:

```
Yang file: Cisco-IOS-XE-acl-oper.yang```
Example configuration using yang model:

Router# show access-lists access-list ACL-1
ACCESS
CONTROL
LIST   RULE   MATCH
NAME   NAME   COUNTER
-------------------------------
ACL-1   1       0
2       0

Router# show access-lists access-list ACL-1 | display xml
<?xml version="1.0" encoding="UTF-8"?>
<config xmlns="http://tail-f.com/ns/config/1.0">
  <access-lists xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-acl-oper">
    <access-list>
      <access-control-list-name>ACL-1</access-control-list-name>
      <access-list-entries>
        <access-list-entry>
          <rule-name>1</rule-name>
          <access-list-entries-oper-data>
            <match-counter>0</match-counter>
          </access-list-entries-oper-data>
        </access-list-entry>
        <access-list-entry>
          <rule-name>2</rule-name>
          <access-list-entries-oper-data>
            <match-counter>0</match-counter>
          </access-list-entries-oper-data>
        </access-list-entry>
      </access-list-entries>
    </access-list>
  </access-lists>
</config>

To display ACL statistics and counters using the CLI, use the command:

show ip access-list [access-list-number | access-list-name]

Example statistics output using the CLI:

show ip access-list [access-list-number | access-list-name]

Router# show ip access-list ACL-1
Extended IP access list ACL-1
10 permit ip host 10.1.1.1 any (3 matches) 30
30 permit ip host 10.2.2.2 any (27 matches)

To clear counters in ACL stats:

clear ip access-list counters [access-list-number | access-list-name]
Verifying ACL Policy on an SNMP Server

Starting from the Cisco IOS XE Release 17.2.1r release, Cisco IOS XE SD-WAN devices support the device-access-policy feature on SNMP servers. In case of SNMP, Cisco VManage validates to block the template push on the device if the SNMP feature template is not configured.

Configuration:

```
snmp-server community private view v2 ro snmp-acl
```

Yang model for the command `snmp-server community`. Following is the ACL settings sample from the yang model:

```
container community {
    description
        "Configure a SNMP v2c Community string and access privs";
        tailf:cli-compact-syntax;
        tailf:cli-sequence-commands;
        leaf community-string {
            tailf:cli-drop-node-name;
            type string;
        }
        container access {
            tailf:cli-drop-node-name;
            tailf:cli-flatten-container;
            leaf standard-acl {
                tailf:cli-drop-node-name;
                tailf:cli-full-command;
                type uint32 {
                    range "1..99";
                }
            }
            leaf expanded-acl {
                tailf:cli-drop-node-name;
                tailf:cli-full-command;
                type uint32 {
                    range "1300..1999";
                }
            }
            leaf acl-name {
                tailf:cli-drop-node-name;
                tailf:cli-full-command;
                type string;
            }
            leaf ipv6 {
                description
                    "Specify IPv6 Named Access-List";
                tailf:cli-full-command;
                type string;
            }
            leaf ro {
                description
                    "Read-only access with this community string";
                type empty;
            }
            leaf rw {
                description
                    "Read-write access with this community string";
                type empty;
            }
        }
}
```
Following is the sample test log for snmp-server ACL settings:

```
Device# sh sdwan ver
16.12.1
Device# config-t
admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_1 RO 80
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
```

```
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:17:19.377: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 518
Device#
```

```
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
Device#
```

```
admin connected from 127.0.0.1 using console on the device
Device(config)# snmp-server community TEST_V6 ipv6 acl-name-1
Device(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
```

```
session_id_for_dmi_vty_100001 from console as NETCONF on vty31266
*Mar 13 21:18:10.041: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by
admin, transaction-id 535
Device#
```

```
Device# sh sdwan run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 ipv6 acl-name-1
Device#
```

```
Device# sh run | i snmp
snmp-server community TEST_1 RO 80
snmp-server community TEST_V6 RO ipv6 acl-name-1
Device#
```

Verifying ACL Policy on SSH

Starting from the Cisco IOS XE Release 17.2.1r release, the Cisco IOS XE SD-WAN devices support
device-access-policy features on SSH servers using Virtual Teletype (VTY) lines. Cisco vManage uses all
the available VTY lines in the backend and pushes the policy accordingly.

Configuration:
```
line vty 0 4
   access-class ssh-acl in vrf-also
```
Following is the ACL settings sample from the yang model:

```yaml
// line */ access-class
container access-class {
    description
    "Filter connections based on an IP access list";
    tailf:cli-compact-syntax;
    tailf:cli-sequence-commands;
    tailf:cli-reset-container;
    tailf:cli-flatten-container;
    list access-list {
        tailf:cli-drop-node-name;
        tailf:cli-compact-syntax;
        tailf:cli-reset-container;
        tailf:cli-suppress-mode;
        tailf:cli-delete-when-empty;
        key "direction";
        leaf direction {
            type enumeration {
                enum "in";
                enum "out";
            }
        }
        leaf access-list {
            tailf:cli-drop-node-name;
            tailf:cli-prefix-key;
            type ios-types:exp-acl-type;
            mandatory true;
        }
        leaf vrf-also {
            description
            "Same access list is applied for all VRFs";
            type empty;
        }
    }
}
```

Following is the sample test log for line-server ACL settings:

```
Device# config transaction
admin connected from 127.0.0.1 using console on Device
Device(config)# line vty 0 4
Device(config-line)# access-class acl_1 in vrf-also
Device(config-line)# transport input ssh
Device(config-line)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
Device#
```

```
May 24 20:51:02.994: %SYS-5-CONFIG_P: Configured programmatically by process iosp_vty_100001.dmi.ned from console as NETCONF on vty31266
May 24 20:51:02.995: %DMI-5-CONFIG_I: R0/0: nesd: Configured from NETCONF/RESTCONF by admin, transaction-id 227
Device#
```

```
Device# show sdwan run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
```

```
Device# line vty 0 4
access-class acl_1 in vrf-also
login local
transport input ssh
line vty 5 80
login local
transport input ssh
```
Device#
Device# sh run | sec vty
Error: Licensing infrastructure is NOT initialized.
Error: Licensing infrastructure is NOT initialized.
line vty 0 4
  access-class acl_1 in vrf-also
  exec-timeout 0 0
  password 7 11051807
  login local
  transport preferred none
  transport input ssh
line vty 5 80
  login local
  transport input ssh
SD-WAN Application Intelligence Engine Flow

The topics in this section provide overview information about the SD-WAN Application Intelligence Engine (SAIE) flow, and how to configure the flow using Cisco vManage or the CLI.

Note

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

- SD-WAN Application Intelligence Engine Flow Overview, on page 117
- Configure SD-WAN Application Intelligence Engine Flow Using Cisco vManage, on page 118
- Configure SD-WAN Application Intelligence Engine Flow Using the CLI, on page 122

SD-WAN Application Intelligence Engine Flow Overview

The SD-WAN Application Intelligence Engine (SAIE) flow provides the ability to look into the packet past the basic header information. The SAIE flow determines the contents of a particular packet, and then either records that information for statistical purposes or performs an action on the packet.

Note

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

Benefits include increased visibility into the network traffic, which enables network operators to understand usage patterns and to correlate network performance information along with providing usage base billing or even acceptable usage monitoring. The SAIE flow can also reduce the overall costs on the network.

You can configure the SAIE flow using a centralized data policy. You define the applications of interest in a Cisco vManage policy list or with the `policy lists app-list` CLI command, and you call these lists in a `policy data-policy` command. You can control the path of the application traffic through the network by defining, in the `action` portion of the data policy, the local TLOC or the remote TLOC, or for strict control, you can define both.
Configure SD-WAN Application Intelligence Engine Flow Using Cisco vManage

To configure the SD-WAN Application Intelligence Engine (SAIE) flow, use the Cisco vManage policy configuration wizard. The wizard consists of the following sequential screens that guide you through the process of creating and editing policy components:

- Create Applications or Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy. For configuration details, see Configure Groups of Interest.
- Configure Traffic Rules—Create the match and action conditions of a policy. For configuration details, see Configure Traffic Rules.
- Apply Policies to Sites and VPNs—Associate policy with sites and VPNs in the overlay network.

**Note**
In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

Apply Centralized Policy for SD-WAN Application Intelligence Engine Flow

To ensure that a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow takes effect, you must apply it to a list of sites in the overlay network.

**Note**
In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

To apply a centralized policy in Cisco vManage, see Configure Centralized Policy Using Cisco vManage.

To apply a centralized policy in the CLI:

```bash
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
```

By default, data policy applies to all data traffic passing through the Cisco vSmart Controller: the policy evaluates all data traffic going from the local site (that is, from the service side of the router) into the tunnel interface, and it evaluates all traffic entering to the local site through the tunnel interface. You can explicitly configure this behavior by including the `all` option. To have the data policy apply only to policy exiting from the local site, include the `from-service` option. To have the policy apply only to incoming traffic, include the `from-tunnel` option.

You cannot apply the same type of policy to site lists that contain overlapping site IDs. That is, all data policies cannot have overlapping site lists among themselves. If you accidentally misconfigure overlapping site lists, the attempt to commit the configuration on the Cisco vSmart Controller fails.
Monitor Running Applications

To enable the SD-WAN Application Intelligence Engine (SAIE) infrastructure on Cisco vEdge devices, you must enable application visibility on the devices:

Note

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

vEdge(config)# policy app-visibility

To display information about the running applications, use the `show app dpi supported-applications`, `show app dpi applications`, and `show app dpi flows` commands on the device.

View SAIE Applications

You can view the list of all the application-aware applications supported by the Cisco SD-WAN software on the router using the following steps:

1. From the Cisco vManage menu, choose Monitor > Devices.
   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose Monitor > Network.

2. Click WAN-Edge, select the Device that supports the SD-WAN Application Intelligence Engine (SAIE) flow. The Cisco vManage Control Connections page is displayed.

Note

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

3. In the left pane, select Real Time to view the device details.

4. From the Device Options drop-down, choose SAIE Applications to view the list of applications running on the device.

5. From the Device Options drop-down, choose SAIE Supported Applications to view the list of applications that are supported on the device.

Action Parameters for Configuring SD-WAN Application Intelligence Engine Flow

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped, and it can be counted. Then, you can associate parameters with accepted packets.

From the Cisco vManage menu, you can configure match parameters from:

- Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > (Application-Aware Routing | Traffic Data | Cflowd) > Sequence Type > Sequence Rule > Action

In the CLI, you configure the action parameters under the `policy data-policy vpn-list sequence action` command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco vManage</th>
<th>CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.</td>
<td>Click <strong>Accept</strong>.</td>
<td>accept</td>
<td>—</td>
</tr>
<tr>
<td>Count the accepted or dropped packets.</td>
<td><strong>Action Counter</strong></td>
<td>count <strong>counter-name</strong></td>
<td>Name of a counter. Use the <code>show policy access-lists counters</code> command on the Cisco device.</td>
</tr>
<tr>
<td>Discard the packet. This is the default action.</td>
<td>Click <strong>Drop</strong>.</td>
<td>drop</td>
<td>—</td>
</tr>
</tbody>
</table>

To view the packet logs, use the `show app log flow` and `show log` commands.

Then, for a packet that is accepted, the following parameters can be configured.

**Note**

You cannot use the SD-WAN Application Intelligence Engine (SAIE) flow with either cflowd or NAT.

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco vManage</th>
<th>CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP value.</td>
<td>Click <strong>Accept</strong>, then action <strong>DSCP</strong>.</td>
<td><code>set dscp value</code></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Forwarding class.</td>
<td>Click <strong>Accept</strong>, then action <strong>Forwarding Class</strong>.</td>
<td><code>set forwarding-class value</code></td>
<td>Name of forwarding class</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco vManage</td>
<td>CLI Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Direct matching packets to a TLOC that matches the color and encapsulation</td>
<td>Click Accept, then action Local TLOC.</td>
<td>set local-tloc color [encap encapsulation]</td>
<td>color can be: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green lte, metro-ethernet mpls, private1 through private6, public-internet, red, and silver. By default, encapsulation is ipsec. It can also be gre.</td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct matching packets to one of the TLOCs in the list if the TLOC matches the color and encapsulation</td>
<td>Click Accept, then action Local TLOC</td>
<td>set local-tloc-list color color [encap encapsulation] [restrict]</td>
<td></td>
</tr>
<tr>
<td>By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the restrict option.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set the next hop to which the packet should be forwarded.</td>
<td>Click Accept, then action Next Hop.</td>
<td>set next-hop ip-address</td>
<td>IP address</td>
</tr>
<tr>
<td>Apply a policer.</td>
<td>Click Accept, then action Policer.</td>
<td>set policer policer-name</td>
<td>Name of policer configured with a policy policer command.</td>
</tr>
<tr>
<td>Direct matching packets to the name service, before delivering the traffic to its ultimate destination.</td>
<td>Click Accept, then action Service.</td>
<td>set service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]</td>
<td>Standard services: FW, IDS, IDP. Custom services: netsvc1, netsvc2, netsvc3, netsvc4 TLOC list is configured with a policy lists tloc-list list.</td>
</tr>
<tr>
<td>The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The VPN identifier is where the service is located.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the services themselves on the Cisco devices that are collocated with the service devices, using the vpn service configuration command.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct matching packets to the named service that is reachable using a GRE tunnel whose source is in the transport VPN (VPN 0). If the GRE tunnel used to reach the service is down, packet routing falls back to using standard routing. To drop packets when a GRE tunnel to the service is unreachable, include the restrict option. In the service VPN, you must also advertise the service using the service command. You configure the GRE interface or interfaces in the transport VPN (VPN 0).</td>
<td>Click Accept, then action Service.</td>
<td>set service service-name [tloc ip-address | tloc-list list-name] [vpn vpn-id]</td>
<td>Standard services: FW, IDS, IDP. Custom services: netsvc1, netsvc2, netsvc3, netsvc4</td>
</tr>
<tr>
<td>Direct traffic to a remote TLOC. The TLOC is defined by its IP address, color, and encapsulation.</td>
<td>Click Accept, then action TLOC.</td>
<td>set local-tloc color [encap encapsulation]</td>
<td>TLOC address, color, and encapsulation</td>
</tr>
</tbody>
</table>
**SD-WAN Application Intelligence Engine Flow**

<table>
<thead>
<tr>
<th>Description</th>
<th>Cisco vManage</th>
<th>CLI Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct traffic to one of the remote TLOCs in the TLOC list.</td>
<td>Click Accept, then action TLOC.</td>
<td><code>set tloc-list list-name</code></td>
<td>Name of a policy lists tloc-list list</td>
</tr>
<tr>
<td>Set the VPN that the packet is part of.</td>
<td>Click Accept, then action VPN.</td>
<td><code>set vpn vpn-id</code></td>
<td>0 through 65530</td>
</tr>
</tbody>
</table>

**Default Action**

If a data packet being evaluated does not match any of the match conditions in a data policy, a default action is applied to the packet. By default, the data packet is dropped.

From the Cisco vManage menu, you modify the default action from Configuration > Policies > Centralized Policy > Add Policy > Configure Traffic Rules > Application-Aware Routing > Sequence Type > Sequence Rule > Default Action.

In the CLI, you modify the default action with the `policy data-policy vpn-list default-action accept` command.

## Configure SD-WAN Application Intelligence Engine Flow Using the CLI

Following are the high-level steps for configuring a centralized data policy for the SD-WAN Application Intelligence Engine (SAIE) flow.

**Note**
In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

1. **Create a list of overlay network sites to which the data policy is to be applied using the `apply-policy` command:**
   ```bash
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-lists-list-name)# site-id site-id
   ``
   The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (–).
   Create additional site lists, as needed.

2. **Create lists of applications and application families that are to be subject to the data policy. Each list can contain one or more application names, or one or more application families. A single list cannot contain both applications and application families.**
   ```bash
   vSmart(config)# policy lists
   vSmart(config-lists)# app-list list-name
   vSmart(config-app-list)# app application-name
   vSmart(config)# policy lists
   vSmart(config-lists)# app-list list-name
   vSmart(config-app-list)# app-family family-name
   ```

**Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x**
3. Create lists of IP prefixes and VPNs, as needed:
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# data-prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id
   ```

4. Create lists of TLOCs, as needed:
   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists tloc-list list-name
   vSmart(config-lists-list-name)# tloc ip-address color color encap encapsulation [preference number]
   ```

5. Define policing parameters, as needed:
   ```
   vSmart(config-policy)# policer policer-name
   vSmart(config-policer)# rate bandwidth
   vSmart(config-policer)# burst bytes
   vSmart(config-policer)# exceed action
   ```

6. Create a data policy instance and associate it with a list of VPNs:
   ```
   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name
   ```

7. Create a series of match–pair sequences:
   ```
   vSmart(config-vpn-list)# sequence number
   vSmart(config-sequence-number)#
   ```
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

8. Define match parameters based on applications:
   ```
   vSmart(config-sequence-number)# match app-list list-name
   ```

9. Define additional match parameters for data packets:
   ```
   vSmart(config-sequence-number)# match parameters
   ```

10. Define actions to take when a match occurs:
    ```
        vSmart(config-sequence-number)# action (accept | drop) [count]
    ```

11. For packets that are accepted, define the actions to take. To control the tunnel over which the packets travels, define the remote or local TLOC, or for strict control over the tunnel path, set both:
    ```
        vSmart(config-action)# set tloc ip-address color color encap encapsulation
        vSmart(config-action)# set tloc-list list-name
        vSmart(config-action)# set local-tloc color color encap encapsulation
        vSmart(config-action)# set local-tloc-list color color encap encapsulation [restrict]
    ```

12. Define additional actions to take.

13. Create additional numbered sequences of match–action pairs within the data policy, as needed.

14. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want nonmatching prefixes to be accepted, configure the default action for the policy:
    ```
    vSmart(config-policy-name)# default-action accept
    ```
15. Apply the policy to one or more sites in the overlay network:

```
vSmart(config)# apply-policy site-list list-name data-policy policy-name (all | from-service | from-tunnel)
```

Use the following show commands for visibility in traffic classification:

- `show app dpi flows`
- `show support dpi flows active detail`
- `show app dpi application`
- `show support dpi flows expired detail`
- `show support dpi statistics`
Application-Aware Routing

- Information About Application-Aware Routing, on page 125
- Configure Application-Aware Routing, on page 133
- Configure Application-Aware Routing Using CLIs, on page 148
- Configure Application Probe Class Using CLI, on page 150
- Application-Aware Routing Policy Configuration Example, on page 151

Information About Application-Aware Routing

Application-aware routing tracks network and path characteristics of the data plane tunnels between Cisco IOS XE SD-WAN devices and uses the collected information to compute optimal paths for data traffic. These characteristics include packet loss, latency, and jitter, and the load, cost and bandwidth of a link. The ability to consider factors in path selection other than those used by standard routing protocols—such as route prefixes, metrics, link-state information, and route removal on the Cisco IOS XE SD-WAN device—offers a number of advantages to an enterprise:

- In normal network operation, the path taken by application data traffic through the network can be optimized, by directing it to WAN links that support the required levels of packet loss, latency, and jitter defined in an application’s SLA.

- In the face of network brownouts or soft failures, performance degradation can be minimized. The tracking of network and path conditions by application-aware routing in real time can quickly reveal performance issues, and it automatically activates strategies that redirect data traffic to the best available path. As the network recovers from the soft failure conditions, application-aware routing automatically readjusts the data traffic paths.

- Network costs can be reduced because data traffic can be more efficiently load-balanced.

- Application performance can be increased without the need for WAN upgrades.
Each Cisco IOS XE SD-WAN device supports up to eight TLOCs, allowing a single Cisco IOS XE SD-WAN device to connect to up to eight different WAN networks. This capability allows path customization for application traffic that has different needs in terms of packet loss and latency.

**Application-Aware Routing Support for Multicast Protocols**

**Table 21: Feature History**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application-Aware Routing Policy Support for Multicast | Cisco IOS XE Release 17.3.1a  
Cisco vManage Release 20.3.1 | This feature enables support for configuring application-aware routing policy for multicast traffic on Cisco IOS XE SD-WAN devices based on source and destination, protocol matching and SLA requirement. |

Starting from Cisco IOS XE Release 17.3.1a, application-aware routing supports overlay multicast traffic on Cisco IOS XE SD-WAN devices. In older releases, an application-route policy is supported only for unicast traffic.

The Cisco IOS XE SD-WAN devices classify the multicast traffic based on the group address and sets the SLA class. The group address can be source IP, destination IP, source prefixes, and destination prefixes. In the forwarding plane, any traffic for group address must use only those TLOC paths that meet the SLA requirement. You can perform the path selection for a group based on the preferred color, backup color, or the default action.

**Restrictions for Multicast Protocols**

Network-Based Application Recognition (NBAR) using the SD-WAN Application Intelligence Engine (SAIE) flow is not supported for multicast.

**Note**

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.
Components of Application-Aware Routing

The Cisco IOS XE SD-WAN Application-Aware Routing solution consists of three elements:

- **Identification**—You define the application of interest, and then you create a centralized data policy that maps the application to specific SLA requirements. You single out data traffic of interest by matching on the Layer 3 and Layer 4 headers in the packets, including source and destination prefixes and ports, protocol, and DSCP field. As with all centralized data policies, you configure them on a Cisco vSmart Controller, which then passes them to the appropriate Cisco IOS XE SD-WAN devices.

- **Monitoring and measuring**—The Cisco IOS XE SD-WAN software uses BFD packets to continuously monitor the data traffic on the data plane tunnels between devices, and periodically measures the performance characteristics of the tunnel. To gauge performance, the Cisco IOS XE SD-WAN device looks for traffic loss on the tunnel, and it measures latency by looking at the one-way and round-trip times of traffic traveling over the tunnel. These measurements might indicate suboptimal data traffic conditions.

- **Mapping application traffic to a specific transport tunnel**—The final step is to map an application’s data traffic to the data plane tunnel that provides the desired performance for the application. The mapping decision is based on two criteria: the best-path criteria computed from measurements performed on the WAN connections and on the constraints specified in a policy specific to application-aware routing.

To create a data policy based on the Layer 7 application itself, configure the SD-WAN Application Intelligence Engine (SAIE) flow with a centralized data policy. With the SAIE flow, you can direct traffic to a specific tunnel, based on the remote TLOC, the remote TLOC, or both. You cannot direct traffic to tunnels based on SLA classes.

**Note**

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.
SLA Classes

Table 22: Feature History

<table>
<thead>
<tr>
<th>Feature</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for SLA Classes</td>
<td>Cisco IOS XE Release 17.2.1r</td>
<td>This feature allows you to configure up to a maximum of eight SLA classes on Cisco vSmart Controller. Using this feature, you can configure additional options in an application-aware routing policy.</td>
</tr>
<tr>
<td>Support for six SLA Classes per Policy</td>
<td>Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1</td>
<td>This feature allows you to configure up to six SLA classes per policy on Cisco IOS XE SD-WAN devices. This enhancement allows additional options in an application-aware routing policy.</td>
</tr>
<tr>
<td>SLA Class Support Enhancement</td>
<td>Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1</td>
<td>This feature is an enhancement to support up to 16 SLA classes on Cisco IOS XE SD-WAN devices.</td>
</tr>
<tr>
<td>Application Aware Routing and Data Policy SLA Preferred Colors</td>
<td>Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1</td>
<td>This feature provides different behaviors to choose preferred colors based on the SLA requirements when both application-aware routing policy and data policies are configured.</td>
</tr>
</tbody>
</table>

A service-level agreement (SLA) determines actions taken in application-aware routing. The SLA class defines the maximum jitter, maximum latency, maximum packet loss, or a combination of these values for data plane tunnels in Cisco IOS XE SD-WAN devices. Each data plane tunnel comprises a local transport locator (TLOC) and a remote TLOC pair. You can configure SLA classes under the `policy sla-class` command hierarchy on Cisco vSmart Controllers. From Cisco IOS XE Release 17.2.1r, you can configure a maximum of eight SLA classes on Cisco vSmart controllers. However, you can define only four unique SLA classes in an application-aware route policy. In releases earlier than Cisco IOS XE Release 17.2.1r, you can configure a maximum of four SLA classes.

Starting from Cisco IOS XE Release 17.3.1a, you can configure up to six SLA classes per policy on the Cisco IOS XE SD-WAN devices.

You can configure the following parameters in an SLA class.

Table 23: SLA Components

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum acceptable packet jitter on the data plane tunnel</td>
<td><code>jitter milliseconds</code></td>
<td>1–1000 milliseconds</td>
</tr>
<tr>
<td>Maximum acceptable packet latency on the data plane tunnel</td>
<td><code>latency milliseconds</code></td>
<td>1–1000 milliseconds</td>
</tr>
</tbody>
</table>
Value or Range
Command
Description
1–100 percent
loss percentage

SLA Support Enhancement

From Cisco IOS XE Release 17.6.1a and Cisco vManage Release 20.6.1, you can configure more than six SLA classes per policy on Cisco IOS XE SD-WAN devices.

Cisco IOS XE SD-WAN devices need 16 GB RAM or more to support up to 16 SLA classes.

This feature enhancement increases the number of SLA classes supported on Cisco vSmart Controller and SD-WAN Edge devices. With the increase in the SLA class support, you can align SLA classes to IP Virtual Private Networks (IP-VPN) on Multi-Protocol Label Switching (MPLS) networks for transporting traffic to a global network.

The SLA enhancement helps in multitenancy, where you can push different SLA classes for different tenants. The multitenancy feature requires the Cisco vSmart Controller to support more than eight SLA classes. To allocate SLA classes to different tenants, the global limit for policies must be 64.

Table 24: Maximum SLA Classes Supported on Cisco IOS XE SD-WAN Devices

<table>
<thead>
<tr>
<th>Supported Platforms and Models</th>
<th>SLA Class prior to Cisco IOS XE Release 17.6.1a (+1 Default SLA Class)</th>
<th>SLA Class from Cisco IOS XE Release 17.6.1a (+1 Default SLA Class)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 1001 HX -16GB</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>• vedge-ASR-1001-HX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASR 1002 X -16GB</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>• vedge-ASR-1002-X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASR 1002 HX -16GB</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>• vedge-ASR-1002-HX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASR 1001 X -16GB</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>• vedge-ASR-1001-X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISR 4451 X</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>• vedge-ISR-4451-X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISR 4431</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>• vedge-ISR-4431</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported Platforms and Models</td>
<td>SLA Class prior to Cisco IOS XE Release 17.6.1a (+1 Default SLA Class)</td>
<td>SLA Class from Cisco IOS XE Release 17.6.1a (+1 Default SLA Class)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Catalyst 8300 Edge Platforms</td>
<td>NA</td>
<td>7</td>
</tr>
<tr>
<td>• vedge-C8300-2N2S-6G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-2N2S-4G2X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-1N1S-6G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-1N1S-4G2X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-1N1S-6T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-1N1S-4T2X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-2N2S-6T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8300-2N2S-4T2X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalyst 8500 Edge platforms</td>
<td>NA</td>
<td>15</td>
</tr>
<tr>
<td>-16GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8500L-8S4X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8500-12X4QC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• vedge-C8500-12X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other Cisco IOS XE SD-WAN</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>devices (C11xx, ISR1100, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSR1000v)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SLA-Preferred Colors**

From Cisco IOS XE Release 17.6.1a, when you configure both application-aware routing policy and data policy, and if data flow matches the app-route and data policy sequences, the following expected behaviors occur:

- If the preferred colors that you configure in application-aware routing meet the SLA requirements, and these preferred colors have some colors that are common with data policy, the common preferred colors are chosen over others for forwarding. (Prior to Cisco IOS XE Release 17.6.1a, the data policy-preferred colors were forwarded and the application-aware routing policy preferences were ignored.)

- If preferred colors in application-aware routing do not meet the SLA, but there are colors that are common with the data policy, and these colors meet the SLA in application-aware routing, then these colors take precedence and are chosen for forwarding.

- If no tunnels or colors meet the SLA in application-aware routing, the data policy takes precedence and is chosen for forwarding. If the data policy has preferred colors, these colors are chosen. Otherwise, load balance occurs across all the colors in the data policy.
Classification of Tunnels into SLA Classes

The process of classifying tunnels into one or more SLA classes for application-aware routing has three parts:

- Measure loss, latency, and jitter information for the tunnel.
- Calculate the average loss, latency, and jitter for the tunnel.
- Determine the SLA classification of the tunnel.

Measure Loss, Latency, and Jitter

When a data plane tunnel in the overlay network is established, a BFD session automatically starts on the tunnel. In the overlay network, each tunnel is identified with a color that identifies a specific link between a local TLOC and a remote TLOC. The BFD session monitors the liveness of the tunnel by periodically sending Hello packets to detect whether the link is operational. Application-aware routing uses the BFD Hello packets to measure the loss, latency, and jitter on the links.

By default, the BFD Hello packet interval is 1 second. This interval is user-configurable (with the `bfd color interval` command). Note that the BFD Hello packet interval is configurable per tunnel.

Calculate Average Loss, Latency, and Jitter

BFD periodically polls all the tunnels on the Cisco IOS XE SD-WAN devices to collect packet latency, loss, jitter, and other statistics for use by application-aware routing. At each poll interval, application-aware routing calculates the average loss, latency, and jitter for each tunnel, and then calculates or recalculates each tunnel's SLA. Each poll interval is also called a "bucket."

By default, the poll interval is 10 minutes. With the default BFD Hello packet interval at 1 second, this means that information from about 600 BFD Hello packets is used in one poll interval to calculate loss, latency, and jitter for the tunnel. The poll interval is user-configurable (with the `bfd app-route poll-interval` command). Note that the application-aware routing poll interval is configurable per Cisco IOS XE SD-WAN device; that is, it applies to all tunnels originating on a device.

Reducing the poll interval without reducing the BFD Hello packet interval may affect the quality of the loss, latency, and jitter calculation. For example, setting the poll interval to 10 seconds when the BFD Hello packet interval is 1 second means that only 10 Hello packets are used to calculate the loss, latency, and jitter for the tunnel.

The loss, latency, and jitter information from each poll interval is preserved for six poll intervals. At the seventh poll interval, the information from the earliest polling interval is discarded to make way for the latest information. In this way, application-aware routing maintains a sliding window of tunnel loss, latency, and jitter information.

The number of poll intervals (6) is not user-configurable. Each poll interval is identified by an index number (0 through 5) in the output of the `show app-route statistics` command.

Determine SLA Classification

To determine the SLA classification of a tunnel, application-aware routing uses the loss, latency, and jitter information from the latest poll intervals. The number of poll intervals used is determined by a multiplier. By default, the multiplier is 6, so the information from all the poll intervals (specifically, from the last six poll intervals) is used to determine the classification. For the default poll interval of 10 minutes and the default multiplier of 6, the loss, latency, and jitter information collected over the last hour is considered when classifying
the SLA of each tunnel. These default values have to be chosen to provide damping of sorts, as a way to prevent frequent reclassification (flapping) of the tunnel.

The multiplier is user-configurable (with the `bfd app-route multiplier` command). Note that the application-aware routing multiplier is configurable per Cisco IOS XE SD-WAN device; that is, it applies to all tunnels originating on a device.

If there is a need to react quickly to changes in tunnel characteristics, you can reduce the multiplier all the way down to 1. With a multiplier of 1, only the latest poll interval loss and latency values are used to determine whether this tunnel can satisfy one or more SLA criteria.

Based on the measurement and calculation of tunnel loss and latency, each tunnel may satisfy one or more user-configured SLA classes. For example, a tunnel with a mean loss of 0 packets and mean latency of 10 milliseconds would satisfy a class that has been defined with a maximum packet loss of 5 and a minimum latency of 20 milliseconds, and it would also satisfy a class that has been defined with a maximum packet loss of 0 and minimum latency of 15 milliseconds.

Regardless of how quickly a tunnel is reclassified, the loss, latency, and jitter information is measured and calculated continuously. You can configure how quickly application-aware routing reacts to changes by modifying the poll interval and multiplier.

## Per-Class Application-Aware Routing

### Table 25: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-Class Application-Aware Routing</td>
<td>Cisco IOS XE Release 17.4.1a, vManage Release 20.4.1</td>
<td>This feature enhances the capabilities of directing traffic to next-hop addresses based on the service level agreement (SLA) definitions. These SLA definitions along with the policy to match and classify traffic types can be used to direct traffic over specific Cisco SD-WAN tunnels. The SLA definition comprises of values of loss, latency, and jitter, which are measured using the Bidirectional Forwarding Detection (BFD) channel that exists between two transport locators (TLOCs).</td>
</tr>
</tbody>
</table>

### Per-Class Application-Aware Routing Overview

The SLA definition comprises of values of loss, latency, and jitter, which are measured using the BFD channel that exists between two TLOCs. These values collectively represent the status of the network and the BFD link. The BFD control messages are sent with a high priority Differentiated Services Code Point (DSCP) marking of 48.

The SLA metrics based on the high priority packet does not reflect the priority that is received by the actual data that flows through the edge device. The data, depending on the application class, can have different DSCP values in the network. Therefore, a more accurate representation of the loss, latency, and jitter for the traffic profiles is required for the networks to use such measurements to direct traffic types to the right tunnels.

Application-aware routing uses policies that constrain paths that can be used for forwarding the application. These constraints are usually expressed in terms of SLA classes that contain loss, latency, and jitter requirements.
that must be met. This requires that these metrics be measured on all the paths to the destination of the traffic using active probing or by passive monitoring.

Active probing methods include generation of synthetic traffic that is injected along with real traffic. The expectation is that the probes and the real traffic is forwarded in the same way. BFD probing, ICMP, periodic HTTP requests and IP SLA measurements are some examples of active probing mechanisms. The Cisco SD-WAN solution uses BFD based probes for active measurements. Passive monitoring methods rely on the SD-WAN Application Intelligence Engine (SAIE) flow and monitoring actual traffic. For example, RTP/TCP traffic is monitored for loss, latency, and jitter.

**Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

### Application Probe Class

An application probe class (app-probe-class) comprises of a forwarding class, color, and DSCP. This defines the marking per color of applications that are forwarded. The color or DSCP mapping is local to a Cisco SD-WAN network site. However, a few colors and the DSCP mapping for a color does not change per site. The forwarding class determines the QoS queue in which the BFD echo request is queued at the egress tunnel port. This is applicable only for BFD echo request packets. The packet-loss-priority for BFD packets is fixed to low. When BFD packets are sent with SLA class, they use the same DSCP value. When BFD packets are sent with app-probe-class along with SLA class, the BFD packets are sent for each SLA app-probe-class separately in a round-robin manner.

**Note** When the application route policy is applied at a site, only the colors relevant to the site are used. Since six SLA classes are supported on Cisco IOS XE SD-WAN devices, the device correspondingly supports up to six app-probe-classes.

### Default DSCP Values

The default DSCP value that is used in the DSCP control traffic is 48. However, there is a provision to change the default value along with the option to configure on the edge devices. All the network service providers may not necessarily use DSCP 48.

The BFD packet having the default DSCP can also be used for other features such as PMTU. A change in the default DSCP means that the other features are affected by the new default DSCP value. Therefore, we recommend that you configure the highest priority DSCP marking that the service provider provides (usually 48, but can be different based on the SLA agreement of the service provider). The color level overrides the global level default DSCP marking.

### Configure Application-Aware Routing

This topic provides general procedures for configuring application-aware routing. Application-aware routing policy affects only traffic that is flowing from the service side (the local/WAN side) to the tunnel (WAN) side of the Cisco IOS XE SD-WAN device.
An application-aware routing policy matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications’ data traffic. The primary purpose of application-aware routing policy is to optimize the path for data traffic being transmitted by Cisco IOS XE SD-WAN devices. An application-aware routing policy is a type of centralized data policy: you configure it on the vSmart controller, and the controller automatically pushes it to the affected Cisco IOS XE SD-WAN devices. As with any policy, an application-aware routing policy consists of a series of numbered (ordered) sequences of match-action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to use to transmit the packet. If a packet matches no parameters in any of the policy sequences, and if no default SLA class is configured, the packet is accepted and forwarded with no consideration of SLA. Because application-aware routing policy accepts nonmatching traffic by default, it is considered to be a positive policy. Other types of policies in the Cisco IOS XE SD-WAN software are negative policies, because by default they drop nonmatching traffic.

Configure Application-Aware Routing Policies Using Cisco vManage

To configure application-aware routing policy, use the Cisco vManage policy configuration wizard. For Centralized Policy configuration details, see Configure Centralized Policies Using Cisco vManage. The wizard consists of four sequential windows that guide you through the process of creating and editing policy components:

- Create Applications or Groups of Interest: Create lists that group together related items and that you call in the match or action components of a policy. For configuration details, see Configure Groups of Interest.

- Configure Topology: Create the network structure to which the policy applies. For topology configuration details, see Configure Topology and VPN Membership.

- Configure Traffic Rules: Create the match and action conditions of a policy.

- Apply Policies to Sites and VPNs: Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard windows, you are creating policy components or blocks. In the last window, you are applying policy blocks to sites and VPNs in the overlay network.

For an application-aware routing policy to take effect, you must activate the policy.

Configure Best Tunnel Path

Table 26: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best of the Worst (BOW) Tunnel Selection</td>
<td>Cisco IOS XE Release 17.5.1a, Cisco vManage Release 20.5.1</td>
<td>This feature introduces a new policy action fallback-to-best-path to pick the best path or color out of the available colors. When the data traffic does not meet any of the SLA class requirements, this feature allows you to select the best tunnel path criteria sequence using the Fallback Best Tunnel option under each SLA class to avoid packet loss.</td>
</tr>
</tbody>
</table>
Best Tunnel Path Overview

To avoid data packet loss and to configure the best application-aware routing tunnel selection when a SLA is not met, you can configure the following policy actions:

- **backup-preferred-color**
- **fallback-to-best-path**

*Figure 14: Flow Chart for Application-Aware Routing Tunnel Selection*

**Recommendation for the Best Tunnel Path**

- Configure the **fallback-to-best-path** policy action in Cisco vManage when configuring a SLA class.
- Configure the **backup-preferred-color** policy action in Cisco vManage when configuring traffic rules.

**Configure Variance for Best Tunnel Path**

Cisco vManage uses best of worst (BOW) to find a best tunnel when no tunnel meets any of the SLA class requirements.

Assume that the required latency is 100 ms to meet the SLA class requirements and tunnel T1 has 110 ms. Tunnel T2 has 111 ms and tunnel T3 has 112 ms.

As per the BOW logic, the best tunnel is T1. T2 and T3 are equally the best tunnels, with only a difference of a few ms.
You configure variance in Cisco vManage when configuring an SLA class. Variance accommodates small deviations as part of the best tunnel selection.

For more information, see Configure SLA Class.

**Example: Without Variance Configured**

At time t0: T1 has 100 ms, T2 has 101 ms, and T3 has 102 ms

At time t1: T1 has 101 ms, T2 has 100 ms, and T3 has 102 ms

At time t3: T1 has 101 ms, T2 has 112 ms, and T3 has 100 ms

At time t1, the best tunnel changes from T1 to T2, and for time t2, the best tunnel changes from T2 to T3. Because variance is not configured, this leads to data path reprogramming and changes to the data traffic paths.

Assume instead that you configure variance to dampen a small deviation in ms.

For example, you configure variance as 5 ms, which means that the best tunnel SLA = 100 ms. The range is from 100 ms to 105 ms.

**Example: With Variance Configured**

BOW(t0) = {T1, T2, T3}

BOW(t1) = {T1, T2, T3}

BOW(t2) = {T1, T2, T3}

With variance configured, there is no data path reprogramming required or changes to data traffic paths.

### Verify Configuration of Variance for Best Tunnel Path

#### Example for Latency Variance

Device# `show sdwan policy from-vsmart`

```
from-vsmart sla-class video
latency      100
jitter      150
fallback-best-tunnel. latency
```

Tunnel T1: Latency: 110 msec, Loss: 0%, Jitter: 200 msec
Tunnel T2: Latency: 115 msec, Loss: 0%, Jitter: 200 msec
Tunnel T3: Latency: 120 msec, Loss: 0%, Jitter: 200 msec

Without latency variance, the best tunnel is T1.

With latency variance configured as 10 ms, T1, T2, and T3 are the best tunnels.

The range is from 110 ms to 120 ms.

The best latency + variance is 110 ms + 10 ms.

Use the following formula to find the best tunnel selection for latency variance:

\( (\text{best}_\text{latency}, \text{best}_\text{latency} + \text{latency}_\text{variance}) \)

#### Example for Jitter Variance

Device# `show sdwan policy from-vsmart`

```
from-vsmart sla-class video
```

Without jitter variance, the best tunnel is T3.

With jitter variance configured as 10 ms, T1, T2, and T3 are the best tunnels.

The range is from 152 ms to 162 ms.

The best jitter + variance is 152 ms + 10 ms.

Use the following formula to find the best tunnel selection for jitter variance:

\( (\text{best jitter}, \text{best jitter} + \text{jitter variance}) \)

**Example for Loss Variance**

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class video
latency 100
jitter 1
fallback-best-tunnel. loss
```

Tunnel T1: Latency: 110 msec, Loss: 2%, Jitter: 200 msec
Tunnel T2: Latency: 115 msec, Loss: 3%, Jitter: 200 msec
Tunnel T3: Latency: 120 msec, Loss: 4%, Jitter: 200 msec

Without loss variance, the best tunnel is T1.

With loss variance configured as 1%, T1 and T2 are the best tunnels.

The range is from 2% to 3%.

The best loss + variance is 2%.

Use the following formula to find the best tunnel selection for loss variance:

\( (\text{best loss}, \text{best loss} + \text{loss variance}) \)

**Configure SLA Class**

1. From the Cisco vManage menu, select **Configuration > Policies**. Centralized Policy is selected and displayed by default.

2. Click **Add Policy**.

3. In the create groups of interest page, from the left pane, click **SLA Class**, and then click **New SLA Class List**.

4. In the **SLA Class List Name** field, enter a name for SLA class list.

5. Define the SLA class parameters:

   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.

   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
c. In the Jitter field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.

d. Choose the required app probe class from the App Probe Class drop-down list.

6. (Optional) Check the Fallback Best Tunnel check box to enable the best tunnel criteria.

This optional field is available from Cisco IOS XE Release 17.5.1a to pick the best path or color from the available colors when a SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and jitter values.

7. Select the Criteria from the drop-down. The available criteria are:

   • None
   • Latency
   • Loss
   • Jitter
   • Latency, Loss
   • Latency, Jitter
   • Loss, Latency
   • Loss, Jitter
   • Jitter, Latency
   • Jitter, Loss
   • Latency, Loss, Jitter
   • Latency, Jitter, Loss
   • Loss, Latency, Jitter
   • Loss, Jitter, Latency
   • Jitter, Latency, Loss
   • Jitter, Loss, Latency

8. (Optional) Enter the Loss Variance (%), Latency Variance (ms), and the Jitter Variance (ms) for the selected criteria.

   For more information, see Configure Variance for Best Tunnel Path.

9. Click Add.

**Configure Traffic Rules**

To configure traffic rules for application-aware routing policy:

1. Click Application-Aware Routing. From the Add Policy drop-down, select Create New.

2. Click Sequence Type. A policy sequence containing the text string App Route is added in the left pane.
3. Double-click the App Route text string and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.

4. In the right pane, click **Sequence Rule**. The Match/Action box opens, and Match is selected by default. The available policy match conditions are listed below the box.

5. Click and select one or more **Match** conditions. Set the values as described in the following table:

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (match all packets)</td>
<td>Do not specify any match conditions.</td>
</tr>
<tr>
<td>Applications/Application Family List</td>
<td>a. In the Match conditions, click <strong>Applications/Application Family List</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the drop-down, select the application family.</td>
</tr>
<tr>
<td></td>
<td>c. To create an application list:</td>
</tr>
<tr>
<td></td>
<td>1. Click <strong>New Application List</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Enter a name for the list.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Application</strong> to create a list of individual applications. Click <strong>Application Family</strong> to create a list of related applications.</td>
</tr>
<tr>
<td></td>
<td>4. In the Select Application drop-down, select the desired applications or application families.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Destination Data Prefix</td>
<td>a. In the Match conditions, click <strong>Destination Data Prefix</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. To match a list of destination prefixes, select the list from the drop-down.</td>
</tr>
<tr>
<td></td>
<td>c. To match an individual destination prefix, type the prefix in the Destination box.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>a. In the Match conditions, click <strong>Destination Port</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the Destination field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
</tr>
<tr>
<td>DNS Application List (to enable split DNS)</td>
<td>a. In the Match conditions, click <strong>DNS Application List</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the drop-down, select the application family.</td>
</tr>
<tr>
<td><strong>DNS (to enable split DNS)</strong></td>
<td><strong>Match conditions</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>a. In the Match conditions, click <strong>DNS</strong>. b. In the drop-down, select <strong>Request to process DNS requests for the DNS applications</strong>, and select <strong>Response to process DNS responses for the applications</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DSCP</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In the Match conditions, click <strong>DSCP</strong>. b. In the DSCP field, type the DSCP value, a number from 0 through 63.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>PLP</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In the Match conditions, click <strong>PLP</strong>. b. In the PLP drop-down, select <strong>Low</strong> or <strong>High</strong>. To set the PLP to high, apply a policer that includes the <strong>exceed remark</strong> option.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Protocol</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In the Match conditions, click <strong>Protocol</strong>. b. In the Protocol field, type the Internet Protocol number, a number from 0 through 255.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ICMP Message</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> This field is available from Cisco IOS XE Release 17.4.1, Cisco vManage Release 20.4.1. For Protocol IPv4 and IPv6 when you select a Protocol value as 1 or 58, the <strong>ICMP Message</strong> field displays where you can select an ICMP message to apply to the data policy. When Protocol is selected as Both, the <strong>ICMP Message or ICMPv6 Message</strong> field displays.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Source Data Prefix</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In the Match conditions, click <strong>Source Data Prefix</strong>. b. To match a list of source prefixes, select the list from the drop-down. c. To match an individual source prefix, type the prefix in the Source box.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Source Port</strong></th>
<th><strong>Match conditions</strong></th>
<th><strong>Protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. In the Match conditions, click <strong>Source Port</strong>. b. In the Source field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. To select actions to take on matching data traffic, click **Actions**. The available policy actions are displayed.

7. Set the policy action for a **Backup SLA Preferred Color** match condition. When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel interface is not available, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching.
a. In the Action conditions, click **Backup SLA Preferred Color**.

b. In the drop-down, select one or more colors.

8. Set the policy action for a **Counter** match condition. Count matching data packets.
   
a. In the Action conditions, click **Counter**.

b. In the Counter Name field, enter the name of the file in which to store packet counters.

9. Set the policy action for a **Log** match condition. Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.
   
a. In the Action conditions, click **Log** to enable logging.

10. Set the policy action for a **SLA Class List** match condition. For the SLA class, all matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.
    
a. In the Action conditions, click **SLA Class List**.

b. In the **SLA Class** drop-down, select one or more SLA classes.

c. Optionally, in the **Preferred Color** drop-down, select the color of the data plane tunnel or tunnels to prefer. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.

d. In the **When SLA not met** field, select one of the following:
   
   • Click **Strict/Drop** to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped.
   
   • Click **Fallback to best path** to select the best available tunnel to avoid a packet drop.

   **Note**

The **Fallback to best path** option is available from Cisco IOS XE Release 17.5.1a.

The **Fallback to best path** action can be selected only when **Fallback Best Tunnel** option is enabled while defining a SLA class. If the **Fallback Best Tunnel** option is not enabled, then the following error message displays in Cisco vManage:

SLA Class selected, does not have Fallback Best Tunnel enabled.
Please change the SLA class or change to Strict/Drop.

   • Click **Load Balance** to balance the tunnel load.

11. Click **Save Match and Actions**.

12. Create additional sequence rules as desired. Drag and drop to re-arrange them.

13. Create additional sequence types as desired. Drag and drop to re-arrange them.
14. Click **Save Application-Aware Routing Policy**.
15. Click **Next** to move to Apply Policies to Sites and VPNs.

**Default Action of Application-Aware Routing Policy**

The default action of the policy defines how to handle packets that match none of the match conditions. For application-aware routing policy, if you do not configure a default action, all data packets are accepted and transmitted based on normal routing decisions, with no consideration of SLA.

To modify this behavior, include the `default-action sla-class sla-class-name` command in the policy, specifying the name of an SLA class you defined in the `policy sla-class` command.

When you apply an SLA class in a policy's default action, you cannot specify the `strict` option.

If no data plane tunnel satisfies the SLA class in the default action, the Cisco IOS XE SD-WAN device selects one of the available tunnels by performing load-balancing across equal paths.

Expected behavior when data flow matches both AAR and data policies:

1. When data policy local TLOC action is configured, the `App-route preferred-color` and `backup-preferred-color` actions are ignored.
2. The `sla-class` and `sla-strict` actions are retained from the application routing configuration.
3. The data policy TLOC takes precedence.

When there is a `local-tloc-list` action that has multiple options, choose the local-TLOC that meets SLA.

- If no `local-tloc` meets SLA, then choose equal-cost multi-path routing (ECMP) for the traffic over the `local-tloc-list`.
- If none of the `local-tloc` is up, then choose a TLOC that is up.
- If none of the `local-tloc` is up and the DP is configured in restrict mode, then drop the traffic.

**Configure Application Probe Class through vManage**

1. From the Cisco vManage menu, choose **Configuration > Policies**.
2. In **Centralized Policy**, click **Add Policy**. The **Create Groups of Interest** page appears.
3. Choose the list type **App Probe Class** from the left navigation panel to create your groups of interest.
4. Click **New App Probe Class**.
5. Enter the probe class name in the **Probe Class Name** field.
6. Choose the required forwarding class from the **Forwarding Class** drop-down list.
   
   If there are no forwarding classes, then create a class from the **Class Map** list page under the **Localized Policy Lists** in the **Custom Options** menu.
   
   To create a forwarding class:
   
   a. In the **Custom Options** drop-down, choose **Lists** from the Localized Policy options.
   b. In the Define Lists window, choose the list type **Class Map** from the left navigation panel.
c. Click New Class List to create a new list.

d. Enter Class and choose the Queue from the drop-down list.

e. Click Save.

7. In the Entries pane, choose the appropriate color from the Color drop-down list and enter the DSCP value.

   Click + sign, to add more entries as required.

8. Click Save.

Add App-Probe-Class to an SLA Class

1. From the left pane, select SLA Class.

2. Click New SLA Class List.

3. In the SLA Class List Name field, enter a name for SLA class list.

4. Enter the required Loss (%), Latency (ms), and Jitter (ms).

5. Choose the required app probe class from the App Probe Class drop-down list.

6. Click Add.

   The new SLA Class created with loss, latency, jitter, and app probe class is added to the table.

Configure Default DSCP on Cisco BFD Template

1. From the Cisco vManage menu, select Configuration > Templates.

2. Click Feature Templates.

   Note: In Cisco vManage Release 20.7.x and earlier releases, Feature Templates is titled Feature.

3. Click Add Template.

4. Select a device from the device list in the left pane.

5. In the right pane, select the BFD template listed under Basic Information.

6. Enter Template Name and Description in the respective fields.

7. In the Basic Configuration pane, enter Multiplier and Poll Interval (milliseconds).

8. In the Default DSCP value for BFD Packets field, enter the required device specific value or choose the default value for DSCP.

9. (Optional) In the Color pane, choose the required color from the drop-down list.

10. Enter the required Hello Interval (milliseconds) and Multiplier.

11. Choose the Path MTU Discovery value.
12. Enter the **BFD Default DSCP value for tloc color**.

13. Click **Add**.

The default DSCP and color values are configured on the BFD template.

---

**Apply Policies to Sites and VPNs**

In the last window of the policy configuration wizard, you associate the policy blocks that you created on the previous three windows with VPNs and with sites in the overlay network.

To apply a policy block to sites and VPNs in the overlay network:

1. From the Cisco vManage menu, choose **Configuration > Policies**. Centralized Policy is selected and displayed by default.

2. Click **Add Policy**. The Create Applications or Groups of Interest page is displayed.

3. Click **Next**. The Network Topology window opens, and in the Topology bar, Topology is selected by default.

4. Click **Next**. The Configure Traffic Rules window opens, and in the Application-Aware Routing bar, Application-Aware Routing is selected by default.

5. Click **Next**. The Apply Policies to Sites and VPNs window opens.

6. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

7. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

8. From the Topology bar, select the type of policy block. The table then lists policies that you have created for that type of policy block.

9. Click **Add New Site List** and **VPN list**. Select one or more site lists and select one or more VPN lists. Click **Add**.

10. Click **Preview** to view the configured policy. The policy is displayed in CLI format.

11. Click **Save Policy**. The **Configuration > Policies** page appears, and the policies table includes the newly created policy.

For an application-aware route policy to take effect, you apply it to a list of sites in the overlay network:

```bash
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
```

When you apply the policy, you do not specify a direction (either inbound or outbound). Application-aware routing policy affects only the outbound traffic on the Cisco IOS XE SD-WAN devices.

For all **app-route-policy** policies that you apply with **apply-policy** commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists **site-list 1**, **site-id 1-100**, and **site-list 2 site-id 70-130**. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different **app-route-policy** policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:
• Centralized control policy (control-policy)
• Centralized data policy (data-policy)
• Centralized data policy used for cflowd flow monitoring (data-policy that includes a cflowd action and apply-policy that includes a cflowd-template command)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for app-route-policy and data-policy policies can have overlapping site IDs. So for the two example site lists above, site-list 1, site-id 1-100, and site-list 2 site-id 70-130, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration on the Cisco vSmart Controller by issuing a commit command, the controller pushes the application-aware routing policy to the Cisco IOS XE SD-WAN devices at the specified sites.

To view the policy configured on the Cisco vSmart Controller, use the show running-config command on the controller.

To view the policy that the Cisco vSmart Controller has pushed to the device, issue the show policy from-vsmart command on the router.

To display flow information for the application-aware applications running on the device, issue the show app dpi flows command on the router.

How Application-Aware Routing Policy is Applied in Combination with Other Data Policies

If you configure a Cisco IOS XE SD-WAN device with application-aware routing policy and with other policies, the policies are applied to data traffic sequentially.

On a Cisco IOS XE SD-WAN device, you can configure the following types of data policy:

• Centralized data policy. You configure this policy on the Cisco vSmart Controller, and the policy is passed to the device. You define the configuration with the policy data-policy configuration command, and you apply it with the apply-policy site-list data-policy, or apply-policy site-list vpn-membership command.

• Localized data policy, which is commonly called access lists. You configure access lists on the device with the policy access-list configuration command. You apply them, within a VPN, to an incoming interface with the vpn interface access-list in configuration command or to an outgoing interface with the vpn interface access-list out command.

• Application-aware routing policy. Application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the Cisco IOS XE SD-WAN device. You configure application-aware routing policy on the Cisco vSmart Controller with the policy app-route-policy configuration command, and you apply it with the apply-policy site-list app-route-policy command. When you commit the configuration, the policy is passed to the appropriate devices. Then, matching data traffic on the device is processed in accordance with the configured SLA conditions. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

You can apply only one data policy and one application-aware routing policy to a single site in the overlay network. When you define and apply multiple site lists in a configuration, you must ensure that a single data policy or a single application-aware routing policy is not applied to more than one site. The CLI does not
check for this circumstance, and the validate configuration command does not detect whether multiple policies of the same type are applied to a single site.

For data traffic flowing from the service side of the router to the WAN side of the router, policy evaluation of the traffic evaluation occurs in the following order:

1. Apply the input access list on the LAN interface. Any data traffic that is not dropped as a result of this access list is passed to the application-aware routing policy for evaluation.

2. Apply the application-aware routing policy. Any data traffic that is not dropped as a result of this policy is passed to the data policy for evaluation. If the data traffic does not match and if no default action is configured, transmit it without SLA consideration.

3. Apply the centralized data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

4. Apply the output access list on the WAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the WAN interface.

For data traffic coming from the WAN through the router and into the service-side LAN, the policy evaluation of the traffic occurs in the following order:

1. Apply the input access list on the WAN interface. Any data traffic that is not dropped as a result of the input access list is passed to the data policy for evaluation.

2. Apply the data policy. Any data traffic that is not dropped as a result of the input access list is passed to the output access list for evaluation.

3. Apply the output access list on the LAN interface. Any data traffic that is not dropped as a result of the output access list is transmitted out the LAN interface, towards its destination at the local site.

As mentioned above, application-aware routing policy affects only traffic that is flowing from the service side (the local/LAN side) to the tunnel (WAN) side of the Cisco IOS XE SD-WAN device, so data traffic inbound from the WAN is processed only by access lists and data policy.

**Activate an Application-Aware Routing Policy**

To activate a policy:

1. From the Cisco vManage menu, choose Configuration > Policies. Centralized Policy is selected and displayed by default.

2. For the desired policy, click ... and select Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable Cisco vSmart Controllers to which the policy is to be applied.

3. Click Activate.

When you activate an application-aware routing policy, the policy is sent to all the connected Cisco vSmart Controllers.

**Monitor Data Plane Tunnel Performance**

The Bidirectional Forwarding Detection (BFD) protocol runs over all data plane tunnels between Cisco IOS XE SD-WAN devices, monitoring the liveness, and network and path characteristics of the tunnels.
Application-aware routing uses the information gathered by BFD to determine the transmission performance of the tunnels. Performance is reported in terms of packet latency and packet loss on the tunnel.

BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The Cisco IOS XE SD-WAN device records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket. If you configure an application-aware routing policy for the device, it is these statistics that the router uses to determine whether a data plane tunnel's performance matches the requirements of the policy's SLA.

The following parameters determine the size of the sliding window:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
<th>Configuration Command</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Hello packet interval</td>
<td>1 second</td>
<td>bfd color color hello-interval seconds</td>
<td>1 through 65535 seconds</td>
</tr>
<tr>
<td>Polling interval for application-aware routing</td>
<td>10 minutes</td>
<td>bfd app-route poll-interval milliseconds</td>
<td>1 through 4,294,967 (2^{32} – 1) milliseconds</td>
</tr>
<tr>
<td>Multiplier for application-aware routing</td>
<td>6</td>
<td>bfd app-route multiplier number</td>
<td>1 through 6</td>
</tr>
</tbody>
</table>

Let us use the default values for these parameters to explain how application-aware routing works:

• For each sliding window time period, application-aware routing sees 600 BFD Hello packets (BFD Hello interval x polling interval: 1 second x 600 seconds = 600 Hello packets). These packets provide measurements of packet loss and latency on the data plane tunnels.

• Application-aware routing retains the statistics for 1 hour (polling interval x multiplier: 10 minutes x 6 = 60 minutes).

• The statistics are placed in six separate buckets, indexed with the numbers 0 through 5. Bucket 0 contains the latest statistics, and bucket 5 the oldest. Every 10 minutes, the newest statistics are placed in bucket 0, the statistics in bucket 5 are discarded, and the remaining statistics move into the next bucket.

• Every 60 minutes (every hour), application-aware routing acts on the loss and latency statistics. It calculates the mean of the loss and latency of all the buckets in all the sliding windows and compares this value to the specified SLAs for the tunnel. If the calculated value satisfies the SLA, application-aware routing does nothing. If the value does not satisfy the SLA, application-aware routing calculates a new tunnel.

• Application-aware routing uses the values in all six buckets to calculate the mean loss and latency for a data tunnel. This is because the multiplier is 6. While application-aware always retains six buckets of data, the multiplier determines how many it actually uses to calculate the loss and latency. For example, if the multiplier is 3, buckets 0, 1, and 2 are used.

Because these default values take action only every hour, they work well for a stable network. To capture network failures more quickly so that application-aware routing can calculate new tunnels more often, adjust the values of these three parameters. For example, if you change just the polling interval to 1 minute (60,000 milliseconds), application-aware routing reviews the tunnel performance characteristics every minute, but it performs its loss and latency calculations based on only 60 Hello packets. It may take more than 1 minute for application-aware routing to reset the tunnel if it calculates that a new tunnel is needed.

To display statistics for each data plane tunnel, use the `show sdwan app-route stats` command:
Device# show sdwan app-route stats

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>DST IP</th>
<th>PROTO</th>
<th>SRC PORT</th>
<th>DST PORT</th>
<th>MEAN LOSS</th>
<th>MEAN LATENCY</th>
<th>INDEX</th>
<th>TOTAL PKETS</th>
<th>LOSS</th>
<th>AVERAGE LATENCY</th>
<th>AVERAGE JITTER</th>
<th>TX DATA PKTS</th>
<th>RX DATA PKTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.1</td>
<td>192.0.2.254</td>
<td>ipsec</td>
<td>12346</td>
<td>12346</td>
<td>0</td>
<td>22</td>
<td>0</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2 596 0 21 2 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>597</td>
<td>1</td>
<td>21</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3 596 0 21 2 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4 596 0 21 2 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>596</td>
<td>0</td>
<td>29</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5 596 0 29 4 0 0</td>
</tr>
<tr>
<td>192.0.2.1</td>
<td>192.0.2.254</td>
<td>ipsec</td>
<td>12346</td>
<td>12346</td>
<td>0</td>
<td>24</td>
<td>0</td>
<td>596</td>
<td>0</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>596</td>
<td>0</td>
<td>25</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2 596 0 25 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>596</td>
<td>0</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3 596 0 24 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>596</td>
<td>0</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4 596 0 24 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>596</td>
<td>0</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5 596 0 24 3 0 0</td>
</tr>
<tr>
<td>192.0.2.1</td>
<td>192.0.2.254</td>
<td>ipsec</td>
<td>12346</td>
<td>34083</td>
<td>0</td>
<td>21</td>
<td>0</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>596</td>
<td>0</td>
<td>22</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2 596 0 22 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3 596 0 21 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4 596 0 21 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>596</td>
<td>0</td>
<td>21</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5 596 0 21 3 0 0</td>
</tr>
<tr>
<td>192.0.2.1</td>
<td>192.0.2.254</td>
<td>ipsec</td>
<td>12346</td>
<td>36464</td>
<td>0</td>
<td>23</td>
<td>0</td>
<td>596</td>
<td>0</td>
<td>23</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>596</td>
<td>0</td>
<td>24</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2 596 0 24 3 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>596</td>
<td>0</td>
<td>23</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3 596 0 23 4 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>596</td>
<td>0</td>
<td>23</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4 596 0 23 4 0 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>596</td>
<td>0</td>
<td>23</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5 596 0 23 4 0 0</td>
</tr>
</tbody>
</table>

To display the next-hop information for an IP packet that a device sends out a service side interface, use the `show policy service-path` command. To view the similar information for packets that the router sends out a WAN transport tunnel interface, use the `show policy tunnel-path` command.

Enable Application Visibility on Cisco IOS XE SD-WAN Devices

You can enable application visibility directly on Cisco IOS XE SD-WAN devices, without configuring application-aware routing policy so that you can monitor all the applications running in all VPNs in the LAN. To do this, configure application visibility on the router:

vEdge(config)# policy app-visibility

To monitor the applications, use the `show app dpi applications` and `show app dpi supported-applications` commands on the device.

Configure Application-Aware Routing Using CLIs

Following are the high-level steps for configuring an application-aware routing policy:

1. Create a list of overlay network sties to which the application-aware routing policy is to be applied (in the `apply-policy` command):

vSmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-site-list)# site-id site-id

The list can contain as many site IDs as necessary. Include one `site-id` command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with a dash (`-`). Create additional site lists, as needed.

2. Create SLA classes and traffic characteristics to apply to matching application data traffic:
3. Create lists of applications, IP prefixes, and VPNs to use in identifying application traffic of interest (in the `match` section of the policy definition):

```bash
vSmart(config)# policy sla-class sla-class-name
vSmart(config-sla-class)# jitter milliseconds
vSmart(config-sla-class)# latency milliseconds
vSmart(config-sla-class)# loss percentage
vSmart(config-sla-class)# app-probe-class app-probe-class
vSmart(config-sla-class)# fallback-best-tunnel criterialatencylossjitter
```

4. Create an application-aware routing policy instance and associate it with a list of VPNs:

```bash
vSmart(config)# policy app-route-policy policy-name
vSmart(config-app-route-policy)# vpn-list list-name
```

5. Within the policy, create one or more numbered sequence of match–action pairs, where the match parameters define the data traffic and applications of interest and the action parameters specify the SLA class to apply if a match occurs.

   a. Create a sequence:

   ```bash
   vSmart(config-app-route-policy)# sequence number
   ```

   b. Define match parameters for data packets:

   ```bash
   vSmart(config-sequence)# match parameters
   ```

   c. Define the action to take if a match occurs:

   ```bash
   vSmart(config-sequence)# action sla-class sla-class-name [strict]
   vSmart(config-sequence)# action sla-class sla-class-name [strict] preferred-color colors
   vSmart(config-sequence)# <userinput>action backup-sla-preferred-color</userinput> <varname>colors</varname>
   <varname>colors</varname>
   ```

   The first two `action` options direct matching data traffic to a tunnel interface that meets the SLA characteristics in the specified SLA class:

   - **sla-class sla-class-name**—When you specify an SLA class with no additional parameters, data traffic that matches the SLA is forwarded as long as one tunnel interface is available. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.

   - **sla-class sla-class-name preferred-color color**—To set a specific tunnel to use when data traffic matches an SLA class, include the `preferred-color` option, specifying the color of the preferred tunnel. If more than one tunnel matches the SLA, traffic is sent to the preferred tunnel. If a tunnel of the preferred color is not available, traffic is sent through any tunnel that matches the SLA class. If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not.
• **sla-class sla-class-name preferred-color colors**—To set multiple tunnels to use when data traffic matches an SLA class, include the `preferred-color` option, specifying two or more tunnel colors. Traffic is load-balanced across all tunnels.

If no tunnel matches the SLA, data traffic is sent through any available tunnel. In this sense, color preference is considered to be a loose matching, not a strict matching, because data traffic is always forwarded, whether a tunnel of the preferred color is available or not. When no tunnel matches the SLA, you can choose how to handle the data traffic:

• **strict**—Drop the data traffic.

• **backup-sla-preferred-color colors**—Direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available; if that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. As with the `preferred-color` option, the backup SLA preferred color is loose matching. In a single action configuration, you cannot include both the `strict` and `backup-sla-preferred-color` options.

d. Count the packets or bytes that match the policy:
   ```
vSmart(config-sequence)# action count counter-name
   ```

e. Place a sampled set of packets that match the SLA class rule into syslog files:
   ```
vSmart(config-sequence)# action log
   ```

f. The match–action pairs within a policy are evaluated in numerical order, based on the sequence number, starting with the lowest number. If a match occurs, the corresponding action is taken and policy evaluation stops.

6. If a packet does not match any of the conditions in one of the sequences, a default action is taken. For application-aware routing policy, the default action is to accept nonmatching traffic and forward it with no consideration of SLA. You can configure the default action so that SLA parameters are applied to nonmatching packets:
   ```
vSmart(config-policy-name)# default-action sla-class sla-class-name
   ```

7. Apply the policy to a site list:
   ```
vSmart(config)# apply-policy site-list list-name app-route-policy policy-name
   ```

---

**Configure Application Probe Class Using CLI**

Configure app-probe-class, real-time-video and map them with the SLA class as shown in the following example:

Device(config)# app-probe-class real-time-video
Device(config)# forwarding-class videofc
Device(config)# color mpls dscp 34
Device(config)# color biz-internet dscp 40
Device(config)# color lte dscp 0

Device(config)# sla-class streamsla
Device(config)# latency 20
Device(config)# loss 10
Device(config)# app-probe-class real-time-video
Configure the default value for DSCP using BFD template as shown:

```
Device(config)# bfd default-dscp 50
Device(config)# bfd color mpls 15
```

**Application-Aware Routing Policy Configuration Example**

This topic shows a straightforward example of configuring application-aware routing policy. This example defines a policy that applies to ICMP traffic, directing it to links with latency of 50 milliseconds or less when such links are available.

You configure application-aware routing policy on a Cisco vSmart Controller. The configuration consists of the following high-level components:

- Definition of the application (or applications)
- Definition of App Probe Class (Optional)
- Definition of SLA parameters
- Definition of sites, prefixes, and VPNs
- Application-aware routing policy itself
- Specification of overlay network sites to which the policy is applied

The order in which you configure these components is immaterial from the point of view of the CLI. However, from an architectural design point of view, a logical order is to first define all the parameters that are invoked in the application-aware routing policy itself or that are used to apply the policy to various sites in the overlay network. Then, you specify the application-aware routing policy itself and the network sites to which you want to apply the policy.

Here is the procedure for configuring this application-aware routing policy on a Cisco vSmart Controller:

1. Define the SLA parameters to apply to matching ICMP traffic. In our example, we want to direct ICMP traffic to links that have a latency of 50 milliseconds or less:

   ```
   vSmart# config
   vSmart(config)# policy sla-class test_sla_class latency 50
   vSmart(config-sla-class-test_sla_class)#
   ```

2. Define the site and VPN lists to which we want to apply the application-aware routing policy:

   ```
   vSmart(config-sla-class-test_sla_class)# exit
   vSmart(config-sla-class-test_sla_class)# lists vpn-list vpn_1_list vpn 1
   vSmart(config-vpn-list-vpn_1_list)# exit
   vSmart(config-lists)# site-list site_500 site-id 500
   vSmart(config-site-list-site_500)#
   ```

3. Configure the application-aware routing policy. Note that in this example, we apply the policy to the application in two different ways: In sequences 1, 2, and 3, we specify the protocol number (protocol 1 is ICMP, protocol 6 is TCP, and protocol 17 is UDP):

   ```
   vSmart(config-site-list-site_500)# exit
   vSmart(config-lists)# exit
   vSmart(config-policy)# app-route-policy test_app_route_policy
   vSmart(config-app-route-policy-test_app_route_policy)# vpn-list vpn_1_list
   vSmart(config-vpn-list-vpn_1_list)# sequence 1 match protocol 6
   ```
4. Apply the policy to the desired sites in the Cisco IOS XE SD-WAN overlay network:

```
 vSmart(config-sequence-4)# top
 vSmart(config)# apply-policy site-list site_500 app-route-policy test_app_route_policy
```

5. Display the configuration changes:

```
 vSmart(config-site-list-site_500)# top
 vSmart(config)# show config
```

6. Validate that the configuration contains no errors:

```
 vSmart(config)# validate
 Validation complete
```

7. Activate the configuration:

```
 vSmart(config)# commit
 Commit complete.
```

8. Exit from configuration mode:

```
 vSmart(config)# exit
 vSmart#
```

Putting all the pieces of the configuration together gives this configuration:

```
vSmart# show running-config policy
policy
sla-class test_sla_class
 latency 50
!
app-route-policy test_app_route_policy
vpn-list vpn_1_list
 sequence 1
 match
 protocol 6
!
 action sla-class test_sla_class strict
!
 sequence 2
 match
 protocol 17
!
 action sla-class test_sla_class
!
 sequence 3
 match
 protocol 1
!
 action sla-class test_sla_class strict
!
```
lists
  vpn-list vpn_1_list
  vpn 1
  site-list site_500
  site-id 500
  site-list site_600
  site-id 600

apply-policy
  site-list site_500
  app-route-policy test_app_route_policy

The following example defines the multicast protocol:

policy

sla-class SLA_BEST_EFFORT
  jitter 900

sla-class SLA_BUSINESS_CRITICAL
  loss 1
  latency 250
  jitter 300

sla-class SLA_BUSINESS_DATA
  loss 3
  latency 400
  jitter 500

sla-class SLA_REALTIME
  loss 2
  latency 300
  jitter 60

app-route-policy policy_multicast
  vpn-list multicast-vpn-list
  sequence 10
  match
    source-ip 10.0.0.0/8
    destination-ip 10.255.255.254/8
  action
    count mc-counter-10
    sla-class SLA_BUSINESS_CRITICAL
  !

sequence 15
  match
    source-ip 172.16.0.0/12
    destination-ip 172.31.255.254/12
  action
    count mc-counter-15
    sla-class SLA_BEST_EFFORT
  !
sequence 20
match
destination-ip 192.168.0.1
!
action
count mc-counter-20
sla-class SLA_BUSINESS_CRITICAL
!
!
sequence 25
match
protocol 17
!
action
count mc-counter-25
sla-class SLA_REALTIME
!
!
sequence 30
match
source-ip 192.168.0.0/16
destination-ip 192.168.255.254
protocol 17
!
action
count mc-counter-30
sla-class SLA_BUSINESS_DATA preferred-color lte
!
!
default-action sla-class SLA_BEST_EFFORT
!
sequence 35
match
source-ip 10.0.0.0/8
destination-ip 10.255.255.254/8
protocol 17
!
action
count mc-counter-35
sla-class SLA_BUSINESS_DATA preferred-color lte
backup-sla-preferred-color 3g
!
!
lists
vpn-list multicast-vpn-list
vpn 1
vpn 60
vpn 4001-4010
vpn 65501-65510
!
site-list multicast-site-list
site-id 1100
site-id 500
site-id 600
!
!
apply-policy
site-list multicast-site-list
app-route-policy policy_multicast
!
## Traffic Flow Monitoring with cFlowd

### Table 28: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexible NetFlow Support for IPv6 and Cache Size Modification</td>
<td>Cisco IOS XE Release 17.4.1a Cisco vManage Release 20.4.1</td>
<td>This feature enables export of packet to external collector over IPv6 transport on Cisco IOS XE SD-WAN devices and provides the visibility of IPv6 network traffic. If you want to monitor IPv4 and IPv6 traffic together, this feature enables you to modify the cache size on the data plane. Cisco Flexible NetFlow (FNF) is a technology that provides customized visibility into network traffic. In Cisco SD-WAN, FNF enables exporting data to Cisco vManage which makes it easy for the customers to monitor and improve their network.</td>
</tr>
<tr>
<td>Log Packets Dropped by Implicit ACL</td>
<td>Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1</td>
<td>You can now enable or disable logging of dropped packets in case of a link failure. You can also configure how often the packet flows are logged.</td>
</tr>
<tr>
<td>Flexible NetFlow Enhancement</td>
<td>Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1</td>
<td>This feature enhances Flexible NetFlow to collect type of service (ToS), sampler ID and remarked DSCP values in netflow records. This enhancement provides the flexibility to define flow record fields to customize flow records by defining flow record fields. The ToS and remarked DSCP fields are supported only on IPv4 records. However, the sampler ID field is supported for both IPv4 and IPv6 records.</td>
</tr>
<tr>
<td>Flexible NetFlow for VPN0 Interface</td>
<td>Cisco IOS XE Release 17.7.1a Cisco vManage Release 20.7.1</td>
<td>This feature supports NetFlow on VPN0 interfaces. Flexible NetFlow acts as a security tool, enables export of data to Cisco vManage, detects attacks on devices, and monitors traffic.</td>
</tr>
</tbody>
</table>

- Information about Traffic Flow Monitoring, on page 156
- Configure Traffic Flow Monitoring on Cisco IOS XE SD-WAN Devices, on page 162
Information about Traffic Flow Monitoring

Traffic Flow Monitoring with Cflowd Overview

Cflowd is a flow analysis tool, used for analyzing Netflow traffic data. It monitors traffic flowing through Cisco IOS XE SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IP Flow Information Export (IPFIX) analyzer. For a traffic flow, Cflowd periodically sends template reports to flow collector. These reports contain information about the flows and the data is extracted from the payload of these reports.

You can create a Cflowd template that defines the location of Cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors (on Cisco vSmart Controllers and on Cisco vManage). You can configure a maximum of four Cflowd collectors per Cisco IOS XE SD-WAN device. To have a Cflowd template take effect, apply it with the appropriate data policy.

You must configure at least one Cflowd template, but it need not contain any parameters. With no parameters, the data flow cache on the nodes is managed using default settings, and no flow export occurs.

Cflowd traffic flow monitoring is equivalent to Flexible Netflow (FNF).

The Cflowd software implements Cflowd version 10, as specified in RFC 7011 and RFC 7012. Cflowd version 10 is also called the IP Flow Information Export (IPFIX) protocol.

Cflowd performs 1:1 sampling. Information about all flows is aggregated in the Cflowd records; flows are not sampled. Cisco IOS XE SD-WAN devices do not cache any of the records that are exported to a collector.

Note

Cisco IOS XE SD-WAN devices support only loopback interfaces as the source interface for external collectors.

Note

Netflow on Secure Internet Gateway (SIG) tunnels is not supported on Cisco IOS XE SD-WAN devices.

Cflowd and SNMP Comparison

Cflowd monitors service side traffic. Cflowd mainly monitors traffic from LAN to WAN, WAN to LAN, LAN to LAN and DIA. If you use Cflowd and SNMP to monitor traffic of LAN interface (input or output), then packets and bytes should be similar. The difference of bytes in SNMP starts from L2 header, but Cflowd starts from L3 header. However, if we use Cflowd and SNMP to monitor traffic of WAN interface (input or...
output), then packets or bytes are unlikely to be the same. All the traffic of WAN interfaces is not service side traffic. For example, Cflowd does not monitor BFD traffic, but SNMP does. The packets or bytes of Cflowd and SNMP traffic are not the same.

**IPFIX Information Elements for Cisco IOS XE SD-WAN Devices**

The Cisco SD-WAN cflowd software exports the following IPFIX information elements to the cflowd collector. Fields vary depending on the release that you are on. Common fields are exported to Cisco vManage and external exporters. Feature fields are exported only to Cisco vManage.

Before Cisco IOS XE Release 17.2.1r, Flexible Netflow exports all fields to external collectors and Cisco vManage. Starting from Cisco IOS XE Release 17.2.1r, FNF export the elements (that are marked yes) in the following table to both external collectors and Cisco vManage. Other fields like “drop cause id” are for specific features and these fields are exported only to Cisco vManage, but not to external collector.

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Element ID</th>
<th>Exported to External Collector</th>
<th>Description</th>
<th>Data Type</th>
<th>Data Type Semantics</th>
<th>Units or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceIPv4Address</td>
<td>8</td>
<td>Yes</td>
<td>IPv4 source address in the IP packet header.</td>
<td>ipv4Address (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>sourceIPv6Address</td>
<td>27</td>
<td>Yes</td>
<td>IPv6 source address in the IP packet header.</td>
<td>ipv6Address (16 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>destinationIPv4Address</td>
<td>12</td>
<td>Yes</td>
<td>IPv4 destination address in the IP packet header.</td>
<td>IPv4Address (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>destinationIPv6Address</td>
<td>28</td>
<td>Yes</td>
<td>IPv6 destination address in the IP packet header.</td>
<td>ipv6Address (16 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>ingressInterface</td>
<td>10</td>
<td>Yes</td>
<td>Index of the IP interface where packets of this flow are being received.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>ipDiffServCodePoint</td>
<td>195</td>
<td>Yes</td>
<td>Value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. This field spans the most significant 6 bits of the IPv4 TOS field.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>0 through 63</td>
</tr>
<tr>
<td>protocolIdentifier</td>
<td>4</td>
<td>Yes</td>
<td>Value of the protocol number in the Protocol field of the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>Information Element</td>
<td>Element ID</td>
<td>Exported to External Collector</td>
<td>Description</td>
<td>Data Type</td>
<td>Data Type Semantics</td>
<td>Units or Range</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>---------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>sourceTransportPort</td>
<td>7</td>
<td>Yes</td>
<td>Source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header. For GRE and IPSec flows, the value of this field is 0.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>destinationTransportPort</td>
<td>11</td>
<td>Yes</td>
<td>Destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>tcpControlBits</td>
<td>6</td>
<td>Yes</td>
<td>TCP control bits observed for the packets of this flow. This information is encoded as a bit field; each TCP control bit has a bit in this set. The bit is set to 1 if any observed packet of this flow has the corresponding TCP control bit set to 1. Otherwise, the bit is set to 0. For values of this field, see the IANA IPFIX web page.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>flowEndReason</td>
<td>136</td>
<td>Yes</td>
<td>Reason for the flow termination. For values of this field, see the IANA IPFIX web page.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>ingressoverlaysessionid</td>
<td>12432</td>
<td>Yes</td>
<td>A 32-bit identifier for input overlay session id.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>VPN Identifier</td>
<td>Enterprise specific</td>
<td>Yes</td>
<td>Cisco IOS XE SD-WAN device VPN identifier. The device uses the enterprise ID for VIP_IANA_ENUM or 41916, and the VPN element ID is 4321.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>0 through 65535</td>
</tr>
<tr>
<td>connection id long</td>
<td>12441</td>
<td>Yes</td>
<td>A 64-bit identifier for a connection between client and server.</td>
<td>Unsigned64 (8 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>application id</td>
<td>95</td>
<td>Yes</td>
<td>A 32 bit identifier for an application name</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>egressInterface</td>
<td>14</td>
<td>Yes</td>
<td>Index of the IP interface where packets of this flow are being sent.</td>
<td>unsigned32 (4 bytes)</td>
<td>default</td>
<td>—</td>
</tr>
<tr>
<td>egressoverlaysessionid</td>
<td>12433</td>
<td>Yes</td>
<td>A 32-bit identifier for output overlay session id.</td>
<td>unsigned32 (4 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>Information Element</td>
<td>Element ID</td>
<td>Exported to External Collector</td>
<td>Description</td>
<td>Data Type</td>
<td>Data Type Semantics</td>
<td>Units or Range</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
<td>--------------------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>---------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>sdwan qos-queue-id</td>
<td>12446</td>
<td>No</td>
<td>Queue index for QoS.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>drop cause id</td>
<td>12442</td>
<td>No</td>
<td>A 16-bit identifier for a drop cause name.</td>
<td>unsigned16 (2 bytes)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>counter bytes sdwan dropped long</td>
<td>12443</td>
<td>No</td>
<td>Total number of dropped octets in incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point. The count includes the IP heads and the IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>totalCounter</td>
<td>Octets</td>
</tr>
<tr>
<td>sdwan sla-not-met</td>
<td>12444</td>
<td>No</td>
<td>A Boolean to indicate if required SLA is met or not.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>sdwan preferred-color-not-met</td>
<td>12445</td>
<td>No</td>
<td>A Boolean to indicate if preferred color is met or not.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
<tr>
<td>counter packets sdwan dropped long</td>
<td>42329</td>
<td>No</td>
<td>Total number of dropped packets in incoming packets for this flow at the observation point since initialization or re-initialization of the metering process for the observation point.</td>
<td>unsigned64 (8 bytes)</td>
<td>totalCounter</td>
<td>Packets</td>
</tr>
<tr>
<td>octetDeltaCount</td>
<td>1</td>
<td>Yes</td>
<td>Number of octets since the previous report in incoming packets for this flow at the observation point. This number includes IP headers and IP payload.</td>
<td>unsigned64 (8 bytes)</td>
<td>deltaCounter</td>
<td>Octets</td>
</tr>
<tr>
<td>packetDeltaCount</td>
<td>2</td>
<td>Yes</td>
<td>Number of incoming packets since the previous report for this flow at this observation point.</td>
<td>unsigned64 (8 bytes)</td>
<td>deltaCounter</td>
<td>Packets</td>
</tr>
<tr>
<td>flowStartMilliseconds</td>
<td>152</td>
<td>Yes</td>
<td>Absolute timestamp of the first packet of this flow.</td>
<td>dateTime-MilliSeconds (8 bytes)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>flowEndMilliseconds</td>
<td>153</td>
<td>Yes</td>
<td>Absolute timestamp of the last packet of this flow.</td>
<td>dateTime-MilliSeconds (8 bytes)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>ip tos</td>
<td>5</td>
<td>Yes</td>
<td>The Type of Service field in the IP header.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>8 bits</td>
</tr>
<tr>
<td>dscp output</td>
<td>98</td>
<td>Yes</td>
<td>Value of a DSCP encoded in the Differentiated Services field. This field spans the most significant 6 bits of the IPv4 TOS field.</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>0 through 63</td>
</tr>
</tbody>
</table>
Flexable Netflow for VPN0 Interface

From Cisco IOS XE Release 17.7.1a, you can enable FNF for bidirectional traffic visibility on a VPN0 interface of a Cisco IOS XE SD-WAN device.

Netflow provides statistics on packets flowing through the device and helps to identify the tunnel or service VPNs. Flexible Netflow on VPN0 provides visibility for all the traffic (both ingress and egress) hitting VPN0 on Cisco IOS XE SD-WAN devices.

A profile is a predefined set of traffic that you can enable or disable for a context. You can create an Easy Performance Monitor (ezPM) profile that provides an express method of provisioning monitors. This new mechanism adds functionality and does not affect the existing methods for provisioning monitors. As part of this feature, you can create `sdwan-fnf` profile to monitor traffic passing through netflow VPN0 configuration.

A context represents a performance monitor policy map that is attached to an interface in ingress and egress directions. A context contains the information about the traffic-monitor that has to be enabled. When a context is attached to an interface, two policy-maps are created, one each in ingress and egress directions. Depending on the direction specified in the traffic monitor, the policy-maps are attached in that direction and the traffic is monitored. You can modify the context to override pre-defined directions.

You can create multiple contexts based on a single profile with different traffic monitors, different exporters, and different parameters for every selected traffic monitor. An ezPM context can be attached to multiple interfaces. Only one context can be attached to an interface.

<table>
<thead>
<tr>
<th>Information Element</th>
<th>Exported to External Collector</th>
<th>Description</th>
<th>Data Type</th>
<th>Data Type Semantics</th>
<th>Units or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow sampler</td>
<td>Yes</td>
<td>A set of properties that are defined in a Netflow sampler map that are applied to at least one physical interface</td>
<td>unsigned8 (1 byte)</td>
<td>identifier</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 29: Flexible Netflow Components

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Cisco SD-WAN Flexible Netflow VPN0 from Cisco vManage Release 20.7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Localized Policy: <code>app-visibility</code> or <code>flow-visibility</code></td>
</tr>
<tr>
<td></td>
<td>Centralized policy: <code>cflowd</code> policy</td>
</tr>
<tr>
<td></td>
<td>Supported on both Cisco vManage feature template and CLI template/</td>
</tr>
<tr>
<td>Interface</td>
<td>Cisco SD-WAN tunnel interface and service VPN interface</td>
</tr>
<tr>
<td></td>
<td>VPN0 interface except Cisco SD-WAN tunnel and VPN interface</td>
</tr>
</tbody>
</table>
Cisco SD-WAN Flexible Netflow

Cisco SD-WAN Flexible Netflow

| Flow Records | Fixed records by default. Supports dynamic monitoring for records such as, FEC, packet duplication, SSL proxy and so on. Also supports collecting type of service (ToS), sampler ID and remarked DSCP values for centralized policies. | Fixed records. You cannot modify or add new fields. |
| Flow Direction | Supports only ingress flows | Supports both ingress and egress by default. |
| NBAR for APP | Network-based Application recognition (NBAR) is enabled only when **app-visibility** is defined. | NBAR is enabled by default. |
| Exporter | JSON file to Cisco vManage and IPFIX to external collector | Can’t export to Cisco vManage IPFIX to external collectors |

Limitations of Flexible Netflow on VPN0 Interface

- Flexible Netflow on VPN0 is not supported on Cisco SD-WAN tunnel and Cisco SD-WAN VPN interfaces.
- The FNF record for VPN0 traffic is a fixed record and cannot be modified.
- Cisco SD-WAN VPN0 flow entries are reported to external collectors defined in CLI configuration and not to Cisco vManage.
- Cisco SD-WAN BFD and Cisco SD-WAN control connections such as OMP, Netconf, and SSH are encapsulated by Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) tunnels. FNF reports on only the DTLS traffic and not the encapsulated protocol packets.
- When FN is configured for a VPN0 WAN interface,
  - For ingress flows (WAN > Cisco SD-WAN-tunnel > LAN) - the output interface is reported as NULL.
  - For egress flows (LAN > Cisco SD-WAN-tunnel > WAN) - input interface is reported as WAN interface (Cisco SD-WAN underlay tunnels).
- VPN0 monitor supports only IPv4 and IPv6 protocols.
- For routing protocols, such as OSPF, BGP, only egress traffic is supported. Ingress OSPF and BGP traffic is treated as high priority packets.
Configure Traffic Flow Monitoring on Cisco IOS XE SD-WAN Devices

Cflowd traffic flow monitoring uses Flexible Netflow (FNF) to export traffic data. Perform the following steps to configure cflowd monitoring:

Configure Global Flow Visibility

To enable cflowd visibility globally on all Cisco IOS XE SD-WAN devices so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN.

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Localized Policy.
3. Click Add Policy.
4. Click Next up to Policy Overview to display the Configure Policy Setting page.
5. Enter Policy Name and Policy Description.
6. Check Netflow to enable flow-visibility on IPv4 traffic.
7. Check Netflow IPv6 to enable flow-visibility on IPv6 traffic.
8. Check Implicit ACL Logging to configure your Cisco IOS XE SD-WAN device to log dropped packets in the traffic.

With this configuration, you have visibility of the packets dropped by implicit access control lists (ACL) in case of a link failure in the system.
9. Enter Log Frequency.

Log frequency determines how often packet flows are logged. Maximum value is 2147483647. It is rounded down to the nearest power of 2. For example, for 1000, the logging frequency is 512. Thus, every 512th packet in the flow is logged.
10. Enter FNF IPv4 Max Cache Entries to configure FNF cache size for IPv4 traffic.

For example, enter 100 to configure FNF cache for IPv4/IPv6 traffic as shown in the following example.
11. Enter FNF IPv6 Max Cache Entries to configure FNF cache size for IPv6 traffic.

For example, enter 100 to configure FNF cache for IPv4/IPv6 traffic as shown in the following example.

---

Note

The minimum cache size value is 16. The maximum of total cache size (IPv4 cache + IPv6 cache) should not exceed the limit for each platform. If cache size is not defined and the platform is not in the list, then default maximum cache entries is 200k.

The maximum cache entries is the maximum concurrent flows that Cflowd can monitor. The maximum cache entries vary on different platforms. For more information, contact Cisco Support.
The following example shows the flow-visibility configuration for both IPv4 and IPv6:

```
policy
  flow-visibility
  implicit-acl-logging
  log-frequency 1000
  flow-visibility-ipv6
  ip visibility cache entries 100
  ipv6 visibility cache entries 100
```

While running `policy flow-visibility` or `app-visibility` to enable the FNF monitor, you may see the following warning message displaying a GLOBAL memory allocation failure. This log is triggered by enabling FNF monitoring (`policy flow-visibility` or `app-visibility`) with a large cache size.

```
Jul 4 01:45:00.255: %CPPEXMEM-3-NOMEM: F0/0: cpp_cp_svr: QFP: 0, GLOBAL memory allocation of 90120448 bytes by FNF failed
Jul 4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: CPR STILE
EXMEM GRAPH, Allocations: 877, Type: GLOBAL
Jul 4 01:45:00.258: %CPPEXMEM-3-TOPUSER: F0/0: cpp_cp_svr: QFP: 0, Top User: SBC, Bytes
Allocated: 53850112, Type: GLOBAL
```

The warning message does not necessarily indicate a flow monitor application failure. The warning message can indicate internal steps that FNF uses for applying memory from the exmem infrastructure.

To ensure that the FNF monitor is enabled successfully, use the `show flow monitor monitor-name` command to check the status (allocated or not allocated) of a flow monitor.

```
Device# sh flow monitor sdwan_flow_monitor
Flow Monitor sdwan_flow_monitor:
  Description: monitor flows for vManage and external collectors
  Flow Record: sdwan_flow_record-003
  Flow Exporter: sdwan_flow_exporter_1
                  sdwan_flow_exporter_0
  Cache:
    Type: normal (Platform cache)
    Status: allocated
    Size: 250000 entries
    Inactive Timeout: 10 secs
    Active Timeout: 60 secs
    Trans end aging: off

SUCCESS
Status: allocated
FAILURE
Status: not allocated
```

### Configure Global Application Visibility

To enable cflowd visibility globally on all Cisco IOS XE SD-WAN devices so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN.

The `app-visibility` enables `nbar` to see each application of the flows coming to the router from all VPNs in the LAN. If `app-visibility` or `app-visibility-ipv6` is defined, then `nbar` is enabled globally for both IPv4 and IPv6 flows.

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Localized Policy.
3. Click Add Policy.
4. Click Next up to Policy Overview to display the Configure Policy Setting page.

5. Enter Policy Name and Policy Description.

6. Select Application to enable app-visibility on IPv4 traffic.

7. Select Application IPv6 to enable app-visibility on IPv6 traffic.

8. Enter FNF IPv4 Max Cache Entries to configure FNF cache size for IPv4 traffic.
   For example, enter 100 to configure FNF cache size for IPv4 traffic as shown in the following example.

9. Enter FNF IPv6 Max Cache Entries to configure FNF cache size for IPv6 traffic.
   For example, enter 100 to configure FNF cache size for IPv6 traffic as shown in the following example.

The following example shows the app-visibility configuration for both IPv4 and IPv6:

```plaintext
policy
    app-visibility

    app-visibility-ipv6
    ip visibility cache entries 100
    ipv6 visibility cache entries 100
```

| Note | The `policy app-visibility` command also enables global flow visibility by enabling `nbar` to get the application name. |

Configure Cflowd Monitoring Policy

To configure policy for cflowd traffic flow monitoring, use the Cisco vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

1. Create Applications or Groups of Interest: Create lists that group together related items and that you call in the match or action components of a policy.

2. Configure Topology: Create the network structure to which the policy applies.

3. Configure Traffic Rules: Create the match and action conditions of a policy.

4. Apply Policies to Sites and VPNs: Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, create policy components or blocks. In the last screen, apply policy blocks to sites and VPNs in the overlay network. For the cflowd policy to take effect, activate the policy.

1. From the Cisco vManage menu, choose Configuration > Policies.

2. Click Custom Options. Under Centralized Policy, click Traffic Policy.

3. Click Cflowd.

4. Click Add Policy and then Create New.
5. Enter the **Name** and **Description** for the policy.

6. In the **Cflowd Template** section, enter **Active Flow Timeout**.

7. In the **Inactive Flow Timeout**, enter the timeout range.

8. In the **Flow Refresh**, enter the range.

9. In the **Sampling Interval**, enter the sample duration.

10. In the **Protocol** field, choose an option from the drop-down list.
    
    Starting from Cisco IOS XE Release 17.6.1a and Cisco vManage Release 20.6.1, the **Advanced Settings** field displays when you choose **IPv4** or **Both** from the options.

11. Under the **Advanced Settings**, do the following to collect additional IPv4 flow records:
    
    - Check the **TOS** check box.
    - Check the **Re-marked DSCP** check box.

12. Under the **Collector List**, click **New Collector**. You can configure up to four collectors.
    
    a. In the **VPN ID** field, enter the number of the VPN in which the collector is located.
    
    b. In the **IP Address** field, enter the IP address of the collector.
    
    c. In the **Port** field, enter the collector port number.
    
    d. In the **Transport Protocol** drop-down, select the transport type to use to reach the collector.
    
    e. In the **Source Interface** field, enter the name of the interface to use to send flows to the collector.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cflowd Policy Name</td>
<td>Enter a name of the cflowd policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the cflowd policy.</td>
</tr>
<tr>
<td>Active Flow Timeout</td>
<td>Specifies the active flow timeout. The range is 30 to 3600 seconds.</td>
</tr>
<tr>
<td>Inactive Flow Timeout</td>
<td>Specifies the inactive flow timeout. The range is 1 to 3600 seconds.</td>
</tr>
<tr>
<td>Flow Refresh</td>
<td>The range is 60 through 86400 seconds.</td>
</tr>
<tr>
<td>Sampling Interval</td>
<td>Specifies the sample duration. The range is 1 through 65536 seconds.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the traffic protocol type. The options are: IPv4, IPv6 or Both.</td>
</tr>
<tr>
<td></td>
<td>The default protocol is IPv4.</td>
</tr>
<tr>
<td>TOS</td>
<td>Specifies the type of field in the IPv4 header.</td>
</tr>
<tr>
<td>Re-marked DSCP</td>
<td>Specifies the traffic output specified by the remarked data policy.</td>
</tr>
<tr>
<td>VPN ID</td>
<td>Specifies the VPN ID. The range is 0 through 65536.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the collector.</td>
</tr>
</tbody>
</table>
### Specifiesthe collector port number. The range is from 1024 through 65535.

### Specifies the transport type to use to reach the collector. The options are: TCP or UDP.

### Specifies the source interface used. The options are:
- Ethernet
- FastEthernet
- FiveGigabit Ethernet
- FortyGigabit Ethernet
- Gigabit Ethernet
- Loopback
- Tunnel
- vlan and so on

13. Click **Save Cflowd Policy**.

### View Cflowd Information

To view cflowd information, use the following commands on the Cisco IOS XE SD-WAN device.

- `show sdwan app-fwd cflowd collector`
- `show sdwan app-fwd cflowd flow-count`
- `show sdwan app-fwd cflowd flows [vpn vpn-id] format table`
- `show sdwan app-fwd cflowd statistics`
- `show sdwan app-fwd cflowd template [name template-name]`
- `show sdwan app-fwd cflowd flows format table`

The following sample output displays the information cflowd:

```
Device# show sdwan app-fwd cflowd flows
Generating output, this might take time, please wait ...
app-fwd cflowd flows vpn 1 src-ip 10.2.2.11 dest-ip 10.20.24.17 src-port 0 dest-port 2048
  dscp 63 ip-proto 1
tcp-cntrl-bits 0
  icmp-opcode 2048
total-pkts 6
  total-bytes 600
  start-time "Fri May 14 02:57:23 2021"
  egress-intf-name GigabitEthernet5
  ingress-intf-name GigabitEthernet1
  application unknown
```
Configure Cflowd Traffic Flow Monitoring Using the CLI

From the CLI on the Cisco vSmart Controller that is controlling the Cisco IOS XE SD-WAN device:

1. Configure a Cflowd template to specify flow visibility and flow sampling parameters:

```bash
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template)# flow-active-timeout seconds
vSmart(config-cflowd-template)# flow-inactive-timeout seconds
vSmart(config-cflowd-template)# flow-sampling-interval number
vSmart(config-cflowd-template)# template-refresh seconds
vSmart(config-cflowd-template)# protocol ipv4|ipv6|Both
```

2. To collect TOS/DSCP output in flow monitor:

```bash
vSmart(config-cflowd-template)# customized-ipv4-record-fields
vSmart(config-customized-ipv4-record-fields)# collect-tos
vSmart(config-customized-ipv4-record-fields)# collect-dscp-output
```

3. Configure a flow collector:

```
Note
Cisco IOS XE SD-WAN devices only support UDP collector. Irrespective of the transport protocol that is configured, UDP is the default collector for Cisco IOS XE SD-WAN devices.
```

4. Configure a data policy that defines traffic match parameters and that includes the action cflowd:

```bash
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# sequence number
vSmart(config-sequence)# match match-parameters
vSmart(config-sequence)# action cflowd
```

For more information, see the `show sdwan app-fwd cflowd flows` command page.
5. Create lists of sites in the overlay network that contain the Cisco IOS XE SD-WAN devices to which you want to apply the traffic flow monitoring policy. To include multiple site in the list, configure multiple `vpn vpn-id` commands.

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-vpn-list)# vpn vpn-id
```

6. Apply the data policy to the sites in the overlay network that contain the Cisco IOS XE SD-WAN devices:

```
vSmart(config)# apply-policy site-list list-name
vSmart(config-site-list)# data-policy policy-name
vSmart(config-site-list)# cflowd-template template-name
```

## Configure Flexible Netflow on VPN0 Interface

You can enable FNF on a VPN0 interface using a CLI template or the CLI add-on template. The ezPM profile helps in creating a new profile to carry all the Netflow VPN0 monitor configuration. On selecting a profile and specifying a few parameters, ezPM provides the remaining provisioning information. A profile is a pre-defined set of traffic monitors that can be enabled or disabled for a context. You can configure Easy Performance Monitor (ezPM) and enable FNF as follows.

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile <sdwan-fnf> traffic-monitor all [ipv4/ipv6]
Device(config-perf-mon)# exporter destination <destination address> source <source interface> transport udp vrf <vrf-name> port <port-number> dscp <dscp>
```

The following example shows how to configure a performance monitor context using the sdwan-fnf profile. This configuration enables monitoring of traffic metrics. Here, 10.1.1.1 is the IP address of the third-party collector, GigabitEthernet5 is the source interface, and 4739 is the listening port of the third-party collector.

```
Device# config-transaction
Device(config)# performance monitor context <monitor_name> profile sdwan-fnf traffic-monitor all [ipv4/ipv6]
Device(config-perf-mon)# exporter destination 10.1.1.1 source GigabitEthernet5 transport udp vrf vrf1 port 4739 dscp 1
```

## Verify Flexible Netflow Configuration on VPN0 Interface

### View Flexible Netflow Record Configuration Summary

You can verify FNF record configuration using the following command.

```
Device# show flow record <monitor-context-name>
```

### Note

The monitor name is used as temp0 in the following examples.

The following sample output displays the information about IPv4 traffic flow records using ezPM profile.
Device# `show flow record temp0-sdwan-fnf-vpn0-monitor_ipv4`

flow record temp0-sdwan-fnf-vpn0-monitor_ipv4:
Description: ezPM record
No. of users: 1
Total field space: 66 bytes
Fields:
  match ipv4 dscp
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match flow direction
  collect routing next-hop address ipv4
  collect transport tcp flags
  collect interface input
  collect interface output
  collect flow sampler
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
  collect application name
  collect flow end-reason

The following sample output displays the information about IPv6 traffic flow records using ezPM profile.

Device# `show flow record temp0-sdwan-fnf-vpn0-monitor_ipv6`

flow record temp0-sdwan-fnf-vpn0-monitor_ipv6:
Description: ezPM record
No. of users: 1
Total field space: 102 bytes
Fields:
  match ipv6 dscp
  match ipv6 protocol
  match ipv6 source address
  match ipv6 destination address
  match transport source-port
  match transport destination-port
  match flow direction
  collect routing next-hop address ipv6
  collect transport tcp flags
  collect interface input
  collect interface output
  collect flow sampler
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
  collect application name
  collect flow end-reason

The following sample output displays the monitor information about IPv4 traffic netflow configuration using ezPM profile.

Device# `show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4`
Flow Monitor temp0-sdwan-fnf-vpn0-monitor_ipv4:
**View Flow Record Cache**

The following sample output displays flow record cache for the specified monitor, in this case, temp0-sdwan-fnf-vpn0-monitor_ipv4.

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv4 cache
Cache type: Normal (Platform cache)
Cache size: 5000
Current entries: 14
High Watermark: 14
Flows added: 170
Flows aged: 156
- Active timeout (60 secs) 156
IPV4 SOURCE ADDRESS: 10.0.0.0
IPV4 DESTINATION ADDRESS: 10.255.255.254
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
FLOW DIRECTION: Input
IP DSCP: 0x00
IP PROTOCOL: 1
ipv4 next hop address: 10.0.0.1
tcp flags: 0x00
interface input: Gi1
interface output: Gi2
flow sampler id: 0
counter bytes long: 840
counter packets long: 10
timestamp abs first: 02:55:24.359
timestamp abs last: 02:55:33.446
flow end reason: Not determined
application name: layer7 ping
```

---

**Traffic Flow Monitoring with cFlowd**

Verify Flexible Netflow Configuration on VPN0 Interface
The following sample output displays flow record cache for the specified IPv6 monitor, temp0-sdwan-fnf-vpn0-monitor_ipv6.

```
Device# show flow monitor temp0-sdwan-fnf-vpn0-monitor_ipv6 cache
Cache type: Normal (Platform cache)
Cache size: 5000
Current entries: 6
High Watermark: 6
Flows added: 10
Flows aged: 4
  - Inactive timeout  { 10 secs} 4

IPV6 SOURCE ADDRESS: 2001:DB8::/32
IPV6 DESTINATION ADDRESS: 2001:DB8::1
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 32768
FLOW DIRECTION: Output
IP DSCP: 0x00
IP PROTOCOL: 58
ipv6 next hop address: 2001:DB8:1::1
tcp flags: 0x00
interface input: Gi2
interface output: Gi1
flow sampler id: 0
counter bytes long: 2912
counter packets long: 28
timestamp abs first: 02:57:06.025
timestamp abs last: 02:57:33.378
flow end reason: Not determined
application name: prot ipv6-icmp
```

The following sample output displays the flow exporter details.

```
Device# show flow exporter temp0
Flow Exporter temp0:
Description: performance monitor context temp0 exporter
Export protocol: IPFIX (Version 10)
Transport Configuration:
  Destination type: IP
  Destination IP address: 10.0.0.1
  VRF label: 1
  Source IP address: 10.0.0.0
  Source Interface: GigabitEthernet5
  Transport Protocol: UDP
  Destination Port: 4739
  Source Port: 51242
  DSCP: 0x1
  TTL: 255
  Output Features: Used
  Export template data timeout: 300
Options Configuration:
  interface-table (timeout 300 seconds) (active)
  vrf-table (timeout 300 seconds) (active)
  sampler-table (timeout 300 seconds) (active)
  application-table (timeout 300 seconds) (active)
  application-attributes (timeout 300 seconds) (active)
```

Traffic Flow Monitoring with cFlowd

Verify Flexible Netflow Configuration on VPN0 Interface
Apply and Enable Cflowd Policy

For a centralized data policy to take effect, you must apply it to a list of sites in the overlay network:

```plaintext
vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

To activate the cflowd template, associate it with the data policy:

```plaintext
vSmart(config)# apply-policy cflowd-template template-name
```

For all `data-policy` policies that you apply with `apply-policy` commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`. Here, sites 70 through 100 are in both lists. If you apply these two site lists to two different `data-policy` policies, the attempt to commit the configuration on the Cisco vSmart Controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (`app-route-policy`)
- Centralized control policy (`control-policy`)
- Centralized data policy (`data-policy`)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for `control-policy` and `data-policy` policies can have overlapping site IDs. So for the two example site lists above, `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`, you could apply one to a control policy and the other to a data policy.

After you successfully activate the configuration by issuing a `commit` command, the Cisco vSmart Controller pushes the data policy to the Cisco IOS XE SD-WAN devices located in the specified sites. To view the policy as configured on the Cisco vSmart Controller, use the `show running-config` command in the Cisco vSmart Controller. To view the policy that has been pushed to the device, use the `show policy from-vsmart` command on the device.

To display the centralized data policy as configured on the Cisco vSmart Controller, use the `show running-config` command:

```plaintext
vSmart# show running-config policy
vSmart# show running-config apply-policy
```

To display the centralized data policy that has been pushed to the Cisco IOS XE SD-WAN device, issue the `show omp data-policy` command on the device:

```plaintext
Device# show sdwan policy from-vsmart
```

Enable Cflowd Visibility on Cisco IOS XE SD-WAN devices

You can enable cflowd visibility directly on Cisco IOS XE SD-WAN devices, without configuring a data policy, so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. To do this, configure cflowd visibility on the device:

```plaintext
Device(config)# policy flow-visibility
```

To monitor the applications, use the `show app cflowd flows` and `show app cflowd statistics` commands on the device.
Cflowd Traffic Flow Monitoring Configuration Example

This topic shows a straightforward example of configuring traffic flow monitoring.

**Configuration Steps**

You enable Cflowd traffic monitoring with a centralized data policy, so all configuration is done on a Cisco vSmart Controller. The following example procedure monitors all TCP traffic, sending it to a single collector:

1. Create a Cflowd template to define the location of the collector and to modify Cflowd timers.

   ```
   vsmart(config)# policy cflowd-template test-cflowd-template
   vsmart(config-cflowd-template-test-cflowd-template)# collector vpn 1 address 172.16.155.1
   port 13322 transport transport_udp
   vsmart(config-cflowd-template-test-cflowd-template)# flow-inactive-timeout 60
   vsmart(config-cflowd-template-test-cflowd-template)# template-refresh 90
   ```

2. Create a list of VPNs whose traffic you want to monitor.

   ```
   vsmart(config)# policy lists vpn-list vpn_1 vpn 1
   ```

3. Create a list of sites to apply the data policy to.

   ```
   vsmart(config)# policy lists site-list cflowd-sites site-id 400,500,600
   ```

4. Configure the data policy.

   ```
   vsmart(config)# policy data-policy test-cflowd-policy
   vsmart(config-data-policy-test-cflowd-policy)# vpn-list vpn_1
   vsmart(config-vpn-list-vpn_1)# sequence 1
   vsmart(config-sequence-1)# match protocol 6
   vsmart(config-match)# exit
   vsmart(config-sequence-1)# action accept cflowd
   vsmart(config-action)# exit
   vsmart(config-sequence-1)# exit
   vsmart(config-vpn-list-vpn_1)# default-action accept
   ```

5. Apply the policy and the Cflowd template to sites in the overlay network.

   ```
   vsmart(config)# apply-policy site-list cflowd-sites data-policy test-cflowd-policy
   Device(config-site-list-cflowd-sites)# cflowd-template test-cflowd-template
   ```

6. Activate the data policy.

   ```
   vsmart(config-site-list-cflowd-sites)# validate
   Validation complete
   vsmart(config-site-list-cflowd-sites)# commit
   Commit complete.
   ```

**Full Example Configuration**

Here is what the full example cflowd configuration looks like:

```
vsmart(config)# show configuration
apply-policy
   site-list cflowd-sites
data-policy test-cflowd-policy
cflowd-template test-cflowd-template
!```
Verify Cflowd Configuration

To verify the Cflowd configuration after activating it on the Cisco vSmart Controller, use the `show running-config policy` and `show running-config apply-policy` commands.

The following is a sample output from the `show sdwan policy from-vsmart cflowd` command:

```
Device# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
flow-active-timeout 30
flow-inactive-timeout 60
template-refresh 90
flow-sampling-interval 1
protocol ipv4/ipv6/both
customized-ipv4-record-fields
collect-tos
collect-dscp-output

collector vpn 1 address 192.0.2.1 protocol ipv4 port 13322 transport transport_udp
```

The following is a sample output from the `show sdwan policy from-vsmart` command:

```
Device# show sdwan policy from-vsmart
from-vsmart data-policy test-cflowd-policy
vpn-list vpn_1
sequence 1
match
protocol 6
action accept
cflowd
default-action accept

from-vsmart cflowd-template test-cflowd-template
flow-active-timeout 30
flow-inactive-timeout 60
```
The following is a sample output when TOS and DSCP fields are chosen for the IPv4 protocols:

Device# show flow record sdwan_flow_record-xxx

flow record sdwan_flow_record-002:
Description: flow and application visibility records
No. of users: 1
Total field space: 138 bytes
Fields:
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match routing vrf service
collect ipv4 tos
collect ipv4 dscp
collect transport tcp flags
collect interface input
collect interface output
collect flow sampler
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
collect application name
collect flow end-reason
collect ipv4 dscp output
collect overlay session id input
collect overlay session id output
collect connection id long
collect drop cause id
collect counter bytes sdwan dropped long
collect sdwan sla-not-met
collect sdwan preferred-color-not-met
collect sdwan qos-queue-id

Check the Flows

On the Cisco IOS XE SD-WAN devices affected by the Cflowd data policy, various commands let you check the status of the Cflowd flows.

Device# show sdwan app-fwd cflowd statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>data_packets</td>
<td>0</td>
</tr>
<tr>
<td>template_packets</td>
<td>0</td>
</tr>
<tr>
<td>total-packets</td>
<td>0</td>
</tr>
<tr>
<td>flow-refresh</td>
<td>123</td>
</tr>
<tr>
<td>flow-ageout</td>
<td>117</td>
</tr>
<tr>
<td>flow-end-detected</td>
<td>0</td>
</tr>
<tr>
<td>flow-end-forced</td>
<td>0</td>
</tr>
</tbody>
</table>
FNF IPv6 Configuration Example for IPv6 traffic

The following example shows the centralized policy configuration with Cflowd for IPv6 traffic:

```plaintext
policy
data-policy _vpn_1_accept_cflowd_vpn_1
  vpn-list vpn_1
    sequence 102
    match
      source-ipv6 2001:DB8:0:/32
      destination-ipv6 2001:DB8:1:/32
    !
    action accept
    count cflowd_ipv6_1187157291
    cflowd
    !
    default-action accept
  
  cflowd-template cflowd_server
  flow-active-timeout 60
  flow-inactive-timeout 30
  protocol ipv6
  
  lists
  vpn-list vpn_1
  vpn 1
  site-list vedge1
  site-id 500
  
apply-policy
site-list vedge1
  data-policy _vpn_1_accept_cflowd_vpn_1 all
  cflowd-template cflowd_server
```
### Overview of Application Performance Monitor

The Application Performance Monitor feature is a simplified framework that enables you to configure intent-based performance monitors. With this feature, you can view real-time, end-to-end application performance filtered by client segments, network segments, and server segments. This information helps you optimize application performance.

An application performance monitor is a predefined configuration that is used to collect performance metrics for specific traffic.

#### Key Concepts in Application Performance Monitoring

**Monitoring Profile:** A profile is a predefined set of traffic monitors that can be enabled or disabled for a context. As part of this feature, the sdwan-performance profile has been enhanced to include Application Response Time (ART) and media monitors to monitor traffic passing through Cisco SD-WAN tunnel interfaces. The sdwan-performance profile has a dedicated policy to filter traffic based on your intent.

When you choose the sdwan-performance profile, the related configuration is generated and applied automatically.

**Context:** A context represents a performance monitor policy map that is attached to an interface for ingress and egress traffic. A context contains information about a traffic monitor that has to be enabled. When a

---

**Table 30: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Performance Monitor</td>
<td>Cisco IOS XE Release 17.5.1a</td>
<td>This feature provides an express method for configuring an intent-based performance monitor with the help of predefined monitoring profiles. Configure this feature using the CLI Add-on feature template in Cisco vManage.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.5.1</td>
<td></td>
</tr>
</tbody>
</table>

- Overview of Application Performance Monitor, on page 177
- Limitations and Restrictions, on page 179
- Configure Application Performance Monitor, on page 180
- Verify Performance Monitoring Configuration, on page 181
context is attached to an interface, two policy-maps are created, one each for ingress and egress traffic. Depending on the direction specified in the traffic monitor, the policy maps are attached in that direction and the traffic is monitored.

Note
A context can be attached to multiple interfaces. Only one context can be attached to an interface. You can modify the context only when it is not attached to an interface.

Traffic Monitoring Specifications: You can choose to filter performance metrics using classification and sampler.

- **Classification**: Classification is a filter that defines the traffic that should be monitored for specified applications. This filter reduces the load on the device and performance collectors because they only need to monitor performance for specific applications.

- **Sampler**: A sampler monitors random traffic flows, based on the sampling rate specified, rather than all the flows. Enabling the sampler reduces scaling and performance impact when the scale of traffic is large.

Features and Benefits

- ART can be monitored for TCP flows. Some of the parameters that can be monitored are—server network delay, client network delay, and application delay.

- Jitter can be monitored for Real-time Transport Protocol (RTP) audio and video traffic.

- Information about input and output interfaces and local and remote TLOCs can be collected for every flow that matches the performance monitor.

- Performance monitor can be configured on all WAN tunnel interfaces or specific WAN tunnel interfaces using CLI commands.

- Global performance sampler is supported. The sampler allows you to monitor random flows based on the sampling rate configured, rather than the entire traffic, therefore, reducing performance and scaling overhead.
How Application Performance Monitor Works

Figure 15: Performance Monitoring Workflow

In this image, performance monitoring has been applied globally (on all tunnel interfaces). You also have the option to enable it on specific interfaces. Performance is monitored for traffic going out of, and coming into the WAN tunnel interfaces. Based on the exporter parameters defined in the context that is initiated from the monitoring profile, the metrics that are collected are sent to the third-party collector that is defined. You can then view details of the application or media that you are monitoring using various show commands.

Limitations and Restrictions

- Performance monitoring is only supported on IPv4 traffic. IPv6 traffic is not supported.
- Once a performance monitor is applied to a device, the configuration cannot be modified and reapplied to the device. Follow these steps to make any modifications to performance monitor configuration:
  1. Edit the CLI Add-on feature template or device CLI template to remove the performance monitor apply command from the template. Update the device CLI template or the device template to which the CLI Add-on feature template is attached.
  2. Edit the performance monitor context in the CLI Add-on feature template, and apply the performance monitor again using the performance monitor apply command. Update the device template to which the CLI Add-on feature template is attached.

Alternatively, configure a new context based on the same monitoring profile, and remove the previous context configuration.
- App visibility must be enabled in a policy to be able to set the connector initiator value appropriately.
Configure Application Performance Monitor

You can enable application performance monitor globally (on all WAN tunnel interfaces) or on specific WAN tunnel interfaces. You can also enable performance monitoring for ART, or media monitors, or both.

To configure application performance monitoring using Cisco vManage, create a CLI add-on feature template and attach it to the device template.

Enable Performance Monitor Globally

The following example shows how to configure a performance monitor context using the sdwan-performance profile. This configuration enables monitoring of traffic metrics for ART and media, and applies the configuration to all SD-WAN tunnel interfaces. Here, 10.0.1.128 is the IP address of the third-party collector, GigabitEthernet9 is the source interface, and 2055 is the listening port of the third-party collector.

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance
  exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
  traffic-monitor application-response-time
  traffic-monitor media
!
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel
```

Enable Performance Monitor on a Specific Interface

The following example shows how to configure a performance monitor context using the sdwan-performance profile. This configuration enables monitoring of traffic metrics for ART and media, and applies it to a specific tunnel interface, in this case, Tunnel1. Here, 10.0.1.128 is the IP address of the third-party collector, GigabitEthernet9 is the source interface, and 2055 is the listening port of the third-party collector.

```
performance monitor context CISCO-APP-MONITOR profile sdwan-performance
  exporter destination 10.0.1.128 source GigabitEthernet9 port 2055
  traffic-monitor application-response-time
  traffic-monitor media
!
interface Tunnel1
  performance monitor context CISCO-APP-MONITOR
```

Specify Additional Monitoring Filters and Sampling Rate

The following example shows how to enable specific type of traffic to be monitored. In this case, the match protocol of rtp-audio is defined in the class map named match-audio. This class in then referenced in traffic-monitor media class-and match-audio so that rtp-audio traffic is specifically monitored. Alternatively, you can use the keyword class-and. In such a case, the customized class map replaces the default class map, which is automatically created when you enable the sdwan-performance profile.

In this example, performance monitor is applied globally, which means that it is applied on all SD-WAN tunnel interfaces. The sampling rate of 10 indicates that one in 10 flows is monitored. Sampling rate 100 indicates that one in 100 flows is monitored.

```
class-map match-any match-audio
  match protocol rtp-audio
!
performance monitor context CISCO-APP-MONITOR profile sdwan-performancekeyword
  exporter destination 10.75.212.84 source GigabitEthernet0/0/0 port 2055
```
traffic-monitor application-response-time
traffic-monitor media class-and (or class-replace) match-audio
!
performance monitor apply CISCO-APP-MONITOR sdwan-tunnel
performance monitor sampling-rate 10

Verify Performance Monitoring Configuration

View Performance Monitor Configuration Summary

The following sample out displays the information about traffic monitors that are enabled and the interfaces to which they are applied.

Device# show performance monitor context CISCO-MONITOR summary

| CISCO-MONITOR | |
|----------------|

Description: User defined

Based on profile: sdwan-performance

Coarse-grain NBAR based profile

Configured traffic monitors

application-response-time:
media: class-and match_audio

Attached to Interfaces

Tunnel1

The following sample out displays operational information about the third-party exporters that are attached to the specified context.

Device# show performance monitor context CISCO-MONITOR exporter

| Exporters information of context CISCO-MONITOR | |
|------------------------------------------------|
Flow Exporter 175_SDWAN-1:

Description: performance monitor context CISCO-MONITOR exporter
Export protocol: IPFIX (Version 10)

Transport Configuration:
Destination type: IP
Destination IP address: 10.75.212.84
Source IP address: 10.74.28.19
Source Interface: GigabitEthernet0/0/0
Transport Protocol: UDP
Destination Port: 2055
Source Port: 63494
DSCP: 0x0
TTL: 255
Output Features: Used

Options Configuration:
interface-table (timeout 600 seconds) (active)
sampler-table (timeout 600 seconds) (active)
application-table (timeout 600 seconds) (active)
sub-application-table (timeout 600 seconds) (active)
application-attributes (timeout 600 seconds) (active)
tunnel-tloc-table (timeout 600 seconds) (active)

Flow Exporter 175_SDWAN-1:
Packet send statistics (last cleared 04:13:19 ago):
Successfully sent: 10270 (13709142 bytes)

Client send statistics:
Client: Option options interface-table
Records added: 312
- sent: 312
Bytes added: 31824
- sent: 31824
Client: Option options sampler-table
Records added: 28
- sent: 28
Bytes added: 1344
- sent: 1344

Client: Option options application-name
Records added: 38766
- sent: 38766
Bytes added: 3217578
- sent: 3217578

Client: Option sub-application-table
Records added: 858
- sent: 858
Bytes added: 144144
- sent: 144144

Client: Option options application-attributes
Records added: 38038
- sent: 38038
Bytes added: 9813804
- sent: 9813804

Client: Option options tunnel-tloc-table
Records added: 26
- sent: 26
Bytes added: 1352
- sent: 1352

Client: MMA EXPORTER GROUP MMA-EXP-1
Records added: 0
Bytes added: 0

Client: Flow Monitor 175_SDWAN-art_ipv4
Records added: 0
Bytes added: 0

For more information, see the `show performance monitor context` command page.

**View Flow Record Cache**

The following sample output displays flow record cache for the specified monitor, in this case, CISCO-MONITOR-art_ipv4.

```
Device# show performance monitor cache
Monitor: CISCO-MONITOR

Data Collection Monitor:

  Cache type: Synchronized (Platform cache)
  Cache size: 4000
  Current entries: 0

  Flows added: 0
  Flows aged: 0
  Synchronized timeout (secs): 60

Monitor: CISCO-MONITOR-art_ipv4

Data Collection Monitor:

  Cache type: Synchronized (Platform cache)
  Cache size: 11250
```
Current entries: 0

Flows added: 0
Flows aged: 0
Synchronized timeout (secs): 60

For more information, see the show performance monitor cache command page.

View Performance Monitor Templates

The following sample output displays flow exporter template information for the specified monitor.

Device# show flow exporter CISCO-MONITOR templates

Flow Exporter CISCO-MONITOR:

Client: Option options sampler-table
Exporter Format: IPFIX (Version 10)
Template ID : 257
Source ID : 6
Record Size : 48

Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLOW SAMPLER</td>
<td>48</td>
<td></td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>flow sampler name</td>
<td>84</td>
<td></td>
<td>4</td>
<td>41</td>
</tr>
<tr>
<td>flow sampler algorithm export</td>
<td>49</td>
<td></td>
<td>45</td>
<td>1</td>
</tr>
<tr>
<td>flow sampler interval</td>
<td>50</td>
<td></td>
<td>46</td>
<td>2</td>
</tr>
</tbody>
</table>

Client: Option options application-name
Exporter Format: IPFIX (Version 10)
Template ID : 258
Source ID : 6
Record Size : 83

Template layout
Verify Performance Monitoring Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION ID</td>
<td>95</td>
<td></td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>application name</td>
<td>96</td>
<td></td>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td>application description</td>
<td>94</td>
<td></td>
<td>28</td>
<td>55</td>
</tr>
</tbody>
</table>

Client: Option sub-application-table

Exporter Format: IPFIX (Version 10)

Template ID : 259
Source ID : 6
Record Size : 168

Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION ID</td>
<td>95</td>
<td></td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>SUB APPLICATION TAG</td>
<td>97</td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>sub application name</td>
<td>109</td>
<td></td>
<td>8</td>
<td>80</td>
</tr>
<tr>
<td>sub application description</td>
<td>110</td>
<td></td>
<td>88</td>
<td>80</td>
</tr>
</tbody>
</table>

Client: Option options application-attributes

Exporter Format: IPFIX (Version 10)

Template ID : 260
Source ID : 6
Record Size : 258

Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
</table>
Client: Option options tunnel-tloc-table
Exporter Format: IPFIX (Version 10)

Template ID : 261
Source ID : 6
Record Size : 52

Template layout

<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLOC TABLE OVERLAY SESSION ID</td>
<td>12435</td>
<td>9</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>tloc local color</td>
<td>12437</td>
<td>9</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>tloc remote color</td>
<td>12439</td>
<td>9</td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td>tloc tunnel protocol</td>
<td>12440</td>
<td>9</td>
<td>36</td>
<td>8</td>
</tr>
<tr>
<td>tloc local system ip address</td>
<td>12436</td>
<td>9</td>
<td>44</td>
<td>4</td>
</tr>
<tr>
<td>tloc remote system ip address</td>
<td>12438</td>
<td>9</td>
<td>48</td>
<td>4</td>
</tr>
</tbody>
</table>

Client: Flow Monitor CISCO-MONITOR-art_ipv4
Exporter Format: IPFIX (Version 10)

Template ID : 0
<table>
<thead>
<tr>
<th>Field</th>
<th>ID</th>
<th>Ent.ID</th>
<th>Offset</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface input snmp</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>connection client ipv4 address</td>
<td>12236</td>
<td>9</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>connection server ipv4 address</td>
<td>12237</td>
<td>9</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>ip dscp</td>
<td>195</td>
<td>12</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ip protocol</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ip ttl</td>
<td>192</td>
<td>14</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>connection server transport port</td>
<td>12241</td>
<td>9</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>connection initiator</td>
<td>239</td>
<td>17</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>timestamp absolute monitoring-interval</td>
<td>359</td>
<td>18</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>flow observation point</td>
<td>138</td>
<td>26</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>overlay session id input</td>
<td>12432</td>
<td>9</td>
<td>34</td>
<td>4</td>
</tr>
<tr>
<td>routing vrf service</td>
<td>12434</td>
<td>9</td>
<td>38</td>
<td>4</td>
</tr>
<tr>
<td>application id</td>
<td>95</td>
<td>42</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>interface output snmp</td>
<td>14</td>
<td>46</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>flow direction</td>
<td>61</td>
<td>50</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>flow sampler</td>
<td>48</td>
<td>51</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>overlay session id output</td>
<td>12433</td>
<td>9</td>
<td>52</td>
<td>4</td>
</tr>
<tr>
<td>timestamp absolute first</td>
<td>152</td>
<td>56</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>timestamp absolute last</td>
<td>153</td>
<td>64</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>connection new-connections</td>
<td>278</td>
<td>72</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>connection sum-duration</td>
<td>279</td>
<td>76</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>connection server counter bytes long</td>
<td>232</td>
<td>84</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>connection server counter packets long</td>
<td>299</td>
<td>92</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>connection client counter bytes long</td>
<td>231</td>
<td>100</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>connection client counter packets long</td>
<td>298</td>
<td>108</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>connection server counter bytes network</td>
<td>8337</td>
<td>116</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Field</td>
<td>ID</td>
<td>Ent.ID</td>
<td>Offset</td>
<td>Size</td>
</tr>
<tr>
<td>-------</td>
<td>----</td>
<td>--------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>ipv4 source address</td>
<td>8</td>
<td></td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>ipv4 destination address</td>
<td>12</td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>interface input snmp</td>
<td>10</td>
<td>8</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>ip dscp</td>
<td>195</td>
<td>12</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ip protocol</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ip ttl</td>
<td>192</td>
<td>14</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ipv6 source address</td>
<td>27</td>
<td>15</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>ipv6 destination address</td>
<td>28</td>
<td>31</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>transport source-port</td>
<td>7</td>
<td>47</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>transport destination-port</td>
<td>11</td>
<td>49</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>connection initiator</td>
<td>239</td>
<td>51</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>timestamp absolute monitoring-interval</td>
<td>359</td>
<td>52</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>flow observation point</td>
<td>138</td>
<td>60</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>overlay session id input</td>
<td>12432</td>
<td>9</td>
<td>68</td>
<td>4</td>
</tr>
<tr>
<td>routing vrf service</td>
<td>12434</td>
<td>9</td>
<td>72</td>
<td>4</td>
</tr>
<tr>
<td>application id</td>
<td>95</td>
<td>76</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>routing forwarding-status</td>
<td>89</td>
<td>80</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>interface output snmp</td>
<td>14</td>
<td>81</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>flow direction</td>
<td>61</td>
<td>85</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>flow sampler</td>
<td>48</td>
<td>86</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>overlay session id output</td>
<td>12433</td>
<td>9</td>
<td>87</td>
<td>4</td>
</tr>
<tr>
<td>transport rtp ssrc</td>
<td>4254</td>
<td>9</td>
<td>91</td>
<td>4</td>
</tr>
<tr>
<td>transport rtp payload-type</td>
<td>4273</td>
<td>9</td>
<td>95</td>
<td>1</td>
</tr>
<tr>
<td>counter bytes long</td>
<td>1</td>
<td>96</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>counter packets</td>
<td>2</td>
<td>104</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>timestamp absolute first</td>
<td>152</td>
<td>108</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>timestamp absolute last</td>
<td>153</td>
<td>116</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>connection new-connections</td>
<td>278</td>
<td>124</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>transport packets expected counter</td>
<td>4246</td>
<td>9</td>
<td>128</td>
<td>4</td>
</tr>
<tr>
<td>transport packets lost counter</td>
<td>4251</td>
<td>9</td>
<td>132</td>
<td>4</td>
</tr>
<tr>
<td>transport packets lost rate</td>
<td>4253</td>
<td>9</td>
<td>136</td>
<td>4</td>
</tr>
<tr>
<td>transport rtp jitter mean</td>
<td>4255</td>
<td>9</td>
<td>140</td>
<td>4</td>
</tr>
<tr>
<td>transport rtp jitter minimum</td>
<td>4256</td>
<td>9</td>
<td>144</td>
<td>4</td>
</tr>
<tr>
<td>transport rtp jitter maximum</td>
<td>4257</td>
<td>9</td>
<td>148</td>
<td>4</td>
</tr>
</tbody>
</table>
For more information, see the `show flow exporter` command page.
Verify Performance Monitoring Configuration
CHAPTER 13

Enhanced Policy Based Routing

Table 31: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Policy Based Routing for Cisco SD-WAN</td>
<td>Cisco IOS XE Release 17.4.1a, Cisco vManage Release 20.4.1</td>
<td>This release extends Enhanced Policy Based Routing (ePBR) to Cisco SD-WAN. ePBR is a protocol-independent traffic-steering mechanism that routes traffic based on flexible policies for traffic flows. You can create ePBR policies using CLI add-on templates in Cisco vManage.</td>
</tr>
</tbody>
</table>

- Overview of ePBR, on page 193
- Configure ePBR, on page 195
- Monitor ePBR, on page 198

Overview of ePBR

Enhanced Policy Based Routing (ePBR) is an advanced version of Policy Based Routing (PBR). With this feature, traffic forwarding is based on policies rather than routing tables, and gives you more control over routing. ePBR extends and complements the existing mechanisms provided by routing protocols. ePBR is an advanced local data policy that routes traffic based on flexible match criteria such as IPv4 and IPv6 addresses, port numbers, protocols, or packet size.

ePBR matches traffic using flexible Cisco Common Classification Policy Language (C3PL language). It supports matching prefixes, applications, Differentiated Services Code Point (DSCP), Security Group Tags (SGT), and so on. With ePBR, based on match conditions, you can configure a single or multiple next hops for traffic forwarding. You also have the option to configure Internet Protocol Service Level Agreement (IP SLA) tracking. If a configured next hop is unavailable, traffic is routed to the next available hop through dynamic probing enabled by the IP SLA tracker.

Features and Benefits

- Supports both IPv4 and IPv6.
- Supports multiple next hops; and if the next hop isn’t reachable, ePBR automatically switches to the next available hop.
• You have the option to configure IP SLA tracking. If this is configured, the next hop is selected only when the IP SLA probe is successful.

SLA probes can be configured in the same or a different VRF.

• If the current hop isn’t reachable, syslog messages are generated and the user is notified of the same.

How ePBR Works

• ePBR is applicable to unicast routing only and is based on traffic matching using C3PL.

• All packets received on an ePBR-enabled interface are passed through policy maps. The policy maps used by ePBR dictate the policy, determining where to forward packets.

• ePBR policies are based on a classification criteria (match) and an action criteria (set) that are applied to traffic flow.

• To enable ePBR, you must create a policy map that specifies the packet match criteria and desired policy-route action. Then you associate the policy map on the required interface.

• The match criteria is specified in a class. The policy map then calls the class and takes action based on the set statement.

• The set statements in ePBR policies define the route in terms of next hops, DSCP, VRFs, and so on.

Usage Example

*Figure 16: Traffic Redirection with ePBR*

This example shows that traffic is coming into VPN 1 interface. Based on the classification configured on VPN 1, the traffic overrides the regular route forwarding and is redirected to a next-hop in VPN 100, where additional network services are applied to the incoming traffic. Network services, such as WAN optimization,
Configure ePBR

To configure ePBR using Cisco vManage, create a CLI add-on feature template and attach it to the device template.

This section provides examples of ePBR configurations that you can add to the CLI add-on template.

**Configure ePBR for IPv4**

In the following example:

- The extended ACLs define the network or the host.
- Class maps match the parameters in the ACLs.
- Policy maps with ePBR then take detailed actions based on the set statements configured.
- Multiple next-hops are configured. ePBR chooses the first available next-hop.

```
ip access-list extended test300
  100 permit ip any 192.0.2.1 0.0.0.255
ip access-list extended test100
  100 permit ip any 192.0.2.20 0.0.0.255
!
class-map match-any test300
  match access-group name test300
class-map match-any test100
  match access-group name test1
!
policy-map type epbr test300
  class test300
    set ipv4 vrf 300 next-hop 10.0.0.2 10.0.40.1 10.0.50.1 ...
policy-map type epbr test100
  class test100
    set ipv4 vrf 100 next-hop 10.10.0.2 10.20.20.2 10.30.30.2 ...
!
interface GigabitEthernet0/0/1
  service-policy type epbr input test300
interface GigabitEthernet0/0/2
  service-policy type epbr input test100
```

**Configure IPv4 Tracking**

This example shows how to configure ePBR along with tracking. In the example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- The number 10 in `set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2` represents the sequence number.

```
ip sla 1
```

are then applied on the redirected traffic before it is forwarded to the SD-WAN overlay network through VPN 0.
Configure ePBR

In the following example:

- The extended ACLs define the network or the host.
- Class maps are used to match the parameters in the ACLs.
- Policy maps with ePBR then take detailed actions based on the set statements configured.
- Single or multiple next-hop addresses can be configured. ePBR selects the first available next-hop address.

```
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB81::/32
ipv6 access-list test100_v6
  sequence 100 permit ipv6 any 2001:DB82::/32
!
class-map match-any test300_v6
  match access-group name test300_v6
class-map match-any test100_v6
  match access-group name test100_v6
policy-map type epbr test300_v6
  class test300_v6
    set ipv6 vrf 300 next-hop 2001:DB8::1
policy-map type epbr test100_v6
  class test100_v6
    set ipv6 vrf 100 next-hop 2001:DB8::2 2001:DB8::FFFF:2 ...
!
interface GigabitEthernet0/0/1
  service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
  service-policy type epbr input test100_v6
```
Configure IPv6 Tracking

This example shows how to configure ePBR for IPv6 along with tracking enabled. In this example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- Tracking is configured such that if the result of the IP SLA is unavailable, the packets aren't sent to the next-hop configured on the class.

```
ip sla 3
  icmp-echo 2001:DB8::1
  vrf 100
  ip sla schedule 3 life forever start-time now
  track 3 ip sla 3 state
ip sla 4
  icmp-echo 2001:DB8::2
  vrf 300
  ip sla schedule 4 life forever start-time now
  track 4 ip sla 4 state
ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2001:DB8::/32
ipv6 access-list test100_v6
  sequence 100 permit ipv6 any 2001:DB8::1/32
class-map match-any test300_v6
  match access-group name test300_v6
class-map match-any test100_v6
  match access-group name test100_v6
policy-map type epbr test300_v6
  class test300_v6
    set ipv6 vrf 300 next-hop verify-availability 2001:DB8::2 10 track 4
policy-map type epbr test100_v6
  class test100_v6
    set ipv6 vrf 100 next-hop verify-availability 2001:DB8::1 10 track 3
interface GigabitEthernet0/0/1
  service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
  service-policy type epbr input test100_v6
```

Configure ePBR for IPv4 with Multiple Next Hops and SLA Tracking

In the following example:

- IP SLA operations of type ICMP Echo are configured and ACLs are defined.
- Class maps are then used to match parameters in the ACLs and the policy map takes action based on the set statements configured.
- Tracking is configured for next hops such that if the previous IP address isn’t reachable, and the IP SLA confirms the next hop as reachable, packets flow to the next hop address.

```
ip sla 1
  icmp-echo 10.0.0.2
  vrf 100
  ip sla schedule 1 life forever start-time now
  track 1 ip sla 1 state
ip sla 2
  icmp-echo 10.10.0.2
  vrf 300
  ip sla schedule 2 life forever start-time now
```
track 2 ip sla 2 state
ip sla 3
    icmp-echo 10.20.0.2
vrf 400
ip sla schedule 3 life forever start-time now
track 3 ip sla 3 state
ip access-list extended test300
    100 permit ip any 192.0.2.0 255.255.255.0
ip access-list extended test100
    100 permit ip any 192.0.2.10 255.255.255.0
! class-map match-any test300
    match access-group name test300
class-map match-any test100
    match access-group name test100
t policy-map type epbr test300
class test300
    set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
    set ipv4 vrf 400 next-hop verify-availability 10.20.0.2 11 track 3	policy-map type epbr test100
class test100
    set ipv4 vrf 100 next-hop verify-availability 10.0.0.2 10 track 1
! interface GigabitEthernet0/0/1
    service-policy type epbr input test300
interface GigabitEthernet0/0/2
    service-policy type epbr input test100
|

**Note** When next hops are configured along with the tracker, if the next hop is unreachable or if the IP SLA fails, the next available hop is selected. This means that when the tracker is configured, both next hop availability and IP SLA results are checked.

## Monitor ePBR

ePBR can't be monitored through Cisco vManage. To verify your configuration or monitor ePBR statistics, use the show commands described below.

### Verify Availability of Next Hop

The following is sample output from the `show platform software epbr track` command.

```
Device# show platform software epbr track
Track Object:
    obj num:2:
        track:0x7F94B4376760
        seq:10, nhop:123.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE240,
        global:0, vrf_name:300, track_reachable:1
        parent:0x7F94B4383778, oce:0x7F94B81193A8
    obj num:1:
        track:0x7F94B8187810
        seq:10, nhop:100.0.0.2, nhop_reachable:1, track_handle:0x7F94AFDAE1D0,
        global:0, vrf_name:100, track_reachable:1
        parent:0x7F94B8187778, oce:0x7F94B81188B8
```
In this example, **nhop_reachable** has the value 1, which indicates that the next hop is reachable. **track_reachable** represents the result of SLA probe and has the value 1, which indicates that the next hop is reachable. If the next hop isn’t reachable, the value would be 0 for these parameters.

**View Next Hop Configuration**

Use the `show platform software epbr R0 feature-object redirect` to view the next hop configuration.

<table>
<thead>
<tr>
<th>Feature Object ID: 9876543211</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: 0x3</td>
</tr>
<tr>
<td>Table ID: 0x4</td>
</tr>
<tr>
<td>Next-hop: 10.10.10.2</td>
</tr>
<tr>
<td>P2P ADJ-ID: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature Object ID: 1234567890</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags: 0x3</td>
</tr>
<tr>
<td>Table ID: 0x2</td>
</tr>
<tr>
<td>Next-hop: 172.16.0.0</td>
</tr>
<tr>
<td>P2P ADJ-ID: 0</td>
</tr>
</tbody>
</table>

**Note**

To be able to view this output, you must have tracker configured.
Monitor ePBR
Forward Error Correction

Table 32: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Error Correction</td>
<td>Cisco IOS XE SD-WAN Release 16.11.x</td>
<td>Feature introduced. FEC is a mechanism to recover lost packets on a link by sending extra “parity” packets for every group (N) of packets.</td>
</tr>
</tbody>
</table>

Forward Error Correction (FEC) is a mechanism to recover lost packets on a link by sending extra “parity” packets for every group (N) of packets. As long as the receiver receives a subset of packets in the group (at least N-1) and the parity packet, up to a single lost packet in the group can be recovered. FEC is supported on Cisco IOS XE SD-WAN devices.

- Configure Forward Error Correction for a Policy, on page 201
- Monitor Forward Error Correction Tunnel Information, on page 202
- Monitor Forward Error Application Family Information, on page 203

Configure Forward Error Correction for a Policy

Step 1 From the Cisco vManage menu, choose Configuration > Policies.
Step 2 Click Centralized Policy and then click Add Policy.
Step 3 Click Next.
Step 4 Click Next again and then click Configure Traffic Rules.
Step 5 Click Traffic Data, and from the Add Policy drop-down list, choose Create New.
Step 6 Click Sequence Type.
Step 7 From the Add Data Policy pop-up menu, choose QoS.
Step 8 Click Sequence Rule.
Step 9 In the Applications/Application Family List, choose one or more applications or lists.
Step 10 Click Accept.
Step 11 Click Actions and click Loss Correction.
Step 12 In the Actions area, choose one of the following:

- **FEC Adaptive**: Only send FEC information when the loss detected by the system exceeds the packet loss threshold.
• **FEC Always**: Always send FEC information with every transmission.

• **Packet Duplication** checkbox: Duplicates packets through secondary links to reduce packet loss if one link goes down.

**Step 13**  Click **Save Match and Actions**.

**Step 14**  Click **Save Data Policy**.

**Step 15**  Click **Next** and take these actions to create a centralized policy:

a)  Enter a **Name** and a **Description**.

b)  Select **Traffic Data Policy**.

c)  Choose VPNs and a site list for the policy.

d)  Save the policy.

---

**Monitor Forward Error Correction Tunnel Information**

**Step 1**  From the Cisco vManage menu, choose **Monitor > Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.

**Step 2**  Choose a device group.

**Step 3**  In the left panel, click **Tunnel**, which displays under WAN.

The WAN tunnel information includes the following:

• A graph that shows the total tunnel loss for the selected tunnels.

• A table that provides the following information for each tunnel endpoint:
  • Name of the tunnel endpoint
  • Communications protocol that the endpoint uses
  • State of the endpoint
  • Jitter, in ms, on the endpoint
  • Packet loss percentage for the endpoint
  • Latency, in ms, on the endpoint
  • Total bytes transmitted from the endpoint
  • Total bytes received by the endpoint
  • Application usage link
Monitor Forward Error Application Family Information

Step 1  From the Cisco vManage menu, choose Monitor > Devices.

Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose Monitor > Network.

Step 2  Choose a device group.

Step 3  In the left panel, click SAIE Applications, which displays under Applications.

Note  In Cisco vManage Release 20.7.x and earlier releases, SAIE Applications is called DPI Applications.

The FEC Recovery Rate application information includes the following:

- A graph for which you can choose the following perspective:
  - Application Usage—Usage of various types of traffic for the selected application families, in KB.

- A table that provides the following for each application family:
  - Name of the application family.
  - Packet Delivery Performance for the application family.

Note  If you need to see the packet delivery performance for the selected application family, ensure that packet duplication is enabled. Packet delivery performance is calculated based on the formula as displayed in the Cisco vManage tooltip for the Packet Delivery Performance column.

- Traffic usage, in KB, MB, or GB for the selected application family.
Monitor Forward Error Application Family Information
Packet Duplication for Noisy Channels

Table 33: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Duplication for Noisy Channels</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video.</td>
</tr>
</tbody>
</table>

- Information about Packet Duplication, on page 205
- Configure Packet Duplication, on page 205
- Monitor Packet Duplication Per Application, on page 206

Information about Packet Duplication

Cisco IOS XE SD-WAN devices use packet duplication to overcome packet loss.

Packet duplication sends copies of packets on alternate available paths to reach Cisco IOS XE SD-WAN devices. If one of the packets is lost, a copy of the packet is forwarded to the server. Receiving Cisco IOS XE SD-WAN devices discard copies of the packet and forward one packet to the server.

Packet duplication is suitable for edges with multiple access links. Once packet duplication is configured and pushed to your device, you can see the tunnel packet duplication statistics.

Note

Packet duplication interop on Cisco IOS XE SD-WAN devices is not supported between Cisco IOS XE Release 16.x and Cisco IOS XE Release 17.x versions.

Configure Packet Duplication

1. Select Configuration > Policies
2. Select Centralized Policy at the top of the page and then click Add Policy.
3. Click Next twice to select Configure Traffic Rules.
4. Select Traffic Data, and from the Add Policy drop-down, click Create New.
5. Click **Sequence Type** in the left pane.
6. From the Add Data Policy pop-up, select **QoS**.
7. Click **Sequence Rule**.
8. In the **Applications/Application Family List/Data Prefix**, Select one or more applications or lists.
9. Click **Actions** and select **Loss Correction**.
10. In the Actions area, select the **Packet Duplication** option to enable the packet duplication feature.
    - **FEC Adaptive**—Only send Forward Error Correction (FEC) information when the system detects a packet loss.
    - **FEC Always**—Always send FEC information with every transmission.
    - **None**—Use when no loss protection is needed.
    - **Packet Duplication**—Enable when packets need to be duplicated and sent on the next available links to reduce packet loss.
11. Click **Save Match and Actions**.
12. Click **Save Data Policy**.
13. Click **Next** and take these actions to create a Centralized Policy:
    - Enter a Name and a Description.
    - Select **Traffic Data Policy**.
    - Choose **VPNs/site list** for the policy.
    - Save the policy.

**Monitor Packet Duplication Per Application**

1. Select **Monitor > Network**
2. Select a device group.
3. In the left pane, click **Applications**.
4. On the Application usage, select the application family of interest, and click on the Application family listed.
5. If packet duplication is enabled for any application, vManage displays Packet Delivery Performance as GOOD, MODERATE, or POOR or the field displays as N/A.
6. GOOD and MODERATE performance is a clickable link. When clicking on the link, the status pops up a window.
7. On the pop-up window, you see Application, Packet Delivery Performance, Overall for the Application, Average Drop Rate, and Overall for the Application information. The time slot graph represents the packets transmitted with different available link colors and the overall performance calculated when packet duplication is enabled.
If you hover over the time slot, you can see the performance status and the average drop rate for each link.
 CHAPTER 16

Integrate Cisco IOS XE SD-WAN Device with Cisco ACI

Table 34: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with Cisco ACI</td>
<td>Cisco IOS XE SD-WAN</td>
<td>The Cisco IOS XE SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI.</td>
</tr>
<tr>
<td></td>
<td>Release 16.12.1b</td>
<td></td>
</tr>
</tbody>
</table>

Cisco ACI release 4.1(1) adds support for WAN SLA policies. This feature enables tenant administrators to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for tenant traffic over the WAN. When a WAN SLA policy is applied to tenant traffic, the Cisco APIC sends the configured policies to a Cisco vSmart Controller. The Cisco vSmart Controller, which is configured in Cisco ACI as an external device manager that provides Cisco IOS XE SD-WAN capabilities, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy.

The WAN SLA policies are applied to tenant traffic through contracts.

As an example of where this feature can be useful, consider a deployment in which branches connect to a data center over a WAN using multiple transport technologies, such as MPLS, Internet, and 4G. In such deployments, there can be multiple paths between the branches and data centers. This feature provides optimized path selection in these situations based on application groups and SLA.

- Guidelines to Integrate with Cisco ACI, on page 210
- Verify Cisco ACI Registration, on page 210
- SLA Classes, on page 210
- Data Prefixes, on page 211
- VPNs, on page 211
- Map Data Prefix and VPN to SLA, on page 211
- Create an App-Route-Policy, on page 211
- Map ACI Sites, on page 212
- Unmap ACI Sites, on page 213
- Delete a Controller, on page 213
Guidelines to Integrate with Cisco ACI

The general steps that you perform in Cisco vManage to configure the integration are:

1. Verify that Cisco ACI has registered the desired controller as a partner with a Cisco vSmart Controller, as described in the procedure, Verify Cisco ACI Registration, on page 210.

2. Attach devices to the Cisco vSmart Controller, as described in the Map ACI Sites section.

The following guidelines apply when integrating Cisco vManage with Cisco ACI:

• Only new Cisco IOS XE SD-WAN deployments support this integration.

• Make sure that any devices to which the Cisco APIC sends policies do not have any application-aware routing policies configured for them.

• Make sure each device to which the Cisco APIC sends policies has an attached template.

• Before you begin the integration, use the CLI policy builder to create a centralized policy and activate it by using the Cisco vManage policy builder.

• Before you apply WAN SLA policies, establish a connection between the Cisco vSmart Controller and the Cisco APIC. For instructions, see Cisco ACI and Cisco IOS XE SD-WAN Integration.

• Before you attach devices, configure Cisco ACI for this integration.

Verify Cisco ACI Registration

After you configure Cisco ACI for integration with Cisco vManage, perform the following steps in the Cisco vManage to verify that Cisco ACI has registered the desired controller as a Cisco vManage partner:

1. In Cisco vManage, select Administration > Integration Management.

   The Integration Management page displays.

2. On the Integration Management page, verify that ACI Partner Registration appears in the Description for the controller to which the Cisco APIC is to send policies.

SLA Classes

Cisco vManage provides preconfigured SLA classes for use with the ACI integration. These SLA classes are available automatically and cannot be modified or deleted.

To view these SLA classes, follow these steps:

1. In Cisco vManage, select Configuration > Policies.

2. From the Custom Options drop-down menu, select Lists.

3. Select SLA Class from the type list on the left.

The following SLA classes are available:
Data Prefixes

Cisco ACI creates data prefix lists that are required for integration and updates these lists dynamically as required. You do not need to configure the data prefixes in Cisco vManage.

To view these data prefixes, follow these steps:

1. In Cisco vManage, select Configuration > Policies.
2. From the Custom Options drop-down menu, select Lists.
3. Select Data Prefix from the type list on the left.

Because Cisco ACI provides these data prefixes automatically, the information in this list can vary. To make sure you are viewing current information, refresh the page occasionally.

VPNs

Cisco ACI creates VPNs that are required for integration and sends them to Cisco vManage. These VPNs become available in Cisco vManage automatically. You do not need to configure the VPNs in Cisco vManage.

To view these VPNs, follow these steps:

1. In Cisco vManage, select Configuration > Policies.
2. From the Custom Options drop-down menu, select Lists.
3. Select VPN from the type list on the left.

Map Data Prefix and VPN to SLA

After Cisco ACI establishes a mapping from a data prefix list and a VPN list to an SLA class, Cisco ACI sends the mapping to Cisco vManage. You can view these mappings in Cisco vManage on the page where you configure the app route policy.

Create an App-Route-Policy

After Cisco ACI maps a data prefix and a VPN to an SLA class list, you can create an app-route-policy to define sequence rules for the Cisco ACI integration.

To create an app-route-policy, follow these steps:
1. In Cisco vManage, select Configuration > Policies.
2. Click the More Actions icon at the right of a row that contains a centralized policy, and then click Edit.
4. Select Add Policy > Create New.
5. Click ACI Sequence Rules.
6. From the VPN drop-down, choose a VPN ID. Cisco vManage displays a list of data prefixes and SLA classes that are mapped to this VPN. (These mappings were sent by Cisco ACI.)
7. Check the box to the left of the data prefix and SLA class that you want to include with the policy, and then click Import.
8. Enter a name for the policy in the Name field and a description of the policy in the Description field, and then click Save Application Aware Routing Policy. Cisco vManage creates the policy.
9. To apply a site list and a VPN list to the policy, select Policy Application, then select Application-Aware Routing, and click New Site Lists and VPN List.
10. Select a site list and a VPN list for the policy.
11. Add sequence rules to the policy as needed.
12. Click Save Policy Changes.

Map ACI Sites

Mapping ACI sites designates the controller devices to which the policies from Cisco APIC apply. Before you begin, review the guidelines in the Guidelines to Integrate with Cisco ACI section.

To attach devices to a controller, follow these steps:

1. In Cisco vManage, select Administration > Integration Management.
2. Click the More Actions icon to the right of the row for the applicable site and select Attach Devices.
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

**Note**

To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click Select All, and then click the arrow pointing left.

5. Click Attach.
Unmap ACI Sites

Unmapping ACI sites stops Cisco APIC policies from being applied to the unmapped devices.

To detach devices from a controller, follow these steps:

1. In Cisco vManage, select **Administration > Integration Management**. The Integration Management page displays.

2. Click the **More Actions** icon to the right of the row for the applicable site and select **Detach Devices**.

3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.

4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

   **Note** To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click **Select All**, and then click the arrow pointing left.

5. Click **Detach**.

Delete a Controller

If you want to remove a controller as a partner with Cisco ACI, we recommend that you remove its registration by using Cisco ACI instead of deleting it in Cisco vManage. Deleting an ACI partner from Cisco vManage automatically deletes the data prefixes and VPNs that Cisco ACI created for the partner.

Before you begin, remove from policy definitions and data prefix lists and VPN lists that ACI created and make sure that these lists are not referenced from any policy.

1. In Cisco vManage, select **Administration > Integration Management**.

2. Detach all devices that are attached to the controller.

   For instructions, see the Detach Devices from a Controller section.

3. Click the **More Actions** icon to the right of the row for the applicable site and select **Delete Controller**.
Delete a Controller
Define Custom Applications

Table 35: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Defining Custom Applications</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>This feature adds support for defining custom applications.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

- Overview, on page 215
- Define Custom Applications Using Cisco vManage, on page 217
- View Custom Applications, on page 219

Overview

Cisco Network-Based Application Recognition (NBAR) is a Cisco technology that performs the SD-WAN Application Intelligence Engine (SAIE) flow on network traffic to identify network applications according to their traffic characteristics.

Note

In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

The specific traffic characteristics of a network application are called an application signatures. Cisco packages the signature for an application, together with other information, as a protocol. Cisco packages a large set of protocols, covering numerous commonly occurring network applications, as a Protocol Pack. Cisco updates and distributes Protocol Packs regularly. They provide a database of network application signatures for NBAR to use to identify network application traffic.

The term network applications is defined broadly, and may include all of the following, and more:

- Social media websites
- Voice over IP (VoIP) applications
- Streaming audio and video, such as Cisco Webex
- Cloud applications, such as for cloud storage
• SaaS applications
• Custom network applications specific to an organization

Identifying applications is useful for monitoring network traffic, configuring application-aware traffic policy, and more.

To summarize network application signatures, protocols, and Protocol Packs, and how NBAR uses them:

• The traffic of a network application has unique characteristics that can be used to identify the traffic as belonging to that specific application. These characteristics are called application signatures.
• Cisco packages the signature for a specific network application as a protocol.
• Cisco packages a large set of protocols, covering commonly occurring internet applications, as Protocol Packs.
• Cisco NBAR performs the SAIE flow on traffic to gather the information required to identify the sources of the traffic, and uses protocols, such as those provided in Protocol Packs, to match that information to specific network applications. The result is that NBAR identifies the network applications producing traffic in the network.

Cisco Software-Defined Application Visibility and Control (SD-AVC) uses Cisco NBAR application identification to provide information about application usage within a network.

Custom Applications

In addition to the standard protocols provided in a Protocol Pack, you can define protocols, called custom applications, to identify internet traffic, often for uncommon network applications that are of specific interest to their organization. Custom applications augment the protocols provided in a Protocol Pack.

You can use custom applications in the same way as any other protocol when configuring:

• Cisco SD-WAN policies
• Application Quality of Experience (AppQoE) policies, such as application-aware routing, TCP acceleration, and Quality of Service (QoS)

Note

The following terms are used in the documentation of related technologies, and are equivalent: custom applications, custom protocols, user-defined applications

Custom Applications in Cisco SD-WAN

One function of Cisco SD-AVC, which is included as a component of Cisco SD-WAN, is to create and manage custom applications. Cisco SD-WAN uses this Cisco SD-AVC functionality, through SD-AVC REST APIs, to enable you to define custom applications within Cisco SD-WAN.

As a Cisco SD-WAN user, you can use Cisco vManage to define custom applications. Cisco SD-AVC then pushes the custom applications to devices in the network. The devices in the network use the custom applications and other application protocols to analyze traffic traversing the devices.

The process of defining a custom protocol includes choosing criteria to identify network traffic as coming from a specific network application. The criteria can include characteristics of hosts originating the traffic, such as server names, IP addresses, and so on.
Priority of Protocols and Custom Applications

It is possible to define custom applications that match some of the same traffic as a protocol included in the Protocol Pack operating with Cisco NBAR. When matching traffic, custom applications have priority over Protocol Pack protocols.

Define Custom Applications Using Cisco vManage

Prerequisite: Install Cisco SD-AVC as a component of Cisco SD-WAN.

1. In Cisco vManage, select Configuration > Policies.
2. Select Centralized Policy.
3. Click Custom Options and select Centralized Policy > Lists.
4. Click Custom Applications, and then click New Custom Application.
5. To define the application, provide an application name and enter match criteria. The match criteria can include one or more of the attributes provided: server names, IP addresses, and so on. You do not need to enter match criteria for all fields.

The match logic follows these rules:

• Between all L3/L4 attributes, there is a logical AND. Traffic must match all conditions.
• Between L3/L4 and Server Names, there is a logical OR. Traffic must match either the server name or the L3/L4 attributes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>(mandatory)</td>
</tr>
<tr>
<td></td>
<td>Enter a name for the custom application.</td>
</tr>
<tr>
<td></td>
<td>Maximum length: 32 characters</td>
</tr>
<tr>
<td>Server Names</td>
<td>One or more server names, separated by commas.</td>
</tr>
<tr>
<td></td>
<td>You can include an asterisk wildcard match character (*) only at the beginning of the server name.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>See Notes and Limitations, on page 218.</td>
</tr>
<tr>
<td>L3/L4 Attributes</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter one or more IPv4 addresses, separated by commas.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>10.0.1.1, 10.0.1.2</td>
</tr>
<tr>
<td></td>
<td>Note The subnet prefix range is 24 to 32.</td>
</tr>
</tbody>
</table>
### Define Custom Applications Using Cisco vManage

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Enter one or more ports or port ranges, separated by commas. Example: 30, 45-47</td>
</tr>
<tr>
<td>L4 Protocol</td>
<td>Select one of the following: TCP, UDP, TCP-UDP</td>
</tr>
</tbody>
</table>

6. Click **Add**. The new custom application appears in the table of custom applications.

---

**Note**

To check the progress of creating the new custom application, click **Tasks** (clipboard icon). A panel opens, showing active and completed processes.

---

**Notes and Limitations**

- Maximum number of custom applications: 1100
- Maximum number of L3/L4 rules: 20000
- Maximum number of server names: 50000
- For server names, maximum instances of wildcard followed by a period (.): 50000
  
  Example: *.cisco.com matches www.cisco.com, developer.cisco.com
- For server names, maximum instances of prefix wildcard as part of server name: 256
  
  Example: *ample.com matches www.example.com
- Mapping the same domain to two different custom applications is not supported.
- Activation of custom applications:
  - When using Cisco vManage releases earlier than 20.5.1: For devices using releases earlier than Cisco IOS XE 17.5.1, the activation of custom applications is as follows:
    - A custom application created in Cisco vManage is not activated for visibility functionality (monitoring traffic) or control functionality (traffic policy) until a policy that makes use of the custom application is applied.
  - When using Cisco vManage Release 20.5.1 or later: For devices using Cisco IOS XE Release 17.5.1a or later, the activation of custom applications is as follows:
    - A custom application created in Cisco vManage is activated immediately for application visibility functionality only (monitoring traffic), such as for protocol-discovery counters and Flexible NetFlow (FNF). When activated for visibility functionality only, custom applications do not affect traffic policy.
    - When the custom application is used by a policy, it becomes activated for control functionality (traffic policy) also.
**Example Custom Application Criteria**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>How to configure fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td><strong>Server Names:</strong> cisco.com</td>
</tr>
<tr>
<td>Set of IP addresses, set of ports, and L4</td>
<td><strong>IP Address:</strong> 10.0.1.1, 10.0.1.2</td>
</tr>
<tr>
<td>protocol</td>
<td><strong>Ports:</strong> 20, 25-37</td>
</tr>
<tr>
<td></td>
<td><strong>L4 Protocol:</strong> TCP-UDP</td>
</tr>
<tr>
<td>Set of ports and L4 protocol</td>
<td><strong>Ports:</strong> 30, 45-47</td>
</tr>
<tr>
<td></td>
<td><strong>L4 Protocol:</strong> TCP</td>
</tr>
</tbody>
</table>

**View Custom Applications**

**View Custom Applications in Cisco vManage**

After you define a custom application, it appears in the Application List, which shows all available protocols and custom applications. The Application List is available here:

**Configuration > Policies > Centralized Policy > Custom Options > Centralized Policy > Lists > Application List.**

**View Protocols and Custom Applications on a Device**

Use the `show ip nbar protocol-id` command to display all protocols and custom applications that are loaded on the router. It is helpful to filter the results. For example, to display all protocols and custom applications with "custom" in the name, use this:

```
v5#show ip nbar protocol-id | include custom
custom_amazon                    3899     PPDK LOCAL
custom_facebook                  3284     PPDK LOCAL
```

See `show ip nbar protocol-id`. 
Service Chaining

Table 36: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service insertion tracker support</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>This feature extends support for service chaining to Cisco IOS XE SD-WAN devices. On Cisco IOS XE SD-WAN devices and Cisco vEdge devices, it adds a tracking feature that logs the availability of a service.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

Service chaining allows data traffic to be rerouted through one or more services, such as firewall, load balancer, and intrusion detection and prevention (IDP) devices.

Services in the Network

Services such as firewall, load balancer, and intrusion detection and prevention (IDP) are often run within a virtualized environment, and they may physically be centralized in one location or in several locations for redundancy. Services may be internal, cloud based, or external subscriptions. Networks must be able to reroute traffic from any location in the network through such services.

Customers want the ability to internally spawn or externally subscribe to new services on demand—for capacity, redundancy, or simply to select best-of-breed technologies. For example, if a firewall site exceeds its capacity, a customer can spawn new firewall service at a new location. Supporting this new firewall would require the configuration of policy-based, weighted load distribution to multiple firewalls.

Following are some of the reasons to reroute a traffic flow through a service or chain of services:

• Traffic flow from a less secure region of a network must pass through a service, such as a firewall, or through a chain of services to ensure that it has not been tampered with.

• For a network that consists of multiple VPNs, each representing a function or an organization, traffic between VPNs must traverse through a service, such as a firewall, or through a chain of services. For example, in a campus, interdepartmental traffic might go through a firewall, while intradepartmental traffic might be routed directly.

• Certain traffic flows must traverse a service, such as a load balancer.
Today, the only way to reroute traffic flow is by provisioning every routing node—from the source to the service node to the systems beyond the service node—with a policy route. This is done either by having an operator manually configure each node or by using a provisioning tool that performs the configuration for each node on behalf of the operator. Either way, the process is operationally complex to provision, maintain, and troubleshoot.

Provisioning Services in the Cisco SD-WAN Overlay Network

In the Cisco SD-WAN solution, the network operator can enable and orchestrate all service chaining from a central controller, that is, from the Cisco vSmart Controller. No configuration or provisioning is required on any of the devices.

The general flow of service chaining in a Cisco SD-WAN network is as follows:

- Devices advertise the services available in their branch or campus—such as firewall, IDS, and IDP—to the Cisco vSmart Controllers in their domain. Multiple devices can advertise the same services.
- Devices also advertise their OMP routes and TLOCs to the Cisco vSmart Controllers.
- For traffic that requires services, the policy on the Cisco vSmart Controller changes the next hop for the OMP routes to the service landing point. In this way, the traffic is first processed by the service before being routed to its final destination.

The following figure illustrates how service chaining works in the Cisco SD-WAN solution. The network shown has a centralized hub router that is connected to two branches, each with a device. The standard network design implements a control policy such that all traffic from branch site 1 to branch site 2 travels through the hub router. Sitting behind the hub router is a firewall device. So now, assume we want all traffic from site 1 to site 2 to first be processed by the firewall. Traffic from the device at site 1 still flows to the hub router, but instead of sending it directly to site 2, the hub router redirects the traffic to the firewall device. When the firewall completes its processing, it returns all cleared traffic to the hub, which then passes it along to the device at site 2.

Service Route SAFI

The hub and local branch devices advertise the services available in their networks to the Cisco vSmart Controllers in its domain using service routes, which are sent by way of OMP using the service route Subsequent Address Family Identifier (SAFI) bits of the OMP NLRI. The Cisco vSmart Controllers maintain the service routes in their RIB, and they do not propagate these routes to the devices.

Each service route SAFI has the following attributes:

- VPN ID (vpn-id)—Identifies the VPN that the service belongs to.
- Service ID (svc-id)—Identifies the service being advertised by the service node. The Cisco SD-WAN software has the following predefined services:
  - FW, for firewall (maps to svc-id 1)
• IDS, for Intrusion Detection Systems (maps to svc-id 2)
• IDP, for Identity Providers (maps to svc-id 3)
• netsvc1, netsvc2, netsvc3, and netsvc4, which are reserved for custom services (they map to svc-id 4, 5, 6, and 7, respectively)

• Label—For traffic that must traverse a service, the Cisco vSmart Controller replaces the label in the OMP route with the service label in order to direct the traffic to that service.

• Originator ID (originator-id)—The IP address of the service node that is advertising the service.

• TLOC—The transport location address of the device that is “hosting” the service.

• Path ID (path-id)—An identifier of the OMP path.

Service Chaining Policy

To route traffic through a service, you provision either a control policy or a data policy on the Cisco vSmart Controller. You use a control policy if the match criteria are based on a destination prefix or any of its attributes. You use a data policy if the match criteria include the source address, source port, DSCP value, or destination port of the packet or traffic flow. You can provision the policy directly using the CLI, or it can be pushed from Cisco vManage.

The Cisco vSmart Controller maintains OMP routes, TLOC routes, and service routes in its route table. A given OMP route carries a TLOC and the label associated with it. On a Cisco vSmart Controller, a policy can be applied that changes the TLOC and its associated label to that of a service.

Tracking the Health of the Service Chain

Beginning with Cisco IOS XE Release 17.3.1a, Cisco SD-WAN periodically probes devices providing network services to test whether they are operational. Tracking the availability of devices in the service chain helps to prevent a null route, which can occur if a policy routes traffic to a service device which is not available. By default, Cisco SD-WAN writes the tracking results to a service log, but this can be disabled.

Service insertion over tunnel interface is not supported on Cisco IOS XE SD-WAN devices.

Note
Configure Service Chaining

Table 37: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service insertion tracker support</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>This feature extends support for service chaining to Cisco IOS XE SD-WAN devices. On Cisco IOS XE SD-WAN devices and Cisco vEdge devices, it adds a tracking feature that logs the availability of a service.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

Here is the workflow for configuring service chaining for a device managed by Cisco SD-WAN:

1. Service devices are accessed through a specific VRF. In the VPN template that corresponds to the VRF for a service device, configure service chaining, specifying the service type and device addresses. By default, the tracking feature adds each service device status update to the service log. You can disable this in the VPN template.

2. Attach the VPN template to the device template for the device managed by Cisco SD-WAN.

3. Apply the device template to the device.

Configure Service Chaining Using Cisco vManage

To configure service chaining for a device:

1. In Cisco vManage, create a VPN template.

2. Click Service.

3. In the Service section, click New Service and configure the following:
   - Service Type: Select the type of service that the service device is providing.
   - IP Address: IP Address is the only working option.
   - IPv4 Address: Enter between one and four addresses for the device.
   - Tracking: Determines whether the periodic health updates of the service device are recorded in the system log. Default: On

4. Click Add. The service appears in the table of configured services.

Note Maximum number of services: 8
**CLI Equivalent for Cisco IOS XE SD-WAN Devices**

The following table shows how configuration of service chaining by CLI corresponds to configuration in Cisco vManage. CLI configuration differs between Cisco IOS XE SD-WAN devices and Cisco vEdge devices. The CLI example below is for a Cisco IOS XE SD-WAN device.

<table>
<thead>
<tr>
<th>CLI (Cisco IOS XE SD-WAN device)</th>
<th>Cisco vManage</th>
</tr>
</thead>
<tbody>
<tr>
<td>service firewall vrf 10</td>
<td>In Cisco vManage, configure service insertion in the VPN template for a specific VRF—VRF 10 in this example. Select the service type from the drop-down—firewall in this example.</td>
</tr>
<tr>
<td>no track-enable</td>
<td>When adding a service in the VPN template <strong>Service</strong>, select <strong>On</strong> or <strong>Off</strong> for <strong>Tracking</strong>.</td>
</tr>
<tr>
<td>ipv4 address 10.0.2.1 10.0.2.2</td>
<td>In the VRF template <strong>Service</strong>, enter one or more IP addresses for the service device providing a specific service.</td>
</tr>
</tbody>
</table>

**Note**

Default: enabled

**CLI Example**

```
sdwan
  service firewall vrf 10
  ipv4 address 10.0.2.1 10.0.2.2
  commit
```

**CLI Equivalent for Cisco vEdge Devices**

The following table shows how configuration of service chaining by CLI corresponds to configuration in Cisco vManage. CLI configuration differs between Cisco IOS XE SD-WAN devices and Cisco vEdge devices. The CLI example below is for a Cisco vEdge device.

<table>
<thead>
<tr>
<th>CLI (Cisco vEdge device)</th>
<th>Cisco vManage</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpn 10</td>
<td>In Cisco vManage, configure service insertion in the VPN template—VPN 10 in this example. Select the service type from the drop-down—firewall in this example.</td>
</tr>
<tr>
<td>service FW address 10.0.2.1</td>
<td>Select the service type from the drop-down—firewall in this example. Provide one or more addresses for the service device.</td>
</tr>
<tr>
<td>no track-enable</td>
<td>When adding a service in the VPN template <strong>Service</strong>, select <strong>On</strong> or <strong>Off</strong> for <strong>Tracking</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Default: enabled</td>
</tr>
</tbody>
</table>

**CLI Example**

```
vpn 10
  service FW address 10.0.2.1
  commit
```
Service Chaining Configuration Examples

Service chaining control policies direct data traffic to service devices that can be located in various places in the network before the traffic is delivered to its destination. For service chaining to work, you configure a centralized control policy on the Cisco vSmart Controller, and you configure the service devices themselves on the device collocated in the same site as the device. To ensure that the services are advertised to the Cisco vSmart Controller, the IP address of the service device must resolve locally.

This topic provides examples of configuring service chaining.

Route Intersite Traffic through a Service

A simple example is to route data traffic traveling from one site to another through a service. In this example, we route all traffic traveling from the device at Site 1 to the device at Site 2 through a firewall service that sits behind a hub (whose system IP address is 100.1.1.1). To keep things simple, all devices are in the same VPN.

For this scenario, you configure the following:

- On the hub router, you configure the IP address of the firewall device.
- On the Cisco vSmart Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall service.
- On the Cisco vSmart Controller, you apply the control policy to Site 1.

Here is the configuration procedure:

1. On the hub router, provision the firewall service, specifying the IP address of the firewall device. With this configuration, OMP on the hub router advertises one service route to the Cisco vSmart Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the hub router and a service label of svc-id-1, which identifies the service type as a firewall. (As mentioned above, before advertising the route, the device ensures that the firewall's IP address can be resolved locally.)

   ```
sdwan
   service firewall vrf 10
   ipv4 address 10.1.1.1
   ```

2. On the Cisco vSmart Controller, configure a control policy that redirects data traffic traveling from Site 1 to Site 2 through the firewall. Then, also on the Cisco vSmart Controller, apply this policy to Site 1.

   ```
policy
   lists
   site-list firewall-sites
   site-id 1
   ```
control-policy firewall-service
  sequence 10
  match route
  site-id 2
  action accept
  set service FW vpn 10
  default-action accept
apply-policy
  site-list firewall-sites control-policy firewall-service out

This policy configuration does the following:

- Create a site list called `firewall-sites` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to. If you later want to scale this policy so that all traffic destined to Site 2 from other sites should also first pass through the firewall, all you need to do is add the additional site IDs to the `firewall-sites` site list. You do not need to change anything in the `control-policy firewall-service` portion of the configuration.

- Define a control policy named `firewall-service`. This policy has one sequence element and the following conditions:
  - Match routes destined for Site 2.
  - If a match occurs, accept the route and redirect it to the firewall service provided by the Hub router, which is located in VPN 10.
  - Accept all nonmatching traffic. That is, accept all traffic not destined for Site 2.

- Apply the policy to the sites listed in `firewall-list`, that is, to Site 1. The Cisco vSmart controller applies the policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:
  - The TLOC is changed from Site 2’s TLOC to the hub router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the hub router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the hub router
  - The label is changed to svc-id-1, which identifies the firewall service. This label causes the hub router to direct the traffic to the firewall device.

When the hub router receives the traffic, it forwards it to the address 10.1.1.1, which is the system IP address of the firewall. After the firewall has finished processing the traffic, the firewall returns the traffic to the hub router, and this router then forwards it to its final destination, which is Site 2.

**Route Inter-VPN Traffic through a Service Chain with One Service per Node**
A service chain allows traffic to pass through two or more services before reaching its destination. The example here routes traffic from one VPN to another through services located in a third VPN. The services are located behind different hub routers. Specifically, we want all traffic from device-1 in VPN 20 and that is destined for prefix x.x.0.0/16 in VPN 30 on device-2 to go first through the firewall behind Hub-1 and then through the custom service netsvc1 behind Hub-2 before being sent to its final destination.

For this policy to work:

- VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet
- VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.
- VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
- VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure four things:

- You configure the IP address of the firewall device on the Hub-1 router.
- You configure the IP address of the custom service device on the Hub-2 router.
- On the Cisco vSmart Controller, you configure a control policy that redirects traffic destined from Site 1 to Site 2 through the firewall device.
- On the Cisco vSmart Controller, you configure a second control policy that redirects traffic to the custom service device.

Here is the configuration procedure:

1. Configure the firewall service on Hub-1. With this configuration, OMP on the Hub-1 router advertises a service route to the Cisco vSmart Controller. The service route contains a number of properties that identify the location of the firewall, including the TLOC of the hub router and a service label of svc-id-1, which identifies the service type as a firewall.

```
sdwan
service firewall vrf 10
ipv4 address 10.1.1.1
```

2. Configure the custom service netsvc1 on Hub-2. With this configuration, OMP on the Hub-2 router advertises a service route to the vSmart controller. The service route contains the TLOC of the Hub-2 and a service label of svc-id-4, which identifies the custom service.

```
sdwan
service netsvc1 vrf 10
ipv4 address 2.2.2.2
```

3. Create a control policy on the Cisco vSmart Controller for first service in the chain—the firewall—and apply it to Site 1, which is the location of the device-1 router:

```
policy
    lists
        site-list firewall-custom-service-sites
            site-id 1
        control-policy firewall-service
            sequence 10
                match route
                    vpn 30
                    site-id 2
                action accept
                set service FW
```
This policy configuration does the following:

• Create a site list called `firewall-custom-service-sites` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to.

• Define a control policy named `firewall-service` that has one sequence element and the following conditions:
  • Match routes destined for both VPN 30 and Site 2.
  • If a match occurs, accept the route and redirect it to a firewall service.
  • If a match does not occur, accept the traffic.

• Apply the policy to the sites in the `firewall-custom-service-sites` site list, that is, to Site 1. The Cisco vSmart controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 1. In these routes:
  • The TLOC is changed from Site 2’s TLOC to the Hub-1 router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the hub. It is because of the change of TLOC that traffic destined for Site 2 is directed to the Hub-1 router.
  • The label is changed to svc-id-1, which identifies the firewall service. This label causes the Hub-1 router to direct the traffic to the firewall device.

When the Hub-1 router receives the traffic, it forwards it to the address 10.1.1.1, which is the system IP address of the firewall. After the firewall completes processing the traffic, it returns the traffic to the Hub-1 router, which, because of the policy defined in the next step, forwards it to the Hub-2 router.

4. Create a control policy on the Cisco vSmart Controller for the second service in the chain, which is the custom service, and apply it to the site of the Hub-1 router:

```
policy
  site-list custom-service
  site-id 3
  control-policy netsvc1-service
  sequence 10
  match route
    vpn 30
    site-id 2
  action accept
  set service netsvc1
  default-action accept
apply-policy
  site-list custom-service control-policy netsvc1-service out
```

This policy configuration does the following:

• Create a site list called `custom-service` that is referenced in the `apply-policy` command and that enumerates all the sites that this policy applies to.

• Define a control policy named `netsvc1-service` that has one sequence element and the following conditions:
  • Match routes destined for both VPN 30 and Site 2.
  • If a match occurs, accept the route and redirect it to the custom service.
• If a match does not occur, accept the traffic.

• Apply the policy to the sites in the custom-service list, that is, to Site 3. The Cisco vSmart controller applies this policy in the outbound direction, that is, on routes that it redistributes to Site 3. In these routes:
  • The TLOC is changed from Site 2’s TLOC to the Hub-2 router’s TLOC. This is the TLOC that the Cisco vSmart Controller learned from the service route received from the Hub-2 router. It is because of the change of TLOC that traffic destined for Site 2 is directed to the Hub-2 router.
  • The label is changed to svc-id-4, which identifies the custom service. This label causes the Hub-2 to direct the traffic to the device that is hosting the custom service.

When the Hub-2 routers receives the traffic, it forwards it to the address 2.2.2.2, which is the system IP address of the device hosting the custom service. After the traffic has been processed, it is returned to the Hub-2 router, which then forwards it to its final destination, Site 2.

**Route Inter-VPN Traffic through a Service Chain with Multiple Services per Node**

If a service chain has more than one service that is connected to the same node, that is, both services are behind the same device, you use a combination of control policy and data policy to create the desired service chain. The example here is similar to the one in the previous section, but instead has a firewall and a custom service (netsvc-1) behind a single hub router. Here, we want all data traffic from device-1 in VPN 20 destined for prefix x.x.0.0/16 on device-2 in VPN 30 to first go through the firewall at Hub-1, then through the custom service netsvc1, also at Hub-1, and then to its final destination.

For this policy to work:
• VPN 10, VPN 20, and VPN 30 must be connected by an extranet, such as the Internet.
• VPN 10 must import routes from VPN 20 and VPN 30. Routes can be selectively imported if necessary.
• VPN 20 must import routes from VPN 30. Routes can be selectively imported if necessary.
• VPN 30 must import routes from VPN 20. Routes can be selectively imported if necessary.

For this scenario, you configure the following:
• On the hub router, you configure the firewall and custom services.
• On the Cisco vSmart Controller, you configure a control policy that redirects data traffic from Site 1 that is destined to Site 2 through the firewall.
• On the Cisco vSmart Controller, you configure a data policy that redirects data traffic to the custom service.
Here is the configuration procedure:

1. On the hub router, configure the firewall and custom services:

```
    sdwan
    service firewall vrf 10
        ipv4 address 10.1.1.1
    service netsvc1 vrf 10
        ipv4 address 2.2.2.2
```

With this configuration, OMP on the hub router advertises two service routes to the Cisco vSmart Controller, one for the firewall and the second for the custom service netsvc1. Both service routes contain the TLOC of the Hub-1 router and a service label that identifies the type of service. For the firewall service, the label is svc-id-1, and for the custom service, the label is svc-id-4.

2. On the Cisco vSmart Controller, configure a control policy controller to reroute traffic destined for VPN 30 (at Site 2) to firewall service that is connected to Hub-1 (at Site 3), and apply this policy to Site 1:

```
    policy
    lists
        site-list device-1
        site-id 1
        control-policy firewall-service
            sequence 10
            match route
            vpn 30
            action accept
            set service FW
    apply-policy
        site-list device-1 control-policy firewall-service out
```

3. On the Cisco vSmart Controller, configure a data policy that redirects, or chains, the data traffic received from the firewall device to the custom service netsvc1. Then apply this policy to Hub-1. This data policy routes packets headed for destinations in the network x.x.0.0/16 to the IP address 2.2.2.2, which is the system IP address of the device hosting the custom service.

```
    policy
    lists
        site-list device-2
        site-id 2
        site-list Hub-1
        site-id 3
        prefix-list svc-chain
            ip-prefix x.x.0.0/16
        vpn-list vpn-10
        vpn 10
        data-policy netsvc1-policy
            vpn-list vpn-10
            sequence 1
            match
            ip-destination x.x.0.0/16
            action accept
            set next-hop 2.2.2.2
    apply-policy
        site-list Hub-1 data-policy netsvc1-policy from-service
```

Monitor Service Chaining

You can monitor different aspects of service chaining on hub and spoke devices.
**Note** Configuring a service device to operate as part of the service chain is called service insertion.

- On a hub device, view the configured services.
  - From the Cisco vManage menu:
    - View the configured services on the Real Time monitoring page (Monitor > Devices > hub-device > Real Time). For Device Options, select OMP Services.
  - Cisco vManage Release 20.6.x and earlier: View the configured services on the Real Time monitoring page (Monitor > Network > hub-device > Real Time). For Device Options, select OMP Services.

- On a spoke device, view the details of the service chain path.
  - Using Cisco vManage:
    - View the service chain path on the Traceroute page (Monitor > Devices > spoke-device > Troubleshooting > Connectivity > Trace Route). Enter the destination IP, VPN, and source interface for the desired path.
  - Cisco vManage Release 20.6.x and earlier: View the service chain path on the Traceroute page (Monitor > Network > spoke-device > Troubleshooting > Connectivity > Trace Route). Enter the destination IP, VPN, and source interface for the desired path.
  - Using the CLI:
    - Use the `traceroute` command. For information, see the Cisco SD-WAN Command Reference.

**Example: View a Service Chain Path Between Two Spoke Devices**

The following example shows how to view the path between two spokes before and after adding a service chain between them, using Cisco vManage or the CLI.

For clarity, the example presents a scenario of two spoke devices, a hub device, and a service device providing a firewall service, and shows how to configure the firewall service chain.

Here are the details for each device in the scenario:

<table>
<thead>
<tr>
<th>Device</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub, through interface ge0/4</td>
<td>10.20.24.15</td>
</tr>
<tr>
<td>Spoke 1</td>
<td>10.0.3.1</td>
</tr>
<tr>
<td>Spoke 2</td>
<td>10.0.4.1</td>
</tr>
<tr>
<td>Service device (firewall service)</td>
<td>10.20.24.17</td>
</tr>
</tbody>
</table>

Configuration of the three devices:

```
Hub
v5# show running-config vpn 1
vpn 1
  name ospf_and_bgp_configs
  service FW
```
address 10.20.24.17
exit
router
ospf
  router-id 10.100.0.1
timers spf 200 1000 10000
redistribute static
redistribute omp
area 0
  interface ge0/4
  exit
exit

! interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
!
interface ge0/5
  ip address 10.30.24.15/24
  no shutdown
!

Spoke 1
-------
  vpn 1
    name ospf_and_bgp_configs
    interface ge0/1
      ip address 10.0.3.1/24
      no shutdown
    

Spoke 2
-------
  vpn 1
    interface ge0/1
      ip address 10.0.4.1/24
      no shutdown
    

1. Without Service Insertion:

At this point, no service insertion policy has been configured, so executing `traceroute` on Spoke 1 to display the path details to Spoke 2 (10.0.4.1) shows a simple path to Spoke 2:

→ Spoke 2 (10.0.4.1)

```
vm4# traceroute vpn 1 10.0.4.1
Traceroute 10.0.4.1 in VPN 1
ttraceroute to 10.0.4.1 (10.0.4.1), 30 hops max, 60 byte packets
  1  10.0.4.1 (10.0.4.1)   7.447 ms 8.097 ms 8.127 ms
```

Similarly, viewing the Traceroute page in Cisco vManage shows a simple path from Spoke 1 to Spoke 2.

2. With Service Insertion:

The following Cisco vSmart Controller policy configures service insertion for a firewall service, using the firewall service device described above.
After configuring the service insertion, executing **traceroute** on Spoke 1 (10.0.3.1) to display the path details to Spoke 2 (10.0.4.1) shows this path:

→ Hub (10.20.24.15) → Firewall service device (10.20.24.17) → Hub (10.20.24.15) → Spoke 2 (10.0.4.1)

```
Traceroute -m 15 -w 1 -s 10.0.3.1 10.0.4.1 in VPN 1
traceroute to 10.0.4.1 (10.0.4.1), 15 hops max, 60 byte packets
1 10.20.24.15 (10.20.24.15) 2.187 ms 2.175 ms 2.240 ms
2 10.20.24.17 (10.20.24.17) 2.244 ms 2.868 ms 2.873 ms
3 10.20.24.15 (10.20.24.15) 2.959 ms 4.910 ms 4.996 ms
4 10.0.4.1 (10.0.4.1) 5.045 ms 5.213 ms 5.247 ms
```

Similarly, viewing the **Traceroute** page in Cisco vManage shows each step of the path from Spoke 1 to Spoke 2, through the hub and firewall service device.
Lawful Intercept

The Lawful Intercept (LI) feature supports service providers in meeting the requirements of law enforcement agencies (LEA) to provide electronic surveillance as authorized by a judicial or administrative order. The surveillance is performed using wiretaps to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual using IP sessions. A user session is tapped using either the Source and Destination IP addresses, or VRF name, which is translated to a vrf-tableid value within the router.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption of Lawful Intercept</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature encrypts lawful intercept messages between a Cisco IOS XE SD-WAN device and a media device using static tunnel information.</td>
</tr>
</tbody>
</table>

- Information About Lawful Intercept, on page 235
- Prerequisites for Lawful Intercept, on page 238
- Install Lawful Intercept using vManage, on page 239
- Lawful Intercept MIBs, on page 239
- Restrict Access to Trusted Hosts (Without Encryption), on page 240
- Restrict Trusted Mediation Device, on page 240
- Configure Lawful Intercept, on page 241
- Configure Lawful Intercept Using CLI, on page 241
- Encrypt Lawful Intercept Traffic, on page 242
- Verify Static Tunnel with Media Device Gateway, on page 244

Information About Lawful Intercept

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance.
**Lawful Intercept Process**

When triggering a lawful intercept for communications from Site A to Site B, the edge platform duplicates the traffic and sends an unencrypted copy of the traffic to a target server, which hosted in the customer network designed for Lawful Intercept. Cisco vManage ensures that Cisco vManage users (non-Lawful Intercept users), who have access to Site A and Site B for any information, are unaware of the duplicated flow of information.

_Figure 17: Cisco-SD-WAN Lawful Intercept Workflow_
Licence-based Lawful Intercept

Cisco SD-WAN solution is a term-based licensed feature. This feature license enables the Cisco vManage component of the Cisco SD-WAN solution and allows the customer to access the Lawful Intercept function. Once the Lawful Intercept license is enabled on the solution, Cisco vManage provides a new privilege in the Manage Users menu of the Cisco vManage UI. By default, this privilege is available to all admin users. In addition, administrators can assign the Lawful Intercept privilege to any other user.

Any user with Lawful Intercept privilege would be able to enable Lawful Intercept function on an edge device in the WAN network. All changes made by any user with Lawful Intercept function would be audit logged and changes will be recorded just like any other change made by any user in the system.

After acquiring a court order or warrant to perform surveillance, any user with Lawful Intercept privilege will be able to make Lawful Intercept related changes on sites with a warrant.

1. Install license for Lawful Intercept on Cisco vManage.
2. Create an lawful intercept admin (liadmin) user on Cisco vManage. The liadmin user must be associated with the user group, Basic.
3. Login to Cisco vManage as liadmin user and configure Lawful Intercept specific templates.
4. Cisco vManage automatically pushes templates to all Cisco IOS XE SD-WAN devices with Lawful Intercept compatible images.
5. Configuration is pushed to device from Cisco vManage using the following:
Prerequisites for Lawful Intercept

Access to the Cisco Lawful Intercept MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS). In DNS, the router IP address is typically the address of the FastEthernet0/0/0 interface on the router.
- The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).
- You must add the mediation device to the Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.
  - When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device’s authorization password if you want. The password must be at least eight characters in length.
- You must configure SNMP service in vManage using the VPN Interface Ethernet page of Feature Template. See VPN Interface Ethernet section in Templates topic.
Install Lawful Intercept using vManage

Note: The following process must be repeated for every Cisco vManage node.

1. Connect to a Cisco vManage device as administrator

2. Request tools license
   ```
   vm12# tools license request
   Your org-name is: XYZ Inc
   Your license-request challenge is: Uwk3u4Vwk18n63fKDIpKDEFkzfeJ1hFQPOHapvwmed0U83LQDgaJO7GnmCIgA
   ```

3. Contact Cisco Support to generate the license using the output of Step 2.

4. Run the install file command and reboot:
   ```
   vm12# tools license install file license.lic
   License installed. Please reboot to activate.
   vm12# reboot
   Are you sure you want to reboot? [yes,no] yes
   ```

5. Verify if the Lawful Intercept license is installed successfully, using the following command:
   ```
   vm12# show system status
   LI License Enabled True
   ```

6. Create lawful intercept admin user using Cisco vManage.

7. Login to Cisco vManage using the lawful intercept admin credentials.

Note: Use the `tools license remove-all` command to remove all licenses after reboot. You will not be able to re-install the previous license.

Lawful Intercept MIBs

Due to its sensitive nature, the Cisco Lawful Intercept MIBs are only available in software images that support the Lawful Intercept feature.

These MIBs are not accessible through the Network Management Software MIBs Support page.

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts must be allowed to access the Lawful Intercept MIBs. To restrict access to these MIBs, you must perform the following actions:
Restrict Access to Trusted Hosts (Without Encryption)

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the `snmp-server` command in global configuration mode.

In the following example, the access list named 99 allows SNMP traffic only from 10.1.1.1 to access Cisco IOS XE SD-WAN devices. This access list is then applied to the SNMP user, testuser.

```plaintext
access-list 99 permit ip host 10.1.1.1
snmp-server user testuser INTERCEPT_GROUP v3 encrypted auth sha testPassword1 priv aes testPassword2 access 99

SNMP traffic is only allowed from WAN interface (gigabitEthernet 1).
```
You can configure up to a maximum of eight Mediation Device List subnets.

**Configure Lawful Intercept**

The following are the two components for Lawful Intercept vManage configuration:

- **Lawful Intercept SNMP template** – This template provisions the configuration for the following:
  - SNMPv3 group for lawful intercept – The group name is `INTERCEPT_GROUP` by default.
  - SNMPv3 users for lawful intercept – All users are restricted by an access list by default.
  - SNMPv3 view is configured by default. The view included Cisco TAP MIBs.
  - The following TAP MIBs are configured:
    - `ciscoIpTapMIB`
    - `ciscoTap2MIB`
    - `ifIndex`
    - `ifDescr`

- **Lawful intercept access list template** – The access list template provides configuration for the following:
  - Mediation Device-List configuration – Provides option to configure up to 8 subnets.
  - SNMP access-list – provides option to configure up to 8 subnets or host addresses, and a wildcard mask.

**Configure Lawful Intercept Using CLI**

```plaintext
control-plane host
management-interface GigabitEthernet0/0/0 allow ftp ssh snmp
management-interface GigabitEthernet0/0/1 allow ftp ssh snmp

md-list 10.101.0.0 255.255.255.0
md-list 10.102.0.10 255.255.255.255
md-list 10.103.0.0 255.255.255.0
md-list 10.104.0.4 255.255.255.255
md-list 10.105.0.0 255.255.255.0
md-list 10.106.0.0 255.255.255.0
md-list 10.107.0.7 255.255.255.255
md-list 10.108.0.0 255.255.0.0

ip access-list standard li-acl
  permit 174.16.50.254
```
Example: Enabling Mediation Device Access Lawful Intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```snmp
snmp-server enable trap
snmp-server engineID local 766D616E6167652Dac10ff31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW notify SNG_VIEW
snmp-server engineID local 766D616E6167652DAC10FF31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW notify SNG_VIEW
snmp-server view INTERCEPT_VIEW ciscoIpTapMIB included
snmp-server view INTERCEPT_VIEW ciscoTap2MIB included
snmp-server view INTERCEPT_VIEW ifIndex included
snmp-server view INTERCEPT_VIEW ifDescr included
```

Encrypt Lawful Intercept Traffic

Encryption of intercepted traffic between the router (the content Intercept Access Point (IAP)) and the Mediation Device (MD) is recommended.

The following is the required configuration:

- Configuring encryption in the router, and either an encryption client in the MD or a router associated with the MD to decrypt the traffic.
- Restricting access to trusted hosts.
- Configuring the VPN client.

Configure Encryption in the Device

To configure encryption, configure Authentication, Authorization, and Accounting (AAA) parameters. The following example shows how to configure the parameters:

```snmp
aaa authentication login userauthen local
username <username> password 0 <password>
```

In CISCO-TAP2-MIB, the source interface must be the tunnel interface of the Cisco IOS XE SD-WAN devices and the destination address must be IP address of the mediation device.
Configure Lawful Intercept Encryption using CLI

In the following example, an IPSec tunnel is configured between Cisco IOS XE SD-WAN device and Media Device Gateway. Media Device Gateway terminates IPSec tunnel and adds a route to Media Device list through the IPSec Tunnel.

In CISCO-TAP2-MIB, source interface is the tunnel interface of the Cisco IOS XE SD-WAN devices; destination address is the IP address of the media device.

crypto ikev2 diagnose error 1000
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123

! crypto ikev2 profile ikev2_profile
authentication local pre-share
authentication remote pre-share
dpd 10 3 on-demand
lifetime 14400
keyring local ikev2_keyring
match identity remote address 0.0.0.0 0.0.0.0
!
crypto ikev2 proposal default
encryption aes-cbc-256
group 14 16 19 2 20 21
integrity sha256 sha384 sha512
!
crypto ipsec profile ipsec_profile
set ikev2-profile ikev2_profile
set pfs group16
set transform-set tfs
set security-association lifetime seconds 7200
set security-association replay window-size 256
!
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
!
interface Tunnel100
no shutdown
ip address 10.2.2.1 255.255.255.0
tunnel address
ip route 10.3.3.0 255.255.255.0 Tunnel100

Use the following configuration to configure media gateway to terminate IPSec tunnel:

crypto ikev2 proposal default
encryption aes-cbc-256
integrity sha384 sha512 sha256
group 20 16 19 14 21 2
!
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123
!
crypto ikev2 profile ikev2_profile
match identity remote address 0.0.0.0 0.0.0.0
authentication remote pre-share
authentication local pre-share
dp 10 3 on-demand
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
crypto ipsec profile ipsec_profile
set security-association lifetime seconds 7200
set security-association replay window-size 256
set transform-set tfs
set pfs group16
set ikev2-profile ikev2_profile
!
interface Tunnel100
ip address 10.2.2.2 255.255.255.0
  □ Tunnel address
tunnel source GigabitEthernet1
  □ MD GW phy interface
tunnel mode ipsec ipv4
tunnel destination 10.74.5.213
  □ cEdge wan interface
tunnel protection ipsec profile ipsec_profile

Verify Static Tunnel with Media Device Gateway

The IPSec tunnel between the Cisco IOS XE SD-WAN device and the Media Device gateway is static and is always in the UP state.

Use the following commands to verify static tunnel configuration with the Media Device gateway:

• show crypto session detail

• show crypto ipsec sa