ılıılı cısco

Prescriptive Deployment Guide Cisco Public

# **Cisco SD-WAN: Application-Aware Routing**

# **Prescriptive Deployment Guide**

May, 2020

# Contents

Introduction	3
About this Guide	4
Define	5
Design	12
Deploy	18
Process: Prerequisites for Application-Aware Routing	18
Process: (Optional) Configuring custom BFD template	21
Process: Configuring Application-Aware Routing policy	24
Process: Appending Application-Aware Routing policy	40
Operate	56
Process: Monitor the Application-Aware Routing policy	56
Process: Monitor the WAN transport path characteristics	60
Process: Monitor the Application-Aware Routing Statistics	64
Process: Monitor Events - SLA, BFD, App-route changes	67
Process: Visualize traffic path selection on the WAN Edge	71
Appendix A: Product List	74
Feedback	75

# Introduction

This guide is intended to provide design and deployment guidance to deploy Application-Aware Routing on the Cisco SD-WAN solution providing Service Level Agreement (SLA) based routing for business-critical applications to optimize application performance. The guide focuses on the step-by-step procedures for defining the network characteristics requirements for an application and leveraging the calculated path liveness and quality measurement to influence the traffic path dynamically, providing the best experience for the applications at all times.

The ability to consider the path characteristic in path selection offers a number of advantages to the Cisco SD-WAN solution:

- In normal network operation, the path taken by application 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 business critical data traffic to the best available paths that meets the SLA. As the network recovers from the brownout or 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.

#### Figure 1. Application Performance optimization using Application-Aware Routing overview



# About this Guide

This prescriptive deployment guide focuses on design considerations and deployment best practices for Application Aware Routing within the Cisco SD-WAN solution. In this guide, SD-WAN controllers are deployed in the cloud and WAN Edge routers are deployed either at remote sites or at the datacenter and are connected to two WAN transports, Internet and MPLS.

Although this deployment guide is about Application Aware Routing. It is presumed that

- Cisco SD-WAN Controllers (vManage, vBond, and vSmart) are already deployed with valid certificates.
- Cisco WAN Edge device is onboarded and have established control connections to Cisco SD-WAN controllers and data tunnels to other WAN Edge devices across all available transports.
- Cisco SD-WAN WAN Edge and vSmart controller have configuration feature templates defined, and device template associated and are in vManage mode.

For more information on SD-WAN controller design and deployment, please refer to the <u>Cisco SD-WAN Design</u> <u>guide</u>, <u>Cisco SD-WAN End-to-End Deployment guide</u> and the <u>Cisco WAN Edge Onboarding Prescriptive</u> <u>Deployment guide</u>.

This document contains four major sections:

The **Define** section provides a high-level overview of the SD-WAN architecture and components and Application-Aware Routing components.

The **Design** section provides detailed discussion on the design considerations and prerequisites needed to deploy Application-Aware Routing.

The **Deploy** section discusses step-by-step procedures to configure Application-Aware Routing policies in the Cisco SD-WAN network. It walks through the best practices and gotchas to consider during the process.

The **Operate** section briefly discusses how to monitor and troubleshoot the common issues.

Refer to Appendix A for details on the platform and software versions used to build this document.

## Audience

The intended audience for this document includes network design engineers and network operations personnel who have deployed the Cisco SD-WAN components and are looking for the best viable option to provide service level quality for applications running on the Cisco SD-WAN infrastructure.

# Define

# About the solution

The Cisco SD-WAN solution is an enterprise-grade SD-WAN architecture overlay that enables digital and cloud transformation for enterprise. The solution fully integrates routing, security, centralized policy and orchestration into large-scale networks and addresses the problems and challenges of common WAN deployments.

The Cisco SD-WAN solution is comprised of separate orchestration, management, control and data plane.

- **Orchestration plane** assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay. The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers.
- **Management plane** is responsible for central configuration and monitoring. The vManage controller is the centralized network management system that provides a single pane of glass GUI interface to easily deploy, configure, monitor and troubleshoot all Cisco SD-WAN components in the network.
- **Control plane** builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.
- **Data plane** is responsible for forwarding packets based on decisions from the control plane. WAN Edge physical or virtual devices provide secure data-plane connectivity between the sites in the same SD-WAN overlay network. WAN Edge devices are responsible for establishing secure connections for traffic forwarding, for security, encryption, Quality of Service (QoS) enforcement and more.



Figure 2. Cisco SD-WAN solution components Orchestration Plane

In this prescriptive deployment guide, we focus on ensuring real-time dynamic path selection for businesscritical application based on the end-to-end WAN network traffic conditions.

Upon securely onboarding the WAN Edge device in the Cisco SD-WAN overlay network, the WAN Edge device establishes secure control connections with all the controllers (vBond, vManage, vSmart) where it receives

configuration, policies and routing information. The WAN Edge device would then establish secure IPsec tunnels with other WAN Edges, which is part of the same SD-WAN overlay network, to forward data-traffic.





The Cisco SD-WAN solution leverages NETCONF to provision the WAN Edge devices with the associated template configuration in the vManage and Overlay Management Protocol (OMP) to convey the control-plane information such as route-prefixes, next-hop routes, crypto keys and policy information between the vSmart controllers and the WAN Edge devices. By default, with no policies defined, the SD-WAN overlay network would form full-mesh topology, allowing each WAN Edge device to establish a secure IPsec connection to other WAN Edge device.

It is important to note that the WAN Edge device establishes a permanent persistent connection to the vSmart controller over each available WAN transport and a single permanent persistence connection to the vManage over only one WAN transport.



Figure 4. SD-WAN components - secure control and data connections

# **Bi-directional Forward Detection (BFD)**

Upon establishing secure IPsec data-plane tunnels between the WAN Edge devices, BFD session are initiated on each of the tunnel established between the WAN Edge devices. The BFD probes monitors the network characteristics – loss, latency and jitter on the tunnels. By default, the BFD Hello packet is sent every 1 second and this value can be changed on a per tunnel basis.

The BFD operates in echo mode where BFD messages generated by the WAN Edge device are reflected (echoed) back by the remote WAN Edge device. Each BFD packet is time-stamped by the originating WAN Edge device to determine the round-trip latency and jitter. Path loss or tunnel liveness is determined based on the lost BFD packets.

The WAN Edge device collects the packet loss, latency and jitter for every BFD probe (default BFD Hello packets are sent 1 sec on every WAN transport) and is preserved for every poll interval (the default poll interval value is 10 minutes). The network path liveliness, by default, is calculated for a period of 6 poll intervals for better accuracy and to dampen any intermittent reclassification (flapping) of the tunnel. At the seventh poll interval, the earliest polling data is discarded to accommodate the latest information.

BFD packets being forwarded at regular intervals enables the SD-WAN overlay network to not only detect any blackout situations but also detect path characteristics such loss, latency, jitter, path-MTU that can then be leveraged by other SD-WAN protocols to make dynamic decision and provide the best quality of experience for business-critical applications.





# Service Level Agreement (SLA)

Cisco SD-WAN solution provides the network administrator procedure to define the desired SLA for the business-critical traffic. The SLA characteristics defines the desired loss, latency and jitter for the specified classified traffic.

The WAN Edge devices determines the WAN transports path characteristics - loss, latency and jitter from the previously discussed BFD probes sent across each tunnel between the WAN Edge devices.

- Packet loss is calculated on the WAN Edge device on a per tunnel basis and is measured as percentage 0 through 100 percent.
- Jitter is calculated on the WAN Edge device on a per tunnel basis and is a measurement of millisecond, 0 through 1000 milliseconds.
- Latency is calculated on the WAN Edge device on a per tunnel basic and is a measurement of millisecond, 0 through 1000 milliseconds.

Note: Calculated Packet Loss, Jitter and Latency are average values for the poll intervals and are round-trip measurements on each tunnel interface on the WAN Edge device.

Application-Aware Routing leverages the calculated network path characteristics values as a measurement and compares with the desired SLA for the application, to dynamically optimize the data path selection for the traffic on the WAN Edge device.

## Policies

The Cisco SD-WAN solution separates the control plane functionality managed by vSmart controller with the data plane functionality operated by the WAN Edge devices. Similarly, the Cisco SD-WAN policy architecture separates the control policies that influence the routing information shared between vSmart controllers and the WAN Edge devices, with the data policies that influences the data traffic between the WAN Edge devices.

Policies, either control or data, are configured in vManage, provisioned and enforced either at vSmart controller influencing network-wide or locally on the WAN Edge influencing a specific parameter for the device.





By default, with no policy associated to the any SD-WAN components in the solution. In this scenario:

- WAN Edge devices advertise routes to vSmart controllers through the OMP protocol.
- The vSmart controller advertises the full routing information that is learnt from all WAN Edge devices to all other WAN Edge devices through the OMP protocol.
- SD-WAN WAN Edge devices establish data plane connections to all other WAN Edge devices forming a full-mesh topology.

Centralized policy, either control policy or data policy, is configured in vManage.

 The centralized control policy is applied to the routing information that is stored in the vSmart controller and enforced before the routes are advertised to the WAN Edge devices allowing for customizing routing decisions and determining the routing paths through the overlay network.

The centralized control policy configuration remains on the vSmart controller and is never pushed to the WAN Edge devices.

 The centralized data policy is applied to the data traffic flow for the specified VPNs in the overlay network. These policies permit or restrict access based on 6-tuples (source-ip, destination-ip, source-port, destination-port, protocol, dscp values) or based on VPN memberships allowing for customizing routing decision and determining routing paths at a local site.

Depending on the policies, the policy is provisioned on vSmart, pushed (via OMP protocol) and enforced on the WAN Edge devices.

Localized policy, either control policy or data policy, is configured in vManage.

- Localized control policy is applied to the routing information that is stored on the WAN Edge device influencing the routing behavior on the device at local site level.
- Localized data policy is applied on the interface of the WAN Edge device. The data policy is leveraged to match traffic and defines QoS, policing, mirroring at the interface level of the WAN Edge device.

Figure 7. Centralized and Localized Policies



## **Application-Aware Routing**

Advanced features set such as Application-Aware Routing provide network administrators the necessary flexibility to pin certain business-critical application to a specific WAN transport on the device. Actively probe the network and path characteristics and dynamically re-route the application traffic, in real-time, on the WAN transport links that meets the specified application SLA requirements.

#### Figure 8. Application-Aware Routing



Cisco SD-WAN WAN Edge device supports up to 8 TLOCs, allowing a single device to be connected to 8 different WAN transports. Each WAN Edge device in the SD-WAN environment advertises its local routes to the vSmart controller using OMP protocol. The vSmart controller computes the best path selection algorithm for the entire SD-WAN environment and applies any configured centralized control policy before advertises the route-selection to the WAN Edge devices.

The WAN Edge device installs the received OMP route in its forwarding table. For destination prefixes with multiple best paths, the device natively performs Layer-3 ECMP (Equal Cost Multiple Path) load-balancing across 4 reachable next-hop TLOCs. The number of paths installed on the WAN Edge device can be increased to 16 as long as the next-hop is reachable.

SLAs for each of the transport tunnels are calculated periodically using BFD probes by the WAN Edge device and is made available for advanced features like Application-Aware Routing to leverage and provide deterministic experience for business-critical applications.

Application-Aware Routing allows the network administrator to evaluate the network path characteristics for the selected business critical applications and set a preferred path as long as the SLAs are satisfied and a backup preferred path. The backup preferred path is chosen when no available WAN transport(s) meets the specified SLA.

Application-Aware Routing policy is configured in vManage as a centralized data policy that maps the serviceside application(s) to specific SLA requirements. The centralized policies provisioned in vSmart controller is pushed to relevant WAN Edge devices for enforcement. The defined policy consists of match-action pairs, where the match statement defines the application-list or the type of traffic to match, and the action statement defines the SLA action the WAN Edge devices must enforce for the specified traffic.

# Design

# **Application-Aware Routing Components**

Cisco SD-WAN Application-Aware Routing consists of three components:

- Identification Classify the traffic / Application group of interest.
- Application SLA Requirement Defining the application SLA requirements.
- Application-Aware Routing Policy Policy maps the classified traffic to the transport tunnel based on the defined SLA requirement.



#### Figure 9. Application Aware Routing components

## Identification - Classify the traffic / Application group of interest

First step in defining the Application-Aware Routing (AAR) is to choose the traffic or application group of interest that requires preferred treatment or Service Level Agreement (SLA) to be met. The vManage centralized policy wizard provides the network administrator options to match and define groups of interest as shown below:

List Type	Groups of Interest
Application List	Application - specify the application or application list Application Family - specify the application family list(s)
Prefix	Network prefix that can be matched for source or destination addresses

In addition to above, network administrator can also match traffic based on:

List Type	Groups of Interest
Cloud SaaS Application List	Leverage the pre-defined Cloud-SaaS Application list
DNS Application List	DNS application list is mainly used when the network deployment needs split DNS lookup for certain application or application-lists.
DNS	DNS lookup (DNS request / response) packets can be matched.
DSCP	Pre-configured traffic with DSCP values, through QoS policy on the service-side traffic, can be leveraged.
PLP	Pre-configured traffic part of the Packet Loss Priority (PLP) queue, configured part of QoS policy, can be matched.
Protocol	Traffic with certain protocol number.
Source Data Prefix	Pre-defined custom data-prefix of the traffic.
Source Port	Data traffic with defined port number.
Destination Data Prefix	Pre-defined custom data-prefix of the traffic.
Destination Port	Data traffic with defined port number.

## Deep Packet Inspection

Cisco WAN Edge device have integrated Deep packet Inspection (DPI) engine to identify and classify applications including voice and video, email, file sharing, gaming, peer-to-peer (P2P), and cloud-based applications. Viptela WAN Edge devices leverages Qosmos DPI to classify the traffic and Cisco IOS-XE SD-WAN devices uses NBAR2 to identify a wide variety of applications from the network traffic flows using L3 to L7 data.

Cisco IOS-XE SD-WAN devices can incorporate SD-AVC along with the NBAR2 DPI engine providing the capability to inspect and classify the flows on the first packet. Once the applications are classified, policies can leverage this information to match on the application and/or application-list and influence the traffic.

## **Service Level Agreement**

Next step in defining the Application-Aware Routing (AAR) Policy is to set Service Level Agreement (SLA). The Service Level Agreement specifics the network path characteristics (loss, latency and jitter) that the application can handle for optimized performance.

The vManage centralized policy wizard provides network administrator options to define custom Service Level Agreement (SLA) or leverage the pre-defined SLA's as shown below:

Name	Loss (%)	Latency (msec)	Jitter (msec)
Transactional-Data	5	50	100
Bulk-Data	10	300	100
Voice-And-Video	2	45	100
Default	25	300	100

The pre-defined SLA values (Loss, Latency and Jitter) are specific to the WAN transport characteristics and are round-trip measurement. The pre-defined SLA class values, shown in the above table, may or may not fit the deployment needs. vManage provides administrates the flexibility to define custom SLA class instead of leveraging the pre-defined SLA class.

#### **Tech tip**

Before defining custom SLA values, monitor the current WAN transport SLA statistics across the SD-WAN environment by navigating to vManage > Main Dashboard > Application-Aware Routing widget.

By default, the Loss, Latency and Jitter values are calculated for every WAN transport available on the WAN Edge device and are made available for a period of up to 7 days. This historical data can be used as a baseline to evaluate and define custom SLA values to better fit the environment and the application requirements.

Careful consideration must to taken when choosing the SLA values. Choosing a more aggressive values might cause undesired result with too many SLA violations, while choosing a more relaxed values might not yield the desired result for the enterprise.

Administrators can define any number of custom SLA's but can associate only 4 SLA's to the Application-Aware Routing policy. Please check the Release Notes for the corresponding software version on the number of SLA supported for the release.

# Application-Aware Routing Policy - Policy maps the classified traffic to the WAN transport based on the defined SLA requirement.

The Application-Aware Routing policy defined in vManage binds the selected application/traffic list with the SLA. For all matched data-traffic traversing from LAN/Service side to remote site through the device WAN transports, the AAR policy defines the

 Preferred Color – the selected data traffic is pinned to the chosen WAN transport(s) as long as the transport(s) meets the specified SLA.

Note that when multiple WAN transports are selected and transports satisfying the SLA requirements, the WAN Edge performs ECMP load balancing across the tunnels for the selected data traffic.

- Strict if enabled, the selected data traffic would be dropped if all the WAN transport(s) do not meet the specified SLA. If there is at least one path meeting the SLA, traffic is forwarded on that path.
- Backup SLA Preferred Color the selected data traffic is pinned to the chosen WAN transport(s) only when no transport(s) meets the specified SLA and Strict option is not enabled.
- Log if enabled, a syslog message is generated first time a packet flow is logged and every 5 minutes thereafter, as long as the flow is active.

For all other data traffic that doesn't match the selected application/traffic list, the traffic would be loadbalanced across all the available WAN transport links available on the WAN Edge device.

Along with defining the preferred dynamic path selection, AAR policy provides the network administrators with flexibility of defining Site-list's and VPN-list's where the policy needs to be enforced across the SD-WAN overlay network.

## Monitoring and Measuring WAN transport path characteristics

The network path characteristics is measured by running Bi-directional Forward Detection (BFD's) probes periodically on device's each WAN transport tunnel interfaces. The BFD probe measures the transport's loss, latency, jitter every polling intervals.

Following the WAN Edge onboarding – authenticating and joining the overlay network, the device would establish secure data-tunnel to other WAN Edge devices part of the same SD-WAN overlay network. Upon establishing the data-tunnel, the WAN Edge device would:

 probe each WAN transport tunnel with BFD Hello packets at every 1 second interval. Below table lists the BFD default values.

List	Description	Default Values
Hello interval	Interval at which BFD Hello Interval are send across the WAN transport	1000 msec (configurable)
BFD Multiplier	Value defines number of BFD Hello Packet Intervals the device waits before declaring that tunnel has failed.	7 (configurable)

Note: The BFD Hello Interval and BFD Multiplier can be changed per tunnel or across all the WAN transports on the WAN Edge device.

 collect and preserve the packet loss, latency and jitter for every BFD poll and calculate the network path characteristics at each poll interval. The default poll interval value is 10 minutes, implies 600 BFD hello packets are considered for each poll interval calculation.

Poll Interval = poll-interval in secs \* BFD Hello packet interval

• collect 6 poll intervals and average these values to calculate network path liveliness for better accuracy and to dampen any intermittent reclassification (flapping) of the tunnel. At the seventh poll interval, the earliest polling data is discarded to accommodate the latest information.

Below table lists the default values for the Application Aware Routing polling data:

List	Description	Default Values
Poll Interval	Interval at which WAN Edge calculates the average loss, latency and jitter for each WAN transport.	10 minutes (configurable)
Multiplier	Value defines number of poll interval(s) to be considered to calculate the tunnel statistics for the AAR.	6 (configurable)

Note: The Poll Interval and Multiplier values can be modified on the WAN Edge device effecting all the tunnel/WAN transport(s) associated with the device.

Careful consideration must be taken before changing the default values as the BFD packets gets high priority treatment on the WAN Edge device. The BFD packets are marked with high priority DSCP 48 marking. By default, the control traffic and the BFD packets are mapped to Queue 0 on the device and is configured for low-latency queuing, strict-priority traffic queue for control and delay-sensitive traffic. Packets in this queue is

transmitted before any other packets in other queues and for congestion avoidance tail-drop is implemented on Queue 0.

Being aggressive by lowering the BFD values would impact the WAN Edge device performance and being conservative by increasing the BFD values would delay the calculations of the network path resulting in undesired dynamic path selection for the business-critical applications.

#### **Tech tip**

For optimal device performance, Cisco recommends not to change the default BFD values as this might impact WAN Edge performance.

In situation where the default values need to be modified to meet the business requirements, such as to meet the SLA requirements for highly susceptible applications or to reduce bandwidth consumption on the tunnel or to reduce the WAN charges at the remote site. Additional caution and tests must be done before deploying in production environment.

It is always recommended to have a consistent BFD values configured across WAN Edge devices in the same site for the same WAN transport type.

Below table shows examples on the modified values and how quickly the path characteristics are calculated:

	Example 3 (Recommended)	Example 1 (Aggressive)	Example 2 (Moderate)
BFD Hello Interval	1000 msec (Default)	1000 msec (Default)	1000 msec (Default)
Poll Interval	120 sec	30 sec	120 sec
App-route Multiplier	6 intervals (Default)	2 intervals	5 intervals
Path characteristics calculated every	120 sec intervals using last 12 minutes poll data	30 sec intervals using last 1minute poll data	120 sec intervals using 10 minutes poll data

#### Figure 10. Values determining the network path characteristics



#### Policies

Policies are an important part of the Cisco SD-WAN solution and are used to influence the overlay topology and to influence the flow of data traffic across the WAN Edge devices in the overlay network. Policies are applied either at control plane or data plane level, configured in the vManage and enforced either on vSmart controllers or on the WAN Edge devices.

It is to be noted that only one centralized policy can be activated at any time on the vSmart controller. The activated policy can contain several different policy definitions that make up the centralized policy, such as Topology, VPN Membership, Application-Aware Routing policy, Traffic Data (QoS, Service Chaining, Traffic Engineering etc.) and Cflowd policy.

Application Aware Routing policy is part of the centralized policy associated to the vSmart controller. The vSmart controller would distribute the policy through the OMP protocol to the appropriate WAN Edge devices in the overlay network that are part of the selected Site Lists, VPN lists and enforced on the WAN Edge devices for the selected traffic traversing from service-side (LAN network) to the WAN-transport (WAN network).

The WAN Edge device can also be associated with other localized policy. Similar to the centralized policy, only one localized policy can be applied to WAN Edge device. The localized policy can contain several different policies such as prefix-lists, access control list policy, route policy, community-lists, QoS etc.

With multiple policies being configured and enforced on the WAN Edge device, it is important to understand the order of precedence when the packet is moving from service-side to WAN transport-side.

### Figure 11. Policy order of operations on a WAN Edge device.



- Local policy/configuration includes QoS classification, policer and marking
- Centralized application application aware routing policy
- Centralized data policy includes QoS classification, policies, marking and path selection
- Routing/Forwarding
- Scheduling and queuing
- Local policy shaping and ACL includes shaping, re-marking and policer

It is possible for a centralized data policy to overwrite the actions of a centralized application-aware routing policy. Careful consideration must be kept in mind when defining multiple policies for the network as mutually exclusive policies can influence the traffic traversing the WAN Edge device.

# Deploy

This section covers needed steps to

- Verify the prerequisites required before proceeding to deploy Application-Aware routing.
- Procedures involved in deploying centralized policy with Application-Aware routing
- Procedures to append Application-Aware Routing policy to the existing centralized policy.

# Process: Prerequisites for Application-Aware Routing

The below procedure lists the prerequisites that are needed before configuring the Application Aware Routing policies.

### Procedure 1. Verify the WAN Edge device is successfully onboarded in the SD-WAN overlay network.

**Step 1.** In vManage, navigate to **Dashboard > Main Dashboard**, make sure WAN Edge devices are successfully onboarded.

≡	cisco vManage			<b>≜</b> ₿	🔎 🕜 admin 🗸			
86	B DASHBOARD   MAIN DASHBOARD							
□ ✿	1 ↑         11 ↑           vSmart - 1         WAN Edge - 11	1 ↑     VBond - 1	● 1 vManage - 1	Reboot 0	Warning 0 Invalid 11			
عر	Control Status (Total 11)	Site Health (Total 7)		Fransport Interface Distribution				
÷	Control Up 11	Sull WAN Connectivity	4 sites	< 10 Mbps	94			
	Partial 0	9 Partial WAN Connectivity	3 sites	10 Mbps - 100 Mbps 100 Mbps - 500 Mbps	0			
	Control Down 0	8 No WAN Connectivity	0 sites	> 500 Mbps	0			
			U sites	3 View Percent Utilization				

Step 2. In vManage, navigate to Monitor > Network, select the device from the WAN-Edge list.

≡	cisco vManage										٠	ê 🍂	🥑 admin 🕶
	MONITOR   NETWORK												
	WAN - Edge Colocation C	Clusters											
	VPN GROUP	VPN SEC	MENT										
•	Select VPN Group	▼ All se	gments										
٩													000
÷	Device Group All +	Q		Search Options 🗸									Total Rows: 15
**	Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Sir	ice	Device Groups
-	G ENT19-vmanage	11.11.11.21	vManage	24b0ba05-b599-45d9-a00a-3dee8	0	reachable	21	-	12	19.2.099	15 Jar	n 2020 4:34:00 PM PST	"No groups"
ш.	SENT19-vsmart1	15.15.15.25	vSmart	Od6c3bd5-ac18-4dfd-bf33-7cb9e	0	reachable	25		22	19.2.099	15 Jar	n 2020 4:33:00 PM PST	"No groups"
	ENT19-vbond	13.13.13.23	vEdge Cloud (vBo	0a0e0ce1-da1a-4f4d-ac6d-56983	0	reachable	23	-	-	19.2.099	15 Jar	n 2020 4:34:00 PM PST	"No groups"
	🔁 RS01-ISR4431-21	1.1.1.21	ISR4431	ISR4431/K9-F0C2228200S	0	reachable	111	17	3	16.12.02r.0.23	10 Jar	n 2020 5:19:00 PM PST	"No groups"
	8 RS01-ISR4431-22	1.1.1.22	ISR4431	ISR4431/K9-F0C20375PH5	0	reachable	111	16 (17)	3	16.12.02r.0.23	10 Jar	n 2020 5:19:00 PM PST	"No groups"

select System Status from the left panel to view the device status.

≡_	Cisco vManage							<b>▲</b> Ê	📌 🛛 admi	n 🔻
::	MONITOR Network >	System Status								
	Select Device 🔫	RS01-ISR4431-21 1.1.1.21 Site	ID: 111 Device !	fodel: ISR4431 🛛 🕕						
	Applications	🕑 Reboot			3	Â	Crash			
Ŧ	Interface									
ય	TCP Optimization	Module		Hardware Invento	ry		Power Supply			
ŝ	WAN Throughput				_	\$	Fans (Total 3)		PO	
<u></u>	Flows	Temperati	emperature Sensors				RPM:0 RPM:1		0	
	Top Talkers	4 USB					RPM:2		0	
-	WAN									
	TIOC	CPU & Memory						🖡 Real Time 1h 3h	6h 12h 24h 7days Custon	n -
	-		100 %							
	Tunnel									
	Security Monitoring									
	Firewall									
	Intrusion Prevention	0.15%	N 50 %							
	URL Filtering	CPU	Ŭ							
	Advanced Malware Protection									
	Umbrella DNS Re-direct		0							_
	Control Connections	Load average over 24 hrs								
	System Status		100 %							
	Events									
	ACL Logs									
	Troubleshooting	$\square$	y (%)			· · ·				-
	Real Time	62.00%	Memo 20 %							
		Memory								
			0 Fe	18, 12:00 Feb 18, 14:00 Feb 18, 16:00 Feb 18, 18:	00 Feb 18, 2	0:00 Feb 18, 22	2:00 Feb 19, 00:00 Feb 19, 02:00	Feb 19, 04:00 Feb 19, 06	00 Feb 19, 08:00 Feb 19, 10	):00
			0 Fe	18, 12:00 Feb 18, 14:00 Feb 18, 16:00 Feb 18, 18:	00 Feb 18, 2	0:00 Feb 18, 22	2:00 Feb 19, 00:00 Feb 19, 02:00	Feb 19, 04:00 Feb 19, 06	00 Feb 19, 08:00 Feb 19, 10	00

# Procedure 2. Verify the WAN Edge device control connections to all the SD-WAN controllers.

**Step 1.** In vManage, navigate to **Monitor > Network**, select the device from the **WAN-Edge** list and select **Control Connections** option from the left panel.

=	Cisco vManage	e									•	Ê	<u>"</u>	0	
::	MONITOR Network >	<ul> <li>Control Conr</li> </ul>	nections												
	Select Device 👻	RS01-ISR443	31-21   1.1.1.21 Site ID: 111	Device Model: ISR44	31 🕕										
<u> </u>	Applications	vSmart Cont	trol Connections (Expected:	2   Actual: 2 )											
<b>*</b>	Interface					<b>a</b>			3						
4	TCP Optimization	Optimization													
ŝ	WAN Throughput					mpls	)		public- internet						
*	Flows					T									
	Top Talkers														
	WAN					vSmart 1/1 vN	lanage 1/1		vSmart 1/1						
	TLOC														
	Tunnel														98
	Security Monitoring	Q		Se	earch Options 🗸						Total Rows: 3				
	Firewall	Y Pee	г Туре	Peer System IP		Peer Protocol	Private Port		Public Port	Controller Gr	oup ID	La	st Updated		
	Intrusion Prevention	✓ mpl	S			-									
		vma	anage	11.11.11.21		dtls	12446	1	12446	0		08	Feb 2020 9	40:09 AM F	ST
	URL Filtering	vsm	nart	15.15.15.25		dtls	12446	1	12446	0		09	Feb 2020 9	40:41 AM F	ST
	Advanced Malware	✓ publ	lic-internet						-						
CISCO VMANAGE MONITOR Network CA Select Device CA Applications VS Interface TCP Optimization WAN Throughput Flows Top Talkers WAN TLOC Tunnel Security Monitoring Firewall Intrusion Prevention URL Filtering Advanced Malware Protection Umbrela DNS Re-direct	vsm	nart	15.15.15.25		dtls	12446	1	12446	0		16	Feb 2020 9	:44:39 PM P	ST	
	Umbrella DNS Re-direct								▲ A Amin → A Amin → Amin → Amin → Amin → Amin → A						
	Control Connections														

# Procedure 3. Verify the WAN Edge device IPSec connections to other WAN Edge devices.

**Step 1.** In vManage, navigate to **Monitor > Network**, select the device from the **WAN-Edge** list and select **WAN > Tunnel** option from the left panel.

≡	Cisco vManage								۵	Ê	<b>*</b> @ @	adm
	MONITOR Network >	WAN - Tunnel										
	Select Device 👻	RS01-ISR4431-21   1.1.1.21 Site ID: 111 Device Model: ISR4431 (	)									
	Applications	🖪 Chart Options 👻							🔻 Real T	ime 1h 3h 6h	12h 24h 7days	Custom
¢	Interface	1%								Legend		
۹.	TCP Optimization	0.75 %								RS0 ISR4	1-ISR4431-21:mpls-R 4331-18:mpls[IPSEC]	S02-
<b>e</b>	WAN Throughput	11499 4 5 7 10								RS0 ISR	1-ISR4431-21:mpls-R 4331-19:mpls[IPSEC]	.S02-
	Flows	9 0.5 %								RS0	1-ISR4431-21:mpls-R 1001X-04:mpls/IPSE0	:S05- Cl
11	Top Talkers	0.25 %								RSO	11-ISR4431-21:mpls-R	S05-
	WAN									RSO	1-ISR4431-21:mpls-R	S06-
	TLOC									RS0	1-ISR4431-21:mpls-R	S21-
	Tunnel									vEd	ge1000-33:mpls[IPSE	.C]
	Security Monitoring	/ Rate										
	Firewall	ecovery										
	Intrusion Prevention	Loss R										
	URL Filtering	FEC										
	Advanced Malware Protection	Feb 18, 12:00 Feb 18, 14:00 Feb 18, 16:00 Feb 18,	18:00 Feb 18, 20:00	Feb 18, 22	:00 Feb 19, 00	:00 Feb 19, 0	2:00 Feb 19, 04:00 Fe	b 19, 06:00 Feb 1	19, 08:00 Feb 1	9, 10:00		
	Umbrella DNS Re-direct	6 Rows Selected									0	-
	Control Connections	Q. Searc	h Options 🗸								Total Rows:	a: 17
	System Status	↓ Down (0) () Init (0) ↑ Up (17)										
	Events	Y Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	FEC Loss Recovery (%)	Latency (ms)	QoE Score	Total Tx Bytes	Total Rx Bytes	
	ACL Logs	✓ mpls										
	Troubleshooting	RS01-ISR4431-21:mpls-RS02-ISR4331-18:mpls	IPSEC	1	0.00	0.00	N/A	0.00	10.00	0 B	52.58 KB	
	requires noting	RS01-ISR4431-21:mpls-RS02-ISR4331-19:mpls	IPSEC	1	0.00	0.00	N/A	0.00	10.00	0 B	4.04 KB	
	Real Time	RS01-ISR4431-21:mpls-RS05-ASR1001X-05:mpls	IPSEC	<b>↑</b>	0.00	0.00	N/A	0.00	10.00	0 B	38.01 KB	
		RS01-ISR4431-21:mpls-RS06-ASR1001HX-03:mpls	IPSEC	1	0.00	0.00	N/A	0.00	10.00	0 B	28.89 KB	
		RS01-ISR4431-21:mpls-RS05-ASR1001X-04:mpls	IPSEC	$\uparrow$	0.00	0.00	N/A	0.00	10.00	0 B	21.13 KB	
		RS01-ISR4431-21:mpls-RS21-vEdge1000-33:mpls	IPSEC	1	0.00	0.00	N/A	0.00	10.00	0 B	2.99 KB	
		RS01-ISR4431-21:mpls-RS23-vEdge2000-29:mpls	IPSEC	1	0.00	0.00	N/A	0.00	10.00	0 B	4.73 KB	

**Procedure 4.** Verify the BFD sessions are established between WAN Edge devices.

**Step 1.** In vManage, navigate to **Monitor > Network**, select the device from the **WAN-Edge** list and select **Real Time** option from the left panel. Search for **BFD sessions** option in the **Device Options** search bar.

	cisco vManage									• E	a 👘	Ø	admin 👻
	MONITOR Network >	Real Time											
h	Select Device 🔹	RS01-ISR4431-21   1.	.1.1.21 Site ID: 111 Device Mode	l: ISR4431 🕕									
	Applications												
Ŀ	Interface	Device Options:	Q BFD Sessions										~
Ŀ		〒 Filter ▼											<b>O</b>
	TCP Optimization	Q		Search Optio	ns 🗸							To	tal Rows: 17
	WAN Throughput	System IP↑	Last Updated	Site ID	State	Source TLOC Color	Remote TLOC Color	Source IP	Destination Public IP	Destination I	Public Port	Enca	sulation
	Flows	2.2.2.18	19 Feb 2020 12:03:48 PM PST	222	up	mpls	mpls	10.5.208.42	10.5.208.34	12346		ipsec	
	Ten Tellione	2.2.2.18	19 Feb 2020 12:03:48 PM PST	222	up	public-internet	public-internet	10.105.207.45	10.5.207.34	12346		ipsec	
	Top Talkers	2.2.2.19	19 Feb 2020 12:03:48 PM PST	222	up	mpls	mpls	10.5.208.42	10.5.208.38	12366		ipsec	
	WAN	2.2.2.19	19 Feb 2020 12:03:48 PM PST	222	up	public-internet	public-internet	10.105.207.45	10.5.207.38	12366		ipsec	
	TLOC	3.3.3.15	19 Feb 2020 12:03:48 PM PST	333	up	public-internet	public-internet	10.105.207.45	10.5.207.26	12426		ipsec	
	Turnel	5.5.5.4	19 Feb 2020 12:03:48 PM PST	555	up	mpls	mpls	10.5.208.42	10.5.208.10	12346		ipsec	
-	Tunner	5.5.5.4	19 Feb 2020 12:03:48 PM PST	555	up	public-internet	public-internet	10.105.207.45	10.5.207.10	12346		ipsec	
	Security Monitoring	5.5.5.5	19 Feb 2020 12:03:48 PM PST	555	up	mpls	mpls	10.5.208.42	10.5.208.14	12346		ipsec	
	Firewall	5.5.5.5	19 Feb 2020 12:03:48 PM PST	555	up	public-internet	public-internet	10.105.207.45	10.5.207.14	12346		ipsec	
	Interview Dressentian	6.6.6.3	19 Feb 2020 12:03:48 PM PST	666	up	mpls	mpls	10.5.208.42	10.5.208.6	12346		ipsec	
	Intrusion Prevention	6.6.6.3	19 Feb 2020 12:03:48 PM PST	666	up	public-internet	public-internet	10.105.207.45	10.5.207.6	12346		ipsec	
	URL Filtering	21.21.21.33	19 Feb 2020 12:03:48 PM PST	21	up	mpls	mpls	10.5.208.42	10.5.208.58	12346		ipsec	
	Advanced Malware	21.21.21.33	19 Feb 2020 12:03:48 PM PST	21	up	public-internet	public-internet	10.105.207.45	10.105.207.102	12366		ipsec	
	Protection	21.21.21.34	19 Feb 2020 12:03:48 PM PST	21	up	mpls	mpls	10.5.208.42	10.105.208.58	12346		ipsec	
	Umbrella DNS Re-direct	21.21.21.34	19 Feb 2020 12:03:48 PM PST	21	up	public-internet	public-internet	10.105.207.45	10.5.207.102	12366		ipsec	
E	Control Connections	23.23.23.29	19 Feb 2020 12:03:48 PM PST	23	up	mpls	mpls	10.5.208.42	10.5.208.66	12346		ipsec	
	control connections	23.23.23.29	19 Feb 2020 12:03:48 PM PST	23	up	public-internet	public-internet	10.105.207.45	10.5.207.110	12346		ipsec	
	System Status												
	Events												
	ACL Logs												
	Troubleshooting												
Γ	Real Time												
-													

### **Procedure 5.** Verify the SD-WAN vSmart controller is in vManage mode.

**Step 1.** In vManage, navigate to **Configuration > Devices**, select the **Controllers** options to verify the vSmart mode.

≡	Cisco vMa	nage								٠	ê	<b>*</b> @	0	admin 🔻
::	CONFIGURATIO	N   DEVICES												
	WAN Edge List	Controllers												
*	Add Controller	✓ [] Change Mode ✓											٢	99
a	Q		Search Options 🗸										Tot	al Rows: 3
Ì	Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Status	Policy Name	Policy Versio	in	UUID		
<b>\$</b>	vManage	ENT19-vmanage	11.11.11.21	21	CLI		In Sync	Installed	-	-		24b0ba05	5-b599-45d9	
	vSmart	ENT19-vsmart1	15.15.15.25	25	vManage	ENT19-vsmart1	In Sync	Installed	-	-		0d6c3bd5	5-ac18-4dfd	
	vBond	ENT19-vbond	13.13.13.23	23	CLI	-	In Sync	Installed	-	-		0a0e0ce1	-da1a-4f4d	
11														

# Process: (Optional) Configuring custom BFD template

This process walks through procedure and steps needed to configure custom BFD template for the SD-WAN environment.

# Procedure 1. (optional) Create custom BFD Template

Following the WAN Edge onboarding, the device establishes secure IPSec data tunnels with other WAN Edge devices and periodically probes the secure tunnels, with BFD Hello packets, to measure the transport tunnel liveliness and path characteristics.

Below table lists the default values for the BFD polling data defined globally for all tunnel on the WAN Edge device:

List	Description	Default Values
Hello interval	Interval at which BFD Hello Interval are send across the WAN transport	1000 msec (configurable)
BFD Multiplier	Value defines number of BFD Hello Packet Intervals the device waits before declaring that tunnel has failed.	7 (configurable)

and the default values used to calculate the network path characteristics:

List	Description	Default Values
Poll Interval	Interval at which WAN Edge calculates the average loss, latency and jitter for each WAN transport.	10 minutes (configurable)
Multiplier	Value defines number of poll interval(s) to be considered to calculate the tunnel statistics for the AAR.	6 (configurable)

The above default value can be changed either effecting all the tunnels on the WAN Edge device or on each tunnel basis on the WAN Edge device. Careful consideration must be taken when changing the BFD values as this may cause adverse effect on the performance of the WAN Edge device.

Below procedure walks through steps on the procedure to change the default BFD values.

Step 1. Create BFD template for the WAN Edge device(s) in the SD-WAN network.

In vManage, navigate to **Configuration > Templates > Feature** and click **Add Template**. Select all the appropriate devices deployed in the SD-WAN network from the **Select Devices** list and choose **BFD** template from the **Basic Information** category.

≡	cisco vManage				•	ê	<b>*</b> ®	0	admin 🔻
::	CONFIGURATION   TEMPLATES								
ᅟᅟ	Device Feature								
۰	Feature Template > Add Template								
عر	Select Devices	Select Template							
÷	Search by device name	BASIC INFORMATION							
	ASR1001-HX			_					
•••	ASR1001-X	AAA-CISCO	BFD		Glob	al Setting	S		
	ASR1002-HX								
	ASR1002-X	NTP	OMP		S	Security			
	C1101-4P								
	C1101-4PLTEP	System							

Step 2. Create custom BFD template for the SD-WAN network.

Input the **Template Name** and **Description** for the template and modify the **Multiplier** and **Poll Interval** under **Basic configuration** section. The modified values in the section would influence all the associated tunnels on the WAN Edge device.

Alternatively, to influence values on the tunnel/color basis, select the **New Color** from the **Color** section, choose the appropriate **Color** from the drop-down menu option and modify the **Hello Interval** and **Multiplier** values. Click **Add** in the Color section and **Save** at the bottom of the page to save the BFD feature template.

ullullu Cicco yManago							A <b>R</b> A	• • • • • • • •
	TEO					• •	Ť.	g admin
Device Feature	1123							
Feature Template > Add Templat	e > BFD							
Device Type	ASR1001-HX,ASR1001-X,ASR1002-HX,A	SR1002-X,ISR4331,ISR4431						
Template Name	Edge_Custom_BFD_Template							
Description	Edge_Custom_BFD_Template							
Basic Configuration	Color							
BASIC CONFIGURATION	l							
Multiplier	c	<b>6</b>						
Poll Interval (milliseconds		600000						
COLOR								
COLOR								
New Color								
						[	Mark as Option	al Row 🕕
Color	•	🕽 👻 – Choose – 🔍 👻	Required					
Hallo Interval (millisaco	nde)	1000						
neno interval (miniseco	ius)							
Multiplier	e	7						
Path MTU Discovery	٩	• On Off						
							Add	Cancel
Ontional		Hello Interval		Multiplier	 Path MTH			Action
	: Internet	✓ 1000		<ul> <li>7</li> </ul>	⊘ On			
				·				
			Save Cano	e1				

**Step 3.** Associate the custom BFD template to the WAN Edge device(s).

In vManage, navigate to vManage > Configuration > Templates > Device, select the devices from the device list and click the three dots (...), located at the end of each table row and choose the Edit option from the drop-down options

	Cisco vManage							<b>▲</b> É	ı 🍂	admin 🗸
: [	CONFIGURATION   TEMPLA	TES								
- I	Device Feature									
	Create Template ▼									0
	۹	S	earch Options 🗸							Total Rows: 15
`	Name↓	Description	Туре	Device Model	Feature Templates	Devices Attached	Updated By	Last Updated	Template St	atus
	RS23-vEdge2000-29	RS23-vEdge2000-29	Feature	vEdge 2000	15	1	admin	24 Jan 2020 6:19:33 P	In Sync	
	RS22-vEdge5000-31	RS22-vEdge5000-31	Feature	vEdge 5000	15	1	admin	24 Jan 2020 6:18:10 P	In Sync	
	RS21-vEdge1000-34	RS21-vEdge1000-34	Feature	vEdge 1000	17	1	admin	24 Jan 2020 5:42:44 P	In Sync	
	RS21-vEdge1000-33	RS21-vEdge1000-33	Feature	vEdge 1000	15	1	admin	21 Jan 2020 6:36:12 P	In Sync	
	RS06-ASR1001HX-03	RS06-ASR1001HX-03	Feature	ASR1001-HX	13	1	admin	17 Jan 2020 6:57:27 P	In Sync	
	RS05-ASR1002X-02	RS05-ASR1002X-02	Feature	ASR1002-X	13	1	admin	17 Jan 2020 7:09:23 P	In Sync	
	RS05-ASR1001X-05	RS05-ASR1001X-05	Feature	ASR1001-X	13	1	admin	17 Jan 2020 6:28:53 P	In Sync	Edit
	RS05-ASR1001X-04	RS05-ASR1001X-04	Feature	ASR1001-X	13	1	admin	17 Jan 2020 6:29:54 P	In Sync	View
	RS03-C1116P-16	RS03-C1116P-16	Feature	C1116-4P	10	1	admin	17 Jan 2020 11:38:30 A	In Sync	Delete
	RS03-C1116P-15	RS03-C1116P-15	Feature	C1116-4P	11	1	admin	17 Jan 2020 12:23:25 P	In Sync	Copy Attach Devices
	RS02-ISR4331-19	RS02-ISR4331-19	Feature	ISR4331	15	1	admin	24 Jan 2020 5:35:46 P	In Sync	Detach Devices
	RS02-ISR4331-18	RS02-ISR4331-18	Feature	ISR4331	13	1	admin	17 Jan 2020 10:52:06 A	In Sync	Export CSV
	RS01-ISR4431-22	RS01-ISR4431-22	Feature	ISR4431	17	1	admin	24 Jan 2020 5:29:01 P	In Sync	Change Device Values
	RS01-ISR4431-21	RS01-ISR4431-21	Feature	ISR4431	17	1	admin	24 Jan 2020 5:23:44 P	In Sync	
	ENT19-vsmart1	ENT19-vsmart1	Feature	vSmart	10	1	admin	28 Jan 2020 11:50:38 A	In Sync	

navigate to the **Basic Information > BFD** section and choose the previously created custom BFD template and click **Update**.

≡	cisco vManage							•	ê	<b>"</b> 2	0	
::	CONFIGURATION   TEMPLA	TES										
	Device Feature											
*	Description	RS01-ISR4431-21										
•	Basic Information	Transport & Management VPN	Service VPN	Cellular	Additional Templa	ites						
*		Transport & management + H		oonalai	Automai Tempie							
2	Basic Information											
*	System *	1_Template_System	•				Additional Sy	stem Te	mplates			
	Logging*	Factory Default Logging Template	•				NTP					
	NTP	0_Tempalte_VPN0_NTP	•									
	AAA	Choose	•	BFD *		Factory_Default_BFD_Template	•					
	AAA-CISCO	Factory Default AAA CISCO Template	Ŧ	OMP *		Edge_Custom_BFD_Template	Edge_Custom	_BFD_Templa	ite			
		·										
	Security *	Factory_Default_vEdge_Security_Templat	te									
	Transport & Manageme	ent VPN				Create Template	View Template					
	VDN 0.+	· · · · · · · · · ·	¥				A deltation of M/P	NI 0 T				
				Update	Cancel							

**Step 4.** Click **Next**, **Configure Devices** to configure the WAN Edge(s) with custom BFD template.

≡	ahaha cisco	' Cisco vManage						٠	ê 4	🧐 💡	admin 🔻
::	<b>\$</b> co	ONFIGURATION   TEMPLATES									
	Device	e Template   RS01-ISR44	131-21								
-											00
	0		Courth Onting								Total Rows: 1
٩,	Q		Search Option	15 🗸							
<b>.</b>		Chassis Number	System IP	Hostname	Interface Name(vpn10_intf_name	) IPv4 Address(vp	n10_intf_ipv4_address)	Interface Na	ame(vpn512_intf_	name)	IPv
-	0	ISR4431/K9-F0C2228200S	1.1.1.21	RS01-ISR4431-21	loopback10	10.1.1.21/32		GigabitEther	net0		21.2 •••
*											
-											
8											
					Next Cancel						
≡	cisco	' Cisco vManage						•		🥙 🕐	admin 🔻
	🖨 ТА	SK VIEW									
	Push I	Feature Template Configuration	🖉 Validation Success 👻						Initiated By:	admin Fror	n: 100.119.42.102
~	Total	Task: 1   Success : 1									
*											00
٩,											
÷	Q		Search Optio	ins 🗸							Total Rows: 1
	>	Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID		vManage IP	
~	>	Success	Done - Push Feature Templa.	. ISR4431/K9-FOC2228200S	ISR4431	RS01-ISR4431-21	1.1.1.21	111		11.11.11.21	

# Process: Configuring Application-Aware Routing policy

Creating Application Aware Routing policies consists of defining the three core components:

- Identification Classify the traffic / Application group of interest.
- Application SLA Requirement Defining the application SLA requirements.

 Application-Aware Routing Policy – Policy maps the classified traffic to the transport tunnel based on the defined SLA requirement.

On creating the policy, associate and activate the centralized policy to appropriate Site list(s) and VPN list(s).

#### **Procedure 1.** Identification - Classify the traffic / Application group of interest.

Below steps walks through steps for classifying the traffic class of interest for the preferred treatment in the SD-WAN environment.

Step 1. In vManage, navigate to Configuration > Policies > Centralized Policy and select Add Policy.

≡	disco vManage	•	ê	۵	0	admin 👻
55					Custom	Options 👻
	Centralized Policy Localized Policy					
٠	O Add Policy					0
a	Q Search Optione v				Т	otal Rows: 1

Step 2. Select Application from the left panel and click New Application List

≡	cisco vManage						•	â (	<u>(</u>	0	admin 🔻
	CONFIGURATION   POLICI	ES Centralized Policy > Add Policy									
▫		O Create Groups of Ir	terest O Configure Topolo	ogy and VPN Membership C	Configure Traffic Rules	Apply Policies to Sites and					
٠	Select a list type on the left and	start creating your groups of interest									
عر	Application	New Application List									
	Color										
-	Data Prefix	Name	Entries	Reference Count	Updated By	Last Updated		Action			
<b></b> .		Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PS	Т				
678	Policer	Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PS	т				
-	Prefix										
	Site										
	SLA Class										
	TLOC										
	VPN										
				Next CANCEL							

name the custom application list and select either Application or Application Family option.

Choose appropriate application family category option from the drop-down option and Click Add.

≡	cisco vManage						•	â (	0	0	admin 🔻
8	CONFIGURATION   POLICIE	S Centralized Policy > Add Policy									
▣		<ul> <li>Create Groups o</li> </ul>	f Interest O Configure Topo		O Configure Traffic Rules	Apply Policies to Sites and V					
۵	Select a list type on the left and s	tart creating your groups of interest									
عر	Application										
÷	Color	Application List Name									
	Data Prefix	Audio_Video_Application_List									
_	Policer	Application     Application File	amily								
ш	Prefix	Audio/Video ×								Ť	
	Site										
	SLA Class								dd	Cancel	
	TLOC										
	VDN	Name	Entries	Reference Count	Updated By	Last Updated	Ac	tion			
	¥1.18	Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PST	/	Ē			
		Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PST	/				
											_

	abab									
≡ _	cisco Cisco vManage					•	Ê	<b>*</b>	0	admin 🔻
::	CONFIGURATION   POLICI	ES Centralized Policy > Add Policy								
		<ul> <li>Create Groups o</li> </ul>	f Interest O Configure Topo	ology and VPN Membership (	Configure Traffic Rules (	<ul> <li>Apply Policies to Sites and VPNs</li> </ul>				
۰	Select a list type on the left and s	start creating your groups of interest								
عر	Application	New Application List								
÷	Color	Name	Entries	Pafarance Count	Lindated By	Last Indated	Action			- 1
*	Data Prefix	Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PST				- II
_	Policer	Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PST	× 0 =			
	Prefix	Audio_Video_Application_List	audio-video	0	admin	20 Feb 2020 12:59:23 PM PST	/0=			
	Site									
	SLA Class									
	TLOC									
	VPN									
				Next CANCEL						

**Step 3.** Alternatively, to previous **Step 2**, network administrators can match on **Data Prefix** to identify traffic based of the network traffic.

To define the data prefix, select the **Data Prefix** option from the list type on the left side panel and click **New Data Prefix List** 

≡	Cisco vManage						•	Ê	<b>"</b> @	Ø	admin 👻
	CONFIGURATION   POLIC	CIES Centralized Policy > Ad	ld Policy								
▫		<ul> <li>Create Grou</li> </ul>	ups of Interest O Configure Topology		— 💿 Configure Traffic Ru	iles O Apply Pc					
٠	Select a list type on the left and	d start creating your groups of i	nterest								
٩	Application	ᅌ New Data Prefix List									
÷	Color		<b>7</b>	Internet Broto and	Defense Origi	Hadred Dr.	Local Herdeneral		Antina		_
	Data Prefix	Name	Entries	Internet Protocol	Reference Count	Opdated By	Last Opdated		Action		
	Policer										
	Prefix			No da	ta availab	le					
	Site										
	SLA Class										
	TLOC										
	VPN										
				Next CAN	ICEL						

Input the **Data Prefix List Name** and select either **IPv4 / IPv6** from the **Internet Protocol** option and add the network prefix that needs to be matched and select **Add** 

	cisco Cisco vManage							•	<b>.</b>	Ø	admin 🔻	
::	CONFIGURATION   POLIC	IES Centralized Policy > Add Poli	icy									
▣		<ul> <li>Create Groups of</li> </ul>	Interest	– 🧿 Configure Topology		—— 🧿 Configure Tra	ffic Rules — 💽					
٠	Select a list type on the left and	start creating your groups of interes	st									
٩	Application	🕂 New Data Prefix List										
÷	Color	Data Prefix List Name										
*	Data Prefix	Custom_DataPrefix_List1										
-	Policer	Internet Protocol										
۵	Prefix	IPv4 IPv6										
	Site	Add Data Prefix										
	SLA Class	10.4.208.0/24										
	TLOC								Add	Cancel		
	VPN											
		Name Ent	tries		Internet Protocol	Reference Count	Updated By	Last Updated	Action			
					Next	CANCEL						

cisco VManag	ge					<b>▲</b> Ê	<b>1</b>	admii
	POLICIES Centralized Policy > Add	Policy						
	<ul> <li>Create Group</li> </ul>	os of Interest O Co		p ——— 🧿 Configure Tr	affic Rules — 🧿			
Select a list type on the le	eft and start creating your groups of in	terest						
Application	New Data Prefix List							
Color		Patrice	Internet Brotonal	Deferring Count	Hedeted Du	Local Mediatori	Action	
Data Prefix	Custom_DataPrefix_List1	10.4.208.0/24	IPv4	Reference Count	admin	20 Feb 2020 1:26:09 PM PST	Action	
Policer								
Prefix								
Site								
SLA Class								
TLOC								
VPN								

**Step 4.** Repeat the above steps to add any additional Application List and/or Data Traffic for the SD-WAN deployment.

## **Procedure 2.** Define Application Service Level requirements.

Below steps walks through steps on defying custom SLA class. But, before defining the custom SLA, it is important to understand the current historical WAN Transport health characteristics.

**Step 1.** Monitor transports health characteristics across the SD-WAN environment.

To view the tunnel characteristics across the SD-WAN infrastructure. Navigate to **vManage** > **Dashboard** > **Main Dashboard** > **Transport Health** widget.

≡	Cisco vManage				•	ê 🍂	9	admin 👻
::	Dashboard SHBOAR	RD						
▣	Main Dashboard	11 1	1 1	<u> </u>	Reboot	0	Warning	0
\$	VPN Dashboard	WAN Edge - 11	vBond - 1	vManag	je - 1 Last 24 hrs	0	4 e invalid	
٩	Security		Site Health (Total 7)		Transport Interface Dist	tribution		
ĉ	Control Up	11	S Full WAN Connectivity	4 sites	< 10 Mbps			94
*	Protect				10 Mbps - 100 Mbps			0
	Partial	0	Partial WAN Connectivity	3 sites	100 Mbps - 500 Mbps			0
11.	Control Down	0	8 No WAN Connectivity	0 sites	> 500 Mbps			0
					Vie	ew Percent Utiliz	ation	
	WAN Edge Inventory		WAN Edge Health (Total 11)		Transport Health		Type: By Loss	\$ ₹ 🖸
	Total	14	$\frown$		100 %			
	Authorized	14		0				
	Deployed	11			50 %			
	Staging	0	Normal Warning	Error		******	-	

**Step 2.** Expand the widget by clicking the **square icon** in the top right corner of the Transport Health widget and select the **Type** option to view the chart **By Loss, By Latency or by Jitter** values and view the transport health over the maximum of past 7 days.



**Step 3.** Select **SLA Class** from the left panel, in the **Configuration > Policies > Centralized Policy** page, to create additional SLA Class list. By default, vManage has 4 pre-defined SLA class (Transactional-Data, Bulk-Data, Voice-And-Video and Default).

In case the pre-defined SLA class does not fit the deployment requirements, Click New SLA Class List to add additional list

≡	Cisco vManage							<b>▲</b> ₿	¥@	0	admin 🔫
-	CONFIGURATION   POLICI	ES Centralized Policy > Add Po	licy								
묘		0	Create Groups of Interest	— O Configure Topology and	I VPN Membership ——— G	Configure Traffic Rules	— O Apply Policies to Sites				
٠	Select a list type on the left and	start creating your groups of intere	est								
٩	Application	● New SLA Class List									
÷	000	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action		
<u></u>	Data Prefix	Transactional-Data	5	50	100	0	system	15 Jan 2020 4:37:53 PM PST	10=		
_	Policer	Bulk-Data	10	300	100	0	system	15 Jan 2020 4:37:53 PM PST	10=		
	Prefix	Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:37:54 PM PST	∕0≡		
	Site	Default	25	300	100	0	system	15 Jan 2020 4:37:55 PM PST	101		
	SLA Class										
	TLOC										
	VPN										
					Next CANCEL						

Input the **SLA Class List Name** and **Loss**, **Latency**, **Jitter** value requirement for the application family and click Add.

≡	cisco VManage							▲ Ê	<b>A</b>	0	admin 👻
5	CONFIGURATION   POLICIE	ES Centralized Policy > Add Po	licy								
▫		0	Create Groups of Interest	— O Configure Topology and		O Configure Traffic Rules —	O Apply Policies to Site				
٠	Select a list type on the left and s	start creating your groups of inter	est								
٩	Application	New SLA Class List									
÷	Color	SLA Class List Name									
	Data Prefix	Custom_SLA_Class_1									
_	Policer	Loss (%)		Latency (m	ns)		Jitter (ms)				
	Prefix	5		70			100				
	Site								Add	Cancel	
	SLA Class										- 1
	TLOC	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action		
		Transactional-Data	5	50	100	0	system	15 Jan 2020 4:37:53 PM PST	<ul> <li>0</li> </ul>		
	VPN	Bulk-Data	10	300	100	0	system	15 Jan 2020 4:37:53 PM PST	<ul> <li></li> <li><th></th><th></th></li></ul>		
		Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:37:54 PM PST	<ul> <li>C =</li> </ul>		
					Next CANCEL						

Step 4. Repeat the previous step to create any additional SLA Class needed

12 X								▲ Ê	🔎 🕜 ai	dmin 🔻
	CONFIGURATION   POLICIE	S Centralized Policy > Add Pol	icy							
D		0	Create Groups of Interest	— O Configure Topology and	d VPN Membership ——— 🕻	Configure Traffic Rules —	Apply Policies to Site:			
🌣 s	Select a list type on the left and st	tart creating your groups of intere	st							
2	Application	➔ New SLA Class List								
~	Color									
-	Data Profix	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action	
*	Data Pielix	Transactional-Data	5	50	100	0	system	15 Jan 2020 4:37:53 PM PST	2 0 ■	
_	Policer	Bulk-Data	10	300	100	0	system	15 Jan 2020 4:37:53 PM PST	101	
	Prefix	Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:37:54 PM PST	201	
		Default	25	300	100	0	system	15 Jan 2020 4:37:55 PM PST	10	
	Site	Custom_SLA_Class_1	5	70	100	0	admin	20 Feb 2020 3:55:09 PM PST	/01	
	SLA Class									
	TLOC									
	VPN									
					Next CANCEL					

#### **Tech tip**

Note that any number of SLA Class can be created, but only 4 SLA class can be associated to the Application Aware Routing policy. Please refer to the Software Release Notes for the latest supported number of SLAs for the version in use.

## Procedure 3. Create Site List

The Site list defines all the sites in the SD-WAN environment. This site-list would be used in the Application-Aware Routing policy to enforce the policy, influencing WAN Edge devices part of the selected site(s).

Step 1. To create Site List, select Site from the left panel and create Site list by clicking New Site List

=	cisco vManage					•	ê 🍂	9	admin 🔻
s [	CONFIGURATION   POLIC	CIES Centralized Policy > Ad	ld Policy						
		Create Greate	oups of Interest O Conf		— O Configure Traffic Rules —	— O Apply Policies to Sites and			
۰	Select a list type on the left and	d start creating your groups of i	interest						
عر	Application	• New Site List							
÷	Color	Namo	Entring	Peference Count	Indated Ry	Last Updated	Action		
<u></u>	Data Prefix	Name	Liules	Reference count	opuated by	Last opuated	Action		
11.	Policer			N.a. da					
	Prefix			No da	ta avallable				
	Site								
	SLA Class								
	TLOC								
	VPN								
				Next CAI	NCEL				

Input the Site List Name and Add Site. click Add.

≡	cisco vManage						•	Ê	<b>"</b> 22	0	admin 👻
::	CONFIGURATION   POLIC	CIES Centralized Policy > Add Policy									
▫		<ul> <li>Create Groups of Inte</li> </ul>	erest O Configure Topolo		O Configure Traffic Rules	Apply Policies to Site					
٠	Select a list type on the left and	start creating your groups of interest									
عر	Application	New Site List									
÷	Color	Site List Name									
	Data Prefix	Site_222									
	Policer	Add Site									
11	Prefix	222									
	Site							1	Add	Canc	el
	SLA Class										
	TLOC										
	VPN	Name	Entries	Reference Count	Updated By	Last Updated		Action			
				Next CANC	EL						

Step 2. Repeat above step to add additional sites

	Cisco vManage					•	ê 🍂 ê	② admin ◄
::	CONFIGURATION   POLI	CIES Centralized Policy > /	Add Policy					
▣		Create C	Groups of Interest O Con		— O Configure Traffic Rules	Apply Policies to Sites and VPNs		
٠	Select a list type on the left an	d start creating your groups o	of interest					
عر	Application	New Site List						
÷	Color	Name	Entries	Reference Count	Updated By	Last Updated	Action	
*	Data Prefix	Site_222	222	0	admin	21 Feb 2020 9:25:28 AM PST	101	
_	Policer	Site_23	23	0	admin	21 Feb 2020 9:26:20 AM PST	< D #	
۵	Prefix							
	Site							
	SLA Class							
	TLOC							
	VPN							
				Next CA	NCEL			
Dro	ocedure 4	Create VPN	list					

The VPN list defines the service VPN deployed in the SD-WAN environment. This VPN-list would be used in the Application-Aware Routing policy to enforce the policy, influencing WAN Edge devices that are associated with the selected VPN.

≡	cisco vManage					•	Ê	<b>≜</b> ®	0	admin 👻
::	CONFIGURATION   POLIC	CIES Centralized Policy > Add Polic	су							
▫		<ul> <li>Create Groups or</li> </ul>	of Interest 📃 💿 Configu		O Configure Traffic Rules —	Apply Policies to Sites and V				
٠	Select a list type on the left and	d start creating your groups of interes	t							
عر	Application	• New VPN List								
÷	Color									
	Data Prefix	Name	Entries	Reference Count	Updated By	Last Updated	A	lotion		
<u> </u>	Policer									
8	Prefix			No data	a available					
	Site									
	SLA Class									
	TLOC									
	VPN									
				Next CANCE	L					

Step 1. To create VPN List, select VPN from the left panel and click New VPN List

## Input the VPN List Name and Add VPN. click Add.

≡	cisco VManage					•	ê 🍂 ê	Ø	admin 🔻
::		CIES Centralized Policy > Add Policy							
		• Create Groups of Intere	st 💿 Configure		Configure Traffic Rules	Apply Policies to Sites and VPNs			
۵	Select a list type on the left and	I start creating your groups of interest							
عر	Application	New VPN List							
ô	Color	VPN List Name							
	Data Prefix	VPN_10							
_	Policer	Add VPN							
	Prefix	10							
	Site						Add	Canc	el
	SLA Class								
	TLOC								
	VPN	Name	Entries	Reference Count	Updated By	Last Updated	Action		
				Next C/	ANCEL				



=	cisco Cisco vManage					<b>€</b>	l 🔎	0	admin 🔻
5	CONFIGURATION   POLIC	IES Centralized Policy > Add Policy							
□		<ul> <li>Create Groups of Int</li> </ul>	erest O Configure Topolog	gy and VPN Membership 🧿	Configure Traffic Rules	Apply Policies to Sites and VPNs			
٠	Select a list type on the left and	start creating your groups of interest							
عر	Application								
<u>~</u>	Color								_
_	Data Prefix	Name	Entries	Reference Count	Updated By	Last Updated	Action		
*		VPN_10	10	0	admin	21 Feb 2020 9:46:45 AM PST	/01		
678	Policer								
-	Prefix								
	Site								
	SLA Class								
	TLOC								
	VPN								
				Next CANCEL					

# Procedure 5. Configuring Application-Aware Routing policy

This procedure walks through steps to create Application-Aware Routing policy.

**Step 1.** Click **Next** twice to navigate the Centralized Policy wizard to **Configure Traffic Rules** and select the **Application Aware Routing** tab.

cisco VMan	nage						<b>▲</b> Ê	🔎 🕢 adr
CONFIGURATION	POLICIES Centralized Policy > Ac	dd Policy						
		Oreate Groups of Interest	O Configure Topo		Configure Traffic Rule	es ——— 💿 Apply Polici		
Select a list type on the	e left and start creating your groups of i	interest						
Application	<ul> <li>New SLA Class List</li> </ul>							
Color								
Data Prefix	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action
Policor	Transactional-Data	5	50	100	0	system	15 Jan 2020 4:37:53 PM PST	
Policer	Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:37:54 PM PST	/0=
Pretix	Default	25	300	100	0	system	15 Jan 2020 4:37:55 PM PST	101
Site	Custom_SLA_Class_1	5	70	100	0	admin	20 Feb 2020 3:55:09 PM PST	/01
SLA Class								
TLOC								
VPN								
				Next	CANCEL			
Cisco vMai	nage						▲ Ê	🔎 🕜 adm
CONFIGURATIO	N   POLICIES Centralized Policy >	Add Policy						
	0	Create Groups of Interest	<ul> <li>Configure Topolo</li> </ul>	ogy and VPN Membership	O Configure Traffic Ru	les 💽 Apply Pol		
Specify your network	topology							
Topology VP	N Membership							
Add Topology	•							0
Q		Search Options 🖌						Total Ro
Name	Туре		Description↑	Referen	ice Count	Updated By	Last Updated	
				No doto ou				
				No data av	allable			
BACK				Next	CANCEL			
DACK				Next	JANGEL			
	nage						▲ <b>白</b>	🔊 🙆 adm
		Add Deline					<u> </u>	📕 🔮 aann
CONFIGURATION	N   POLICIES Centralized Policy > .	Add Policy				_		
	0	Create Groups of Interest	Configure Topolo	ogy and VPN Membership	<ul> <li>Configure Traffic Rul</li> </ul>	es 📃 💿 Apply Poli		
Choose a tab and add	Traffic rules under the selected type							
Application Awar	re Routing Traffic Data Cflo	wd						
		nolicy)						0
Add Policy	(Create an application-aware routing							S
Add Policy +	(Create an application-aware routing	Present Particular						Total Roy
Add Policy ▼	(Create an application-aware routing	Search Options 🗸						Total Ro
<ul> <li>Add Policy </li> <li>Q</li> <li>Name</li> </ul>	(Create an application-aware routing	Search Options 🗸	Description	Referen	ce Count	Updated By	Last Updated	Total Ro
● Add Policy ▼ Q Name	(Create an application-aware routing Type	Search Options V	Description	Referen	ce Count	Updated By	Last Updated	Total Ro
<ul> <li>✿ Add Policy ▼</li> <li>Q</li> <li>Name</li> </ul>	(Create an application-aware routing	Search Options V	Description	Referen	ce Count	Updated By	Last Updated	Total Ro
✿ Add Policy ► Q Name	(Create an application-aware routing	Search Options V	Description	Referen	∝e count ∕ailable	Updated By	Last Updated	Total Ro
✿ Add Policy ▼       Q       Name	(Create an application-aware routing	Search Options V	Description	Referen	∝ count ∕ailable	Updated By	Last Updated	Total Ro

Step 2. Click Add Policy > Create New to create a new Application Aware Routing Policy.

■	cisco vManage					•	Ê	<b>*</b> @	0			
	CONFIGURATION   POLICIES Centralized Police	cy > Add Policy										
		Create Groups of Interest	Configure Topology and VPN Membe	rship O Configure Traffic Rules	Apply Policies to Sites and VPI							
۰	Choose a tab and add Traffic rules under the selected	l type										
عر	Application Aware Routing Traffic Data	Cflowd										
ê	• Add Policy • (Create an application-aware re	outing policy)								0		
	Create New	Search Options 🗸								Total Rows: 0		
-	Name Type	•	Description	Reference Count	Updated By	Last Upc	dated					
	No data available											
	NO UATA AVAIIADIE											
				_								
	BACK		Next	CANCEL								

Input the **Name** and **Description** for the policy. To add the policy, click **Sequence Type** and under **App Route** tab select **Sequence Rule** option

≡	cisco Cisco vMar	age	•	â	<b>*</b> @	🕜 ad	lmin 🔻
		POLICIES Add Application Aware Route Policy					
▣	Name	Voice, Video, AAR, Policy1					
٠	Description	Voice_Video_AAR_Policy1					
٩							
÷	Sequence Typ	App Route				Application	Route
	↑ Drag & drop to red	rder O Sequence Rule O ACI Sequence Rules Drag and drop to re-arrange rules					
*	App Route						
•••	Default Action						
		Save Application Aware Routing Policy CANCEL					

Step 3. select the traffic by matching on the options available in the Match tab.

=	cisco Cisco vMan	age														•		Ē	٠	0	admin 🔫
55	CONFIGURATION	POLI	CIES Add Application	Aware Route Policy																	
ᅟ	Name	Voice	_Video_AAR_Policy1																		
٠	Description	Voice	_Video_AAR_Policy1																		
ગ																					
<u> </u>	Sequence Type	e	Pe App Route																	Applic	ation Route
-	↑↓ Drag & drop to reo	order	Sequence Rule	ACI Sequence Ru	ules Drag and	drop to re-arrange	e rules														
*	App Route	÷							Ма	atch Act	ons								_		
	Default Action		Protocol	IPv4 💌	•	.pplication/	Application Family List	t Cloud Saas	Application List	DNS Applic	ition List DN	IS DSCP	PLP	Protocol	Source Data Pr	efix Source	Port	Destinati	►		
			Match Conditions									Actions									
																		Save Ma	ch And Act	ions	Cancel
																		_		_	_
							Save	Application Av	vare Routing Po	olicy C/	NCEL										

The match criteria matches the data traffic originating from the service side. Below table lists the different options available to match on:

Possible Match options		Description
Application / Application Family List	Pre-defined / custom-defined list	Leverage the pre-defined Application/Applications-list or create custom application-list to match (defined in the guide steps 1 -5).

Cloud SaaS Application List	Pre-defined list	Leverage the pre-defined Cloud-Saas Application list
DNS Application List	Pre-defined / custom-defined list	DNS application list is used to split DNS lookup per the selected application-lists.
DNS	DNS request / response option	DNS packets.
DSCP	0-63	Pre-configured traffic with DSCP values through QoS policy on the service-side traffic can be used to match the traffic.
PLP	High / Low options	Pre-configured traffic part of the Packet Loss Priority (PLP) queue, configured part of Policer QoS section policy, can be matched. 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.
Protocol	Protocol number	Traffic with defined protocol number can be matched
Source Data Prefix	custom-defined data prefix	Pre-defined custom data-prefix of the traffic can be matched on
Source Port	Port number	Data traffic with defined port number can be matched.
Destination Data Prefix	custom-defined data prefix	Pre-defined custom data-prefix of the traffic can be matched on
Destination Port	Port number	Data traffic with defined port number can be matched.

For this guide, lets pick the previously created custom Application Family list.

≡	cisco Cisco vMar	nage		۵	Ê	<b>*</b> ®	0	admin 🔻
:	CONFIGURATION	N   POLIC	CIES Add Application Aware Route Policy					
	Name	Voice_	_Video_AAR_Policy1					
٠	Description	Voice_	_Video_AAR_Policy1					
حر 19 ::	• Sequence Typ † Drag & drop to rea App Route	pe eorder	App Route     Sequence Rule     ACI Sequence Rules     Drag and drop to re-arrange rules     Match     Actions				Appl	ication Route
11	Default Action		Protocol IPv4  pplication/Application Family List Cloud Saas Application List DNS Application List DNS DSCP PLP Protocol Sou	irce Data Prefix	Source Port	l I	•	
			Match Conditions Actions					
			Application/Application Family List ×					
			Audio_Video_Application_List ×					
					Save M	atch And Ad	tions	Cancel
			Save Application Aware Routing Policy CANCEL					

Note that multiple match statements can be configured within the same sequence to select more specific traffic, as shown below

≡	Cisco vManage		•	ê	<u>¢</u>	0	
		ES Add Application Aware Route Policy					
	Name Voice_	ideo_AAR_Policy1					
۰	Description Voice_	ideo_AAR_Policy1					
× ≞	• Sequence Type  t Drag & drop to reorder	App Route     Sequence Rule     O ACI Sequence Rules     Drag and drop to re-arrange rules				Applic	ation Route
	App Route	Match Actions Protocol IPv4	DNS DSCP PLP Protocol Source Data Prefo	Source P	ort	►	
		Match Conditions	Actions				
		Apolication/Application_List ×					
		Source Data Prefix List × Custom_DataPrefix_List1 ×					
		Source: IP Prefix Example: 10.0.0.0/12					
				Sav	e Match And	Actions	Cancel

Step 4. Select the preferred Actions to be performed for the matched traffic.

Possible Action options	
Backup SLA Preferred Color	choose predefined color(s) that traffic is forwarded if the SLA is not met
Counter	Specify name to store the count for matching packets
Log	If enabled, syslog message is generated first time a packet flow is logged and every 5 minutes thereafter, as long as the flow is active. <b>'show log'</b> can be leveraged to view the log.
SLA Class List	Select the custom/pre-defined SLA Class List and choose preferred color(s) that traffic gets forwarded as long as the specified SLA is satisfied.
Cloud SLA	Enabled (if selected)

App Route policy actions statement allows us to define **Preferred Color** list as long as the **SLA class** is satisfied and action if SLA is breached, either to use the **Backup SLA Preferred Color** or drop the traffic by enabling the **Strict** option.

=	cisco VMan	age									•	Û	<u>¢</u> @	0	
:	CONFIGURATION	POLICIES Add Applicatio	n Aware Route Policy												
	Name	Voice_Video_AAR_Policy1													
٠	Description	Voice_Video_AAR_Policy1													
۹ 4	Sequence Type	App Route	2	_										Applic	ation Route
	t↓ Drag & drop to reo	rder Sequence Rule	<ul> <li>ACI Sequence Rules</li> </ul>	Drag and drop to re-arrange rules			Match	Actions							
•	Default Action	Protoco	I IPv4 💌			Backup SLA P	referred Color	Counter	Log SLA	Class List Cloud SLA					
		Match Condition:	ŝ						Actio	ins					
		Application/Appli	ication Family List					;	×						
		Audio_Video_A	kpplication_List ×					*							
												Save M	latch And Act	tions	Cancel
					Save Applic	cation Aware Routin	g Policy	CANCEL							

App Route policy actions statement allows us to define **Preferred Color** list as long as the **SLA class** is satisfied and action if SLA is breached, either to use the **Backup SLA Preferred Color** or drop the traffic by enabling the **Strict** option.

Select SLA class List, Backup SLA Preferred Color option from the Actions. Select the previously created SLA Class, Preferred Color and Backup SLA Preferred Color from the drop-down menu.

Click Save Match and Actions option.

≡	cisco VMan	ige		•	â	<b>*</b> ®	Ø	admin 🔫
	CONFIGURATION	POLICIES						
▫	Name	Voice_Vide	2,ARLPolicy1					
۰	Description	Voice_Vide	LAAR_Policy1					
√ 41 ∺ 8	Sequence Type     tube     tube	der	App Route       Sequence Rule     O ACI Sequence Rules       Drag and drop to re-arrange rules       Match       Actions       Protocol       IPv4       Backup SLA Preferred Color       Counte     Log       SLA Class List       Cloud SLA	Bia Masu Jac				
			Match Conditions Actions					
			Application/Application Family List × SLA Class					×
			Audio_Video_Application_List × Custom_SLA_Class_1 ×					*
			Preferred Color					
			mpis X					¥
			Strict					
			Backup SLA Preferred Color					×
			public-internet ×					-
			Log En	abled				×
					Save N	Match And A	tions	Cancel
	PREVIEW		Save Application Aware Routing Policy CANCEL					

**Step 5.** Multiple App-Route rule can be defined part of the same policy, each rule is recognized by different sequence number, each rule containing a match-action pair defining the preferred treatment for the classified traffic. The data-traffic matching a sequence rule (executed from low to high sequence number), executes the appropriate action and exists the policy.

If no policy matches the traffic, Default Action rule is applied for the traffic. The WAN Edge behavior for Default Action is to perform load-balance the traffic across all available WAN transports

≡	cisco Cisco vMan	age							•	Ê	<b>*</b> ®	0	admin 👻
::	CONFIGURATION	ON   POLICIES Add Application Aware Route Policy											
▫	Name	Voice_Vid	se_Video_AAR_Policy1										
٠	Description	Voice_Vid	vice_Video_JAR_Policy1										
∢ ∎ :	Sequence Type       Page App Route         T <sub>1</sub> Drag & drop to reorder       Sequence Rule       ACI Sequence Rules         Drag and drop to re-arrange rules       Drag and drop to re-arrange rules										Applic	ation Route	
	App Route	1		Match Conditions			Actions						1
	Default Action			Application/Application Family List:	Audio_Video_Application_List		SLA Class:	List	Custom_SLA_Class_1				
				Source Data Prefix List:	VPN10_Prefix			Preferred Color	mpls				
		2		Match Conditions			Actions						1
				Source Data Prefix List:	VPN10_Prefix		SLA Class:	List	Custom_SLA_Class_1				Ē
				Source: IP				Preferred Color	mpls				
**Step 6.** (optional) Changing the Default Action behavior.

Modify the default behavior to redirect the data traffic to a preferred WAN transport that meets the specified SLA class list.

Click the **Default Action** and click **Edit** option.

≡	cisco VMan	je	•	Ê	<b>≜</b> ®	0	admin 👻
		POLICIES Add Application Aware Route Policy					
▫	Name	/oice_VideoAAR_Policy1					
٠	Description	/aice_VideoAAR_Policy1					
٩		Default Action					
÷	Drag & drop to reg						
*	App Route	None Enabled					
	App Route						
	Default Action						

select the SLA Class List and select the appropriate SLA Class from the drop-down menu. Click Save Match and Actions option.



### Tech tip

If no WAN transports satisfies the selected SLA class in the default action, the WAN Edge device will load-balance the data traffic across all the available links.

≡	cisco VMan	2		▲ Ê	<u>🔎</u> 🛛	admin 💌
		OLICIES Add Application Aware Route Policy				
D	Name	pice_Video_AAR_Policy1				
۰	Description	pice_Video_AAR_Policy1				
√ <b>1</b> ∷	Sequence Type     Type	App Route     Sequence Rule     ACI Sequence Rules     Drag and drop to re-arrange rule	8		Ap	oplication Route
68	App Koute	■ ■ Match Conditions	Actions			1
	Default Action	Application/Application Family List: Audio_Video_Application_L	ISLA Class	: List Custom_SLA_Class_1 Preferred Color mpls		
=	cisco vManag	Save Applicat	on Aware Routing Policy CANCEL	•	Ê <b>4</b> 8 6	) admin ◄
55	CONFIGURATION   P	IES Centralized Policy > Add Policy				
a		Screate Groups of Interest Configure Topology and	/PN Membership O Configure Traffic Rules	Apply Policies to Sites and VPNs		
٠	Choose a tab and add Traf	les under the selected type				
4	Application Aware Ro	g Traffic Data Cflowd				
÷	Add Policy      (Cre	an application-aware routing policy)				0
*	Q	Search Options 🗸				Total Rows: 1
	Name	Type Description	Reference Count Updated	By Last Upda	ted	
	Voice_Video_AAR_Policy	App Route Voice_Video_AAR_Policy1	u admin	20 Feb 20	20 6:13:38 PM PST	
	BACK		Next CANCEL			

Step 7. Click Save Application Aware Routing Policy and then Next.

Step 8. Create any additional Application-Aware Routing policies as shown in previous steps if necessary.

≡	cisco vManage					● B	<b>*</b> ®	🥝 admin 👻
5	CONFIGURATION   POLICIES Centralized	Policy > Add Policy						
▫		Create Groups of Interest	<ul> <li>Configure Topology and VPN Members</li> </ul>	hip O Configure Traffic Rules	Apply Policies to Sites and VPNs			
۵	Choose a tab and add Traffic rules under the sele	ected type						
٩	Application Aware Routing Traffic Dat	ta Cflowd						
â	Add Policy      (Create an application-aw	are routing policy)						0
<b></b>	Q	Search Options 🗸						Total Rows: 2
_	Name	Туре	Description	Reference Count	Updated By	Last Updated		
	Voice_Video_AAR_Policy1	App Route	Voice_Video_AAR_Policy1	1	admin	22 Feb 2020 4:09	0:17 PM PST	
	Voice_Video_AAR_Policy2	App Route	Voice_Video_AAR_Policy2	4	admin	07 Apr 2020 9:55	:11 AM PDT	
	BACK		Next	CANCEL				

**Step 9.** Final step in configuring the Application Aware Routing Policy is to choose the Site List and VPN list for the policy to be associated with

In the Centralized Policy wizard, select **Next** to navigate to **Apply Policies to Sites and VPNS** and select **Application-Aware Routing** tab.

Input **Policy Name** and **Policy Description** and under the previously created App-Aware policy section, click the **New Site List and VPN List** option.

=	cisco Cisco vMan	nage							•	ê	<b>*</b> @	0	admin 🔻
:	CONFIGURATION	I POLICIES Centralized Policy	> Add Policy										
⊐			Create Groups of Interest	Configure Topolo	ogy and VPN Membership —	📀 Configure Traffi	fic Rules	<ul> <li>Apply Policies to Site</li> </ul>	s and VPNs				
•	Add policies to sites an	nd VPNs											
	Policy Name	Maximum of 32 characters											
8	Policy Description	Description of the policy											
	Topology App	plication-Aware Routing	ffic Data Cflowd										
1.	Voice_Video_AA	AR_Policy1											
	New Site List:	and VPN List											
	Site List			VPN List			Act	tion					
	BACK				Preview Save Pol	CANCEL							

Select the previously defined Site List and VPN List. Click Add and click Save Policy.

cisco VMan	age							•	6 🍂	9	admin •
CONFIGURATION	POLICIES Centralized Pol	icy > Add Policy									
		📀 Create Groups o	f Interest 🛛 🔗 C	onfigure Topology and VPN Mem	nbership ——— 🤣 Co	onfigure Traffic Rules	<ul> <li>Apply Policies to S</li> </ul>	ites and VPNs			
Add policies to sites an	d VPNs										
Policy Name	AAR_Policy										
Policy Description	AAR_Policy										
Topology Appl	lication-Aware Routing	Traffic Data Cflowd									
Voice_Video_AA	R_Policy1										
New Site List a	and VPN List										
Select Site List											
Site_222 ×	Site_23 ×										*
Select VPN List											
VPN10 ×											×
_										_	
										Add Canc	;el
Site List↑			VPN Li	st			Action				
											_
BACK				Preview	Save Policy CANCE	EL.					
ululu Cisco vMan	lage								e 🖌	a a	admin
										Custom	Ontions
Centralized Policy	Localized Policy									- Oubtoin	options
,	,										~
• Add Policy											
• Add Policy		Search Options 🗸								1	Total Rows:
Add Policy     Add Policy     Name	Descripti	Search Options V	Туре	Activated	U	odated By	Policy Version		Last Updated	7	Total Rows:

## Step 10. Activate the policy

Configuring the Application Aware Routing policy does not push the policy to vSmart controller. Final step is to configure the vSmart controller and enforce the policy by activating the policy.

In vManage, navigate to **Configuration > Policies > Centralized Policy**. Choose the configured Application Aware Routing Policy, on the far right-side select the three dots (...) to the right of each table row and select **Activate** option from the menu.

≡	Cisco vManage						•	Ê	<b>*</b> ®	0	admin 👻
	CONFIGURATION   POLICIES									💷 Custom 0	ptions 👻
	Centralized Policy Localized P	olicy									
*	Add Policy										0
3	Q	Se	earch Options 🗸							To	al Rows: 1
	Name	Description		Туре	Activated	Updated By	Policy Version	Last l	Jpdated		
2	AAR_Policy	AAR_Policy		UI Policy Builder	false	admin	02222020T002255638	21 Fe	b 2020 4:22:	55 PM PST	•••
**										View	
										Preview	
										Edit	
										Delete	
										Activate	

Pop-up window will ask for confirmation to push the configuration to all vSmart controllers for enforcement. Click **Activate** 

≡		Cisco vManage							¢®		
55	<b>\$</b> c	ONFIGURATION   POLICIES								I Custom	n Options 👻
	Cen	tralized Policy Localized	Policy								
\$	٥	Add Policy		Activate Policy		×					00
a,	Q		Search Option	Policy will be applied to the reachable vSmarts:							Total Rows: 1
	Nai			15.15.15.25		Policy Version					
*	AA	R_Policy	AAR_Policy			02222020T0022556	38	21 Fel	b 2020 4:22	:55 PM PST	
*					Activate	Cancel					
≡	cisco	Cisco vManage					•	Ê	<b>*</b> *	0	admin 🔻
5		SK VIEW									
묘	Push v	vSmart Policy   😋 Validation Succ	ess 👻					Init	iated By: ad	min From: 1	00.119.42.142
\$	Total T	Task: 1   Success : 1									
т 3											08
	Q		Search Options 🗸								Total Rows: 1
÷		Statue	Massona	Hostname	System ID	Site ID		vManag	o IP		
*	>	Success	Done - Push vSmart Po	icy ENT19-vsmart1	15.15.15.25	25		11.11.1	1.21		
1											

# Process: Appending Application-Aware Routing policy

It is important to note that only one Centralized Policy can be associated and activated in the SD-WAN environment. The centralized policy can have multiple policies embedded within the same policy.

Deployments with an existing active centralized policy can add the Application-Aware Routing policy to the existing policy. This process walks through procedure needed to append the Application-Aware routing policy

Creating Application Aware Routing policies consists of defining the three core components:

- Identification Classify the traffic / Application group of interest.
- Application SLA Requirement Defining the application SLA requirements.

 Application-Aware Routing Policy – Policy maps the classified traffic to the transport tunnel based on the defined SLA requirement.

On creating the policy, associate and activate the centralized policy to appropriate Site list(s) and VPN list(s).

#### Procedure 1. Identification - Classify the traffic / Application group of interest.

The below procedure walks through steps needed to classify the traffic.

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** from the top right menu options and select **Lists** from the **Centralized Policy** section.

≡	cisco vManage						•	Ê	<b>*</b>	Ø	admin 🔫
::	CONFIGURATION   POLICIES									III Custom	Options 👻
	Centralized Policy Localized F	Policy					🜐 Centralized	Policy		ocalized Pol	icy
-	Add Policy						CLI Policy		CLI P	olicy	
- 🕶							Lists		Lists		
a.	Q	Search Options	<b>*</b>				Topology		Forw	arding Class	/QoS
Ť	Name	Description	Туре	Activated	Updated By	Policy Version	Traffic Policy		Acce	ss Control L	ists
2	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T00			Rout	e Policy	
*											_

Step 2. Select Application from the left panel and click New Application List

≡	cisco vManage					•	â	<b>≜</b> @	0	admin 🔻
s [	CONFIGURATION   POLICI	ES Centralized Policy > Add Policy								
▫		O Create Groups of I	nterest O Configure Topolo	ogy and VPN Membership O	Configure Traffic Rules O	Apply Policies to Sites and VPNs				
٠	Select a list type on the left and	start creating your groups of interest								
ع	Application	New Application List								
ĉ	Color	Name	Entries	Reference Count	Updated By	Last Updated	Action			- 1
*	Data Prefix	Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PST	/01			_
_	Policer	Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PST	/01			
8	Prefix									
	Site									
	SLA Class									
	TLOC									
	VPN									
				Next CANCEL						

Select the **Application** or **Application Family** and choose appropriate option from the drop-down option. Provide an **Application List Name** and Click **Add**.

	cisco Cisco vManage					•	Ē	<b>*</b>	0	adn
Γ	CONFIGURATION   POLICI	ES Centralized Policy > Add Policy								
		Create Group	ps of Interest O Configure Top		Configure Traffic Rules	— O Apply Policies to Sites and VPNs				
	Select a list type on the left and	start creating your groups of interest								
	Application	New Application List								
	Color	Application List Name								
	Data Prefix	Audio_Video_Application_List								
	Policer	Application     Application	on Family							
	Prefix	Audio/Video ×								Ŧ
	Site									
	SLA Class							Add	Cancel	
	TLOC									
	1011	Name								
	VPN	Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PST	/ 🗇 🗉			
		Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PST	/0=			

	abab									
≡ _	cisco Cisco vManage					•	Ê	<b>*</b>	0	admin 🔻
::	CONFIGURATION   POLICI	ES Centralized Policy > Add Policy								
		<ul> <li>Create Groups o</li> </ul>	f Interest O Configure Topo	ology and VPN Membership (	Configure Traffic Rules (	<ul> <li>Apply Policies to Sites and VPNs</li> </ul>				
۰	Select a list type on the left and s	start creating your groups of interest								
عر	Application	New Application List								
÷	Color	Name	Entries	Pafarance Count	Lindated By	Last Indated	Action			- 1
*	Data Prefix	Microsoft_Apps	bing, hockeyapp, live_hotmail, lync, l	0	system	15 Jan 2020 4:37:54 PM PST				- II
_	Policer	Google_Apps	blogger, chrome_update, gcs, gmail,	0	system	15 Jan 2020 4:37:55 PM PST	× 0 =			
	Prefix	Audio_Video_Application_List	audio-video	0	admin	20 Feb 2020 12:59:23 PM PST	/0=			
	Site									
	SLA Class									
	TLOC									
	VPN									
				Next CANCEL						

Step 3. Alternatively, to previous step, network administrator can match on Data Prefix to identify the traffic.

To define the data prefix. In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** from the top right menu options and select **Lists** from the **Centralized Policy** section.

≡	cisco vManage						•	Ê	<u>*</u>	Ø	admin 🛨
::	CONFIGURATION   POLICIES									III Custom	Options 👻
	Centralized Policy Localized P	olicy					🜐 Centralized	Policy	🛅 Lo	calized Poli	су
-	Add Policy						CLI Policy		CLI Po	olicy	
	0	Search Ontions					Lists		Lists		
ચ	~	ocaron epitone					Topology		Forwa	arding Class	QoS
	Name			Activated			Traffic Policy		Acces	s Control Li	sts
2	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T00			Route	Policy	
*											_

select the Data Prefix option from the List type on the left side panel, and click New Data Prefix List

	cisco vManage					•	Ê	<b>*</b>	0	
	CONFIGURATION   POLIC	IES Centralized Policy > Define Lists							E Custom	Options 👻
	Select a list type on the left and	start creating your groups of interest								
*	Application	● New Data Prefix List								
*	Color									_
۲.	Data Prefix	Name Entries	Internet Protocol	Reference Count	Updated By	Last Updated		A	ction	
ŝ	Policer									
*	Prefix		No data	a availabl	е					
	Site									
	SLA Class									
	TLOC									
	VPN									

Input the **Data Prefix List Name** and select either **IPv4** / **IPv6** from the **Internet Protocol** option and add the prefix that needs to be matched and select **Add** 

<ul> <li>Verify C Cloco VManage</li> <li>CONFIGURATION   POLICIES Centralized Policy &gt; Define Lists</li> <li>Select a list type on the left and start creating your groups of interest</li> <li>Application</li> <li>New Data Prefix List</li> <li>Data Prefix</li> <li>Data</li></ul>		Custom Options
CONFIGURATION   POLICIES Centralized Policy > Define Lists  Coor  Application Color  Data Prefix Color  Prefix SLA Class TLOC VPN N Name Entries Internet Protocol Reference Count Updated By Last Upd  Control L	Ac	Cancel
Select a list type on the left and start creating your groups of interest   Application   Color   Data Prefix   Data Prefix   Policer   Prefix   Site   SLA Class   TuOC   VPN     Name   Entries   Internet Protocol   Name   Entries     Internet Protocol     Internet Protocol     Name     Entries     Internet Protocol     Internet Protocol <t< th=""><th>Ac</th><th>d Cancel</th></t<>	Ac	d Cancel
Application   Color   Data Prefix   Data Prefix   Data Prefix <th>Ac</th> <th>ld Cancel</th>	Ac	ld Cancel
Color   Data Prefix   Policer   Prefix   Site   Site   Site   Site   Add Data Prefix   10.4.208.0/24     Internet Protocol   VPN     Name   Entrifes   Internet Protocol     Reference Count   Updated By     Last Updated State	Ac	Id Cancel
Das Prefix   Policer   Prefix   Site   Site   SLA Class   TLOC   VPN	Ac	id Cancel
Policer   Prefix   Site   SLA Class   TLOC   VPN	Ac	Id Cancel
Prefix Site Site SLA Class TLOC VPN Name Entries Internet Protocol Reference Count Updated By Last Upd ConFIGURATION   POLICIES Centralized Policy > Define Lists	Ac	Id Cancel
Image: State of the state	Ad	Gancel
Add Data Prefix SLA Class TLOC VPN Name Entries Internet Protocol Reference Count Updated By Last Upd Cisco VManage Cisco Cisco vManage Cisco Contriguration   Policies Centralized Policy > Define Lists	Ad	id Cancel
SLA Class TLOC VPN Name Entries Internet Protocol Reference Count Updated By Last Upd cisco Cisco vManage	Ad	Id Cancel
TLOC       VPN       Name       Entries       Internet Protocol       Reference Count       Updated By       Last Updated By         Internet Protocol       Cisco vManage       Constiguration   Policies       Centralized Policy > Define Lists	Ad	ld Cancel
VPN       Name       Entries       Internet Protocol       Reference Count       Updated By       Last Updated By         Image: tissue tisue tisue tissue tissue tisue tissue tissue tisue tiss		
Name     Entries     Internet Protocol     Reference Count     Updated By     Last Upd 		
	ted	Action
Cisco vManage Cisco vManage Configuration   POLICIES Centralized Policy > Define Lists		
CISCO VManage Control POLICIES Centralized Policy > Define Lists	@	
CONFIGURATION   POLICIES Centralized Policy > Define Lists	E #	🌒 admir
		Eustom Options
Select a list type on the left and start creating your groups of interest		
Application O New Data Prefix List		
Color		Autor
Name         Entries         Internet Protocol         Reference Count         Updated By         Last Updated Dy           Data Prefix         Custome_DataPrefix_Li         10.4.208.0/24         IPv4         0         admin         25 Aor 20	0 4:43:21 PM PDT	Action
Policer		
Prefix P		
ii) Site		
STM (1922		
TLOC		
VPN		

## **Procedure 2.** Define Application Service Level requirements.

This procedure walks through steps needed to define custom SLA class.

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** from the top right menu options and select **Lists** from the **Centralized Policy** section.

≡	cisco vManage						•	Ê	<b>*</b>	Ø	admin 👻
::	CONFIGURATION   POLICIES									I Custom	Options 👻
	Centralized Policy Localized P	Policy					Centralized	Policy		ocalized Pol	icy
-	Add Policy						CLI Policy		CLI P	olicy	
	0	Castaly Ontion					Lists		Lists		
ચ	Ч.	Search Option	· ·				Topology		Forw	arding Class	/QoS
	Name					Policy Version	Traffic Policy		Acce	ss Control L	sts
2	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T00			Rout	e Policy	
											_

Step 2. select the SLA Class option from the List type on the left side panel, and click New SLA Class List

_	ululu Cisco yManage							• •		•	admin -
		S. Operational Delivery of De	finalista					• •	· •	Custor	auriin •
==	Select a list type on the left and s	start creating your groups of i	nterest								ropuono -
□ ≎	Application	• New SLA Class List									
٩	Data Profix	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated		Action	
÷	Data Prenx	Transactional-Data	5	50	100	2	system	15 Jan 2020 4:	37:53 PM	<ul> <li>© =</li> </ul>	
	Policer	Bulk-Data	10	300	100	0	system	26 Mar 2020 1	1:17:27 A		
*	Prefix	Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:	37:54 PM		
11	Site	Default	25	300	100	0	system	15 Jan 2020 4:	37:55 PM	× •	
		Custom_SLA_Class_1	5	70	100	3	admin	20 Feb 2020 3:	55:09 PM		
	SLA Class										
	TLOC										
	VPN										

### Input the SLA Class List Name and Loss, Latency, Jitter value requirement for the application and click Add.



Step 3. Create additional SLA Class as shown in the previous step, if needed.

	cisco vManage							▲ Ê	1 <sup>69</sup> 0	admin 🛨	
::	CONFIGURATION   POLICI	ES Centralized Policy > De	fine Lists						III Custom C	ptions 👻	
	Select a list type on the left and start creating your groups of interest										
*	Application	• New SLA Class List									
۹.	Color	Name	Loss (%)	Latency (ms)	Jitter (ms)	Reference Count	Updated By	Last Updated	Action		
<b>a</b> .	Data Prefix	Transactional-Data	5	50	100	2	system	15 Jan 2020 4:37:53 PM	🖊 🗇 🗉		
1	Policer	Bulk-Data	10	300	100	0	system	26 Mar 2020 11:17:27 A.	. 🖊 🔁 🗉		
<b>.</b>	Prefix	Voice-And-Video	2	45	100	1	system	15 Jan 2020 4:37:54 PM	🖊 🖸 🗉		
		Default	25	300	100	0	system	15 Jan 2020 4:37:55 PM	🖊 🔁 🗉		
	Site	Custom_SLA_Class_1	5	70	100	3	admin	20 Feb 2020 3:55:09 PM	🖊 🗅 🗉		
	SLA Class	Custom_SLA_Class_2	5	70	100	0	admin	25 Apr 2020 5:08:59 PM	🖊 🗅 🕷		
	TLOC										
	VPN										

#### Tech tip

Any number of SLA Class can be created, but only 4 SLA class can be associated to the Application Aware Policy. Please refer to the corresponding version Release Notes for the latest supports number of SLAs.

The Site list defines the sites in the SD-WAN environment. This site list can be used to enforce the Application-Aware Routing to influence WAN Edge devices in the specified site(s).

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** from the top right menu options and select **Lists** from the **Centralized Policy** section.

≡	cisco vManage						۵	Ê	<b>*</b> @	ø	admin 👻
	CONFIGURATION   POLICIES									III Custom	Options 👻
ᆸ	Centralized Policy Localized	Policy					Centralized Po	olicy	🛅 La	ocalized Pol	.icy
~	Add Policy						CLI Policy		CLI P	olicy	
*	Q	Search Opti	ons 🗸				Lists		Lists		
۹.						_	Topology		Forwa	arding Class	/QoS
	Name						Traffic Policy		Acce	ss Control L	ists
<b>2</b>	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T00			Route	Policy	
*											

Step 2. Select Site from the left panel and create Site list by clicking New Site List

≡	Cisco vManage					<b>▲</b> 8	<b>*</b> @	Ø	admin 👻
::	CONFIGURATION   POLICI	ES Centralized Policy > Define Lists						E Custom	Options 👻
	Select a list type on the left and	start creating your groups of interest							
- *	Application	New Site List							
	Color								_
્ય		Name	Entries	Reference Count	Updated By	Last Updated	Action		
-	Data Prefix	Site_19	19	10	admin	16 Apr 2020 3:34:29 AM PDT	/01		
*	Policer	Site_12	12	3	admin	16 Apr 2020 3:33:43 AM PDT	101		
*	Prefix	Site_23	23	3	admin	21 Feb 2020 9:26:20 AM PST	<ul> <li>0</li> </ul>		
		Site_21	21	1	admin	04 Apr 2020 10:14:41 AM PDT	∕0∎		
ш	Site	Site_11	11	1	admin	16 Apr 2020 3:33:20 AM PDT	10		
	SLA Class	Site_13	13	1	admin	16 Apr 2020 3:34:01 AM PDT	< D =		
	TLOC	Site_20	20	1	admin	16 Apr 2020 3:34:37 AM PDT	<ul> <li>0</li> </ul>		
	1600	All_Sites	11, 12, 13, 19, 20, 21, 22, 23	13	admin	16 Apr 2020 3:35:28 AM PDT	< D II		
	VPN	Site 22	22	1	admin	04 Apr 2020 10:14:48 AM PDT	/01		

Input the Site List Name and Add Site. click Add

≡	cisco VManage		•	Ê	<b>"</b> 22	Ø	admin 👻
::	CONFIGURATION   POLICI	ES Centralized Policy > Define Lists				Custom	Options 👻
	Select a list type on the left and	start creating your groups of interest					
*	Application	O New Site List					
*	Color	Site List Name					
*	Data Prefix	Site_222					
ĉ	Policer	Add Site					
*	Prefix	222					
	Site				Add	Cance	əl
	SLA Class						

Step 3. Add additional sites by clicking the New Site List.

	cisco vManage					▲ Ê	单 😨 admir
		ES Centralized Policy > Define Lists					III Custom Options
	Select a list type on the left and s	start creating your groups of interest					
•	Application	New Site List					
عر	Color	Name	Entries	Reference Count	Updated By	Last Updated	Action
	Data Prefix	Site_19	19	10	admin	16 Apr 2020 3:34:29 AM PDT	/01
*	Policer	Site_12	12	3	admin	16 Apr 2020 3:33:43 AM PDT	101
**	Prefix	Site_23	23	3	admin	21 Feb 2020 9:26:20 AM PST	20 <b>1</b>
_	_	Site_21	21	1	admin	04 Apr 2020 10:14:41 AM PDT	20I
	Site	Site_11	11	1	admin	16 Apr 2020 3:33:20 AM PDT	2 D II
	SLA Class	Site_13	13	1	admin	16 Apr 2020 3:34:01 AM PDT	201
	TLOC	Site_20	20	1	admin	16 Apr 2020 3:34:37 AM PDT	20 <b>1</b>
		All_Sites	11, 12, 13, 19, 20, 21, 22, 23	13	admin	16 Apr 2020 3:35:28 AM PDT	20 <b>1</b>
	VPN	Site_22	22	1	admin	04 Apr 2020 10:14:48 AM PDT	20×
		Site_222	222	0	admin	25 Apr 2020 5:18:27 PM PDT	201
		Spoke_Lists	11-13, 20-23	12	admin	16 Apr 2020 4:31:28 AM PDT	✓ □■

### Procedure 4. Create VPN List

The VPN list defines the VPN defined in the SD-WAN environment. This VPN list can be used to enforce the Application-Aware Routing to influence traffic in the specified VPN.

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** from the top right menu options and select **Lists** from the **Centralized Policy** section.

≡	cisco vManage						•	Ê	<b>*</b> @	0	admin 👻
::	CONFIGURATION   POLICIES									III Custom	Options 👻
	Centralized Policy Localized P	Policy					🜐 Centralized	Policy	Lo	calized Pol	су
-	Add Policy						CLI Policy		CLI P	olicy	
	0	0					Lists		Lists		
عر	Q	Search Uptions	~				Topology		Forwa	arding Class	/QoS
	Name				Updated By	Policy Version	Traffic Policy		Acces	ss Control Li	sts
ŝ	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T00			Route	Policy	
<u></u>											_

Step 2. Select VPN from the left panel and create VPN list by clicking New VPN List

=	cisco vManage					<b>▲</b> ₿	🜲 🚱 admin 🗸
	CONFIGURATION   POLICI	ES Centralized Policy > Define Lists					III Custom Options -
	Select a list type on the left and	start creating your groups of interest					
*	Application	New VPN List					
	Color						
×	Data Brafix	Name	Entries	Reference Count	Updated By	Last Updated	Action
~	Data Pienx	VPN_14	14	0	admin	04 Apr 2020 10:18:53 AM PDT	× 0 •
2	Policer	VPN_10	10	4	admin	21 Feb 2020 9:46:45 AM PST	×01
*	Prefix	Full_Mesh_VPN_List	10-14	10	admin	09 Apr 2020 6:22:05 PM PDT	2 D II
_		VPN_11	11	0	admin	04 Apr 2020 10:18:26 AM PDT	10
w	Site	VPN_12	12	0	admin	04 Apr 2020 10:18:33 AM PDT	2 D #
	SLA Class	VPN_150	150	0	admin	04 Apr 2020 10:19:07 AM PDT	201
	TLOC	VPN_153	153	0	admin	04 Apr 2020 10:19:31 AM PDT	101
		AII_VPN	11-14, 151-154	0	admin	04 Apr 2020 10:20:24 AM PDT	×0.
	VPN	VPN_154	154	0	admin	04 Apr 2020 10:19:40 AM PDT	201
		VPN_13	13	0	admin	04 Apr 2020 10:18:45 AM PDT	×01
		The Arthough Annu and	400.404	**	a desta	00 A 0000 C-01-45 DM DDT	255

Input the VPN List Name and Add VPN. click Add.

=	cisco VManage					▲ €	ä 4 <sup>89</sup> Ø	
	CONFIGURATION   POLICI	IES Centralized Policy > Define List	s				🗰 Custom C	Options 👻
	Select a list type on the left and	start creating your groups of interest						
•	Application	New VPN List						
	Color	VPN List Name						
<u></u>	Data Prefix	VPN_15						
<b>ê</b>	Policer	Add VPN						
<b></b>	Prefix	15						
1	Site						Add Cancel	I
	SLA Class							
	TLOC							
	VPN	Name	Entries	Reference Count	Updated By	Last Updated	Action	
		VPN_14	14	0	admin	04 Apr 2020 10:18:53 AM PDT	2 0 ∎	
		VPN_10	10	4	admin	21 Feb 2020 9:46:45 AM PST	10 1	

Step 3. Add any additional VPN by clicking the New VPN List.

≡	cisco vManage					۵	Ê	<b>*</b> ®	0	admin 👻
::		ES Centralized Policy > Define Lists							III Custom	Options 👻
	Select a list type on the left and s	start creating your groups of interest								
	Application S New VPN List									
\$	Color									
۹.		Name								
	Data Prefix	VPN_14	14	0	admin	04 Apr 2020 10:18:53 AM PDT	10			
-	Policer	VPN_10	10	4	admin	21 Feb 2020 9:46:45 AM PST	10			
*	Prefix	Full_Mesh_VPN_List	10-14	10	admin	09 Apr 2020 6:22:05 PM PDT	10			
_		VPN_11	11	0	admin	04 Apr 2020 10:18:26 AM PDT	10			
	Site	VPN_12	12	0	admin	04 Apr 2020 10:18:33 AM PDT	10			
	SLA Class	VPN_150	150	0	admin	04 Apr 2020 10:19:07 AM PDT	10			
	TLOC	VPN_153	153	0	admin	04 Apr 2020 10:19:31 AM PDT	10			
		AIL_VPN	11-14, 151-154	0	admin	04 Apr 2020 10:20:24 AM PDT	10			
	VPN	VPN_154	154	0	admin	04 Apr 2020 10:19:40 AM PDT	/0			
		VPN_13	13	0	admin	04 Apr 2020 10:18:45 AM PDT	10			
		Hub_Spoke_VPN_List	150-154	18	admin	09 Apr 2020 6:21:45 PM PDT	10	•		
		VPN_151	151	0	admin	04 Apr 2020 10:19:13 AM PDT	10	•		
		VPN_152	152	0	admin	04 Apr 2020 10:19:23 AM PDT	10			

#### **Procedure 5.** Configuring Application-Aware Routing policy

This procedure walks through the steps needed to create Application-Aware Routing policy. The policy binds the previously created traffic class to the specified WAN Edge device transport tunnel that satisfies the selected SLA class requirements.

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Click **Custom Options** and select **Traffic Policy** from the **Centralized Policy** section.

=	Cisco vManage						•	Ê	<b>*</b>	Ø	admin 👻
::	CONFIGURATION   POLICIES									III Custom	Options 👻
	Centralized Policy Localized Policy	olicy					🜐 Centralized I	Policy	Lo	calized Pol	су
-							CLI Policy		CLI Po	blicy	
	0	Search Options V					Lists		Lists		
۹.	~						Topology		Forwa	irding Class	/QoS
	Name					Policy Version	Traffic Policy		Acces	s Control Li	sts
ĉ	Centralized_Policy	Centralized_Policy	UI Policy Builder	true	admin	03062020T045:			Route	Policy	
*											
_											

Step 2. Select the Application Aware Routing tab and select Add Policy > Create New

≡	cisco vManage	•	1	<b>*</b> @	0	admin 👻
	CONFIGURATION   POLICIES Centralized Policy > Appliciation Aware Routing Policy				Custom (	Options 👻
	Choose a tab and add Traffic rules under the selected type					
*	Application Aware Routing Traffic Data Cflowd					
•••	Add Policy - Create an application-aware routing policy)					
	Create New Search Options V				Тс	otal Rows: 2

**Step 3.** Input the **Name** and **Description** for the policy and click **Sequence Type** and under **App Route** tab select **Sequence Rule** option.

≡	Cisco vMana	e	•	Ê	<b>*</b> @	Ø	admin 👻
::	CONFIGURATION	POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy					
▫	Name	/olce_Video_AAR_Policy2					
۵	Description	/oice_Video_AAR_Policy2					
√ <b>4</b> 1 :i	Sequence Type     Type	App Route     O Sequence Rule     O ACI Sequence Rules     Drag and drop to re-arrange rules				Applic	ation Route
	App Route Default Action						
	PREVIEW	Save Application Aware Routing Policy CANCEL					

**Step 4.** Select the match statement options to match the application/traffic set by clicking on the options available.

≡	cisco VMan	age 🔺 🌢 🏚	<b>@</b> a	dmin 👻
8	CONFIGURATION	POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy		
▫	Name	Voice_Video_AAR_Policy2		
٠	Description	Voice_Video_AAR_Policy2		
∢ ⇔ ∷	Sequence Type     T <sub>1</sub> Drag & drop to reo     App Route     Default Action	Image: App Route       Image: App Route         der       Image: Action and the property of the pro	Applicatio	n Route
		Match Conditions Actions		
	PREVIEW	Save Application Aware Routing Policy CANCEL		

Data traffic originating from the service side can be classified and matched. Below table points on to different possible options to match on:

Possible Match options		Description
Application / Application Family List	Pre-defined / custom-defined list	Leverage the pre-defined Application/Applications- list or create custom application-list to match (defined in the guide steps 1 -5).
Cloud SaaS Application List	Pre-defined list	Leverage the pre-defined Cloud-Saas Application list
DNS Application List	Pre-defined / custom-defined list	DNS application list is used to split DNS lookup per the selected application-lists.

DNS	DNS request / response option	DNS packets.
DSCP	0-63	Pre-configured traffic with DSCP values through QoS policy on the service-side traffic can be used to match the traffic.
PLP	High / Low options	Pre-configured traffic part of the Packet Loss Priority (PLP) queue, configured part of Policer QoS section policy, can be matched. 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.
Protocol	Protocol number	Traffic with defined protocol number can be matched
Source Data Prefix	custom-defined data prefix	Pre-defined custom data-prefix of the traffic can be matched on
Source Port	Port number	Data traffic with defined port number can be matched.
Destination Data Prefix	custom-defined data prefix	Pre-defined custom data-prefix of the traffic can be matched on
Destination Port	Port number	Data traffic with defined port number can be matched.

In this guide, we would pick the previously created custom Application Family list.

	Cisco VManag				•	Ê	<b>*</b>	Ø	admin 👻
=	CONFIGURATION	DLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy	_						
	Name	ice_Video_AAR_Policy2							
٠	Description	ice_Video_AAR_Policy2							
۹ ۳	Sequence Type	Pa App Route						Арр	lication Route
-	↑ Drag & drop to reord	Sequence Rule     ACI Sequence Rules     Drag and drop to re-arrange rules     Match     Actions							
13	Default Action	Protocol IPv4 - oplication/Application Family List Cloud Sass Application List DMS	Applica	ation List DNS DSCP PLF	Protocol	Source	Data Pré	►	
		Match Conditions		Actions					
		Application/Application Family List Audio_Video_Application_List ×	×						
						Save	Match And A	ctions	Cancel
	PREVIEW	Save Application Aware Routing Policy	CANC	EL					

Multiple match statements can be configured within the same sequence to select more specific traffic, as shown below:

≣	cisco VMan	nage 🛆 🖨 🍋 🥥 admir
:	CONFIGURATION	V POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy
2	Name	Volce_Video_AAR_Policy2
2	Description	Voice_Video_AAR_Policy2
⊾ ≌	Sequence Type	Application Ro
	T Drag & drop to reo	Cloud Saas Application List     DNS     DSCP     PLP     Protocol     Source Data     Protocol     Source Data     Protocol     Prv4
		Match Conditions Application_List Audio_Video_Application_List Source Data Prefix_List Source IIP Prefix Example: 10.0.00/12
		Save Match And Actions Cancel
	PREVIEW	Save Application Aware Routing Policy CANCEL

<b>Step 5.</b> Select the Actions to be performed for the above matched that	Step 5	5. Select the	Actions to be	performed f	or the	above	matched	traffic
--	--------	---------------	---------------	-------------	--------	-------	---------	---------

Possible Action options	
Backup SLA Preferred Color	choose predefined color(s) that traffic is forwarded if the SLA is not met
Counter	Specify name to store the count for matching packets
Log	If enabled, syslog message is generated first time a packet flow is logged and every 5 minutes thereafter, as long as the flow is active. 'show log' can be leveraged to view the log.
SLA Class List	Select the custom/pre-defined SLA Class List and choose preferred color(s) that traffic gets forwarded as long as the specified SLA is satisfied.
Cloud SLA	Enabled (if selected)

≡	Cisco vMana	ge	٠	Ê	<b>*</b>	Ø	admin 👻
::	CONFIGURATION	POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy					
□	Name	Voice_Video_AAR_Policy2					
\$	Description	Voice_Video_AAR_Policy2					
∢ ≙	Sequence Type	Poi         App Route           O Sequence Dula         O ACL Sequence Dulas				Applic	ation Route
*	T↓ Drag & drop to reor	er V Sequence kule V ACI Sequence kules Vrag and drop to te-arrange rules					1
	App Route Default Action	Protocol IPv4   Protocol IPv4 Protocol IPv4 Proto					
		Match Conditions Actions					
		Application/Application Family List ×					
		Audio_Video_Application_List ×					
				Save	Match And A	ctions	Cancel
		Save Application Aware Routing Policy CANCEL					

Application Aware Routing actions statement allows us to define **Preferred Color** list as long as the **SLA class** is satisfied and action to be performed in case the SLA is not met, either to use the **Backup SLA Preferred Color** or drop the traffic by enabling the **Strict** option.

Select **SLA class List,** Backup **SLA Preferred Color** option from the Actions. Select the previously created **SLA Class, Preferred Color** and **Backup SLA Preferred Color** from the drop-down menu.

≡	Cisco vMar	nage		•	Ê	¢@	0	admin 👻
	CONFIGURATION	N   POLIC	IES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy					
ᅟ	Name	Voice_	Video_AAR_Policy2					
٠	Description	Voice_	Video_AAR_Policy2					
<b>√</b> ∰ ∷ ⊟	Sequence Typ     T_ Drag & drop to re     App Route     Default Action	e order E	App Route     O ACI Sequence Rule     O ACI Sequence Rule     Drag and drop to re-arrange rules     Match     Actions      Protocol     IPy4     IDy4     Counter     Log     SLA Class Lat     Cloud SLA				Applic	ation Route
			Match Conditions Actions					_
			Application/Application Family List × SLA Class					×
			Audio, Video, Application_List x					-
			Preferred Color					
			( mpis ×)					•
			Strict					
			Backup SLA Preferred Color					×
			( public-internet ×)					-
			Log Enable	d				×
			Save Match And Actions Cancel					
	DDEVIEW		Save Application Aware Routing Policy CANCEL					

Click Save Match and Actions option

Multiple App-Route rule can be defined part of the same policy, each rule recognized by sequence number, each rule containing a match-action pair defining the preferred treatment for the classified traffic. When the data-traffic matches a rule (executed from low to high sequence number), the appropriate action is applied for the classified traffic. If no policy matches the traffic, Default Action rule is applied for the traffic.

WAN Edge behavior for Default Action is to perform load-balance the traffic across all available WAN transports.

Step 6. (optional) Changing the Default Action behavior.

Modify the default behavior to redirect data traffic to the WAN transports that meets the selected SLA Class List in the Actions tab as shown below.

Click the Default Action from the Sequence Type section and click Edit option.

≡	cisco VMan	age										•	Ċ.	<b>*</b>	0	admin 👻
	CONFIGURATION	POLICIES	Centralized Policy >	<ul> <li>Application Aware Rol</li> </ul>	uting Policy > Add	d Application Awa	are Route Policy									
▫	Name	Voice_Vide	o_AAR_Policy2													
٠	Description	Voice_Vide	eo_AAR_Policy2													
٩	Sequence Type	e D	efault Action													
<b>≙</b> 	↑ Drag & drop to rec	rder	None				Enabl	led								
	App Route	:														
	Default Action															
https://10	00.119.104.198/index.html						Save Applicatio	on Aware Routing Policy	CAN	NCEL						

Select the SLA Class List and select the appropriate SLA Class from the drop-down menu. Click Save Match and Actions option.

=	cisco VMar	age	•	Ê	<u>*</u>	ø	admin 👻
		POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy					
□	Name	Voice_Video_AAR_Policy2					
\$	Description	Voice_Video_AAR_Policy2					
عر							
	Sequence Typ	e Default Action					
	$\uparrow_{\downarrow}$ Drag & drop to red	Actions					
Ä	App Route	None SLA Class List					
	Default Action						
		SLA Class Select one or more sla class lists					
		Search					
		Transactional-Data					
		Bulk-Data		Save Ma	ch And Actic	ns Ca	ncel
		Voice-And-Video					_
		Default					
		Custom_SLA_Class_1					
		New SLA Class List					
	PREVIEW	Save Application Aware Routing Policy CANCEL					
_							
=	cisco Cisco vMan	age	•	Ê	<b>*</b>	0	admin 👻
	CONFIGURATION	POLICIES Centralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy					
▣	Name	Voice_Video_AAR_Policy2					
۵	Description	Voice_Video_AAR_Policy2					
عر							
	<ul> <li>Sequence Type</li> </ul>	Default Action					
_	↑↓ Drag & drop to rec	rder SLA Class Transactional-Data					
<u> </u>	App Route	<u>.</u>					
	Default Action						
	PREVIEW	Save Application Aware Routing Policy CANCEL					
Те	ch tip						

If none of the WAN transports satisfies the selected SLA class in the default action, the WAN Edge device will load-balance the data traffic across all the available links.

Step 7. Click Save Application Aware Routing Policy.

=	Cisco vMana	age				•	•	Ê	<b>*</b> @	0	admin 👻
::	CONFIGURATION	POLIC	IES (	entralized Policy > Application Aware Routing Policy > Add Application Aware Route Policy							
	Name	Voice_	/ideo_/	AR_Policy2							
٠	Description	Voice_	/ideo_/	AR_Policy2							
× ۹	<ul> <li>Sequence Type</li> <li>T<sub>1</sub> Drag &amp; drop to reor</li> </ul>	rder	C S	App Route           quence Rule         • ACI Sequence Rules         Drag and drop to re-arrange rules						Applicat	ion Route
	App Route Default Action		1	Match Conditions     Actions     Application/Application_List     SLA Class	:: List Preferred Color	Custom_SLA_C mpls	lass_1				
	PREVIEW			Save Application Aware Routing Policy CANCEL	A						_

Step 8. Create any additional Application Aware Routing policies if necessary.

=	cisco vManage					È	<b>#</b> @ @	) admin <del>v</del>
::	CONFIGURATION   POLICIES Centraliz			III Cu	istom Options 👻			
	Choose a tab and add Traffic rules under the							
-	Application Aware Routing Traffic	Data Cflowd						
•	Add Policy      (Create an application-							
٩,	Q				Total Rows: 2			
<b>2</b>	Name↑	Туре	Description	Reference Count	Updated By	Last Updated		
*	Voice_Video_AAR_Policy1	App Route	Voice_Video_AAR_Policy1	1	admin	22 Feb 2020 4:09	0:17 PM PST	
-	Voice_Video_AAR_Policy2	App Route	Voice_Video_AAR_Policy2	4	admin	07 Apr 2020 9:55	5:11 AM PDT	

#### **Procedure 6.** Associate and activate the Application-Aware Routing policy

To apply the App-Aware routing policy to the already existing centralized policy, create a copy of the existing activated policy and edit the copied policy. Making a copy of the existing policy allows administrators to keep the existing configured policy active, while making the new changes to the copied policy.

**Step 1.** In vManage, navigate to **Configuration > Policies > Centralized Policy**. Select the policy and click the three dots (...) and select **Copy**.

≡	Cisco vManage					•	) ê	<b>*</b> @	0	admin 🔻
::	CONFIGURATION   POLICIES								III Custom C	Options 👻
	Centralized Policy Localized Policy	olicy								
\$	Add Policy									0
ચ	Q	Search Options 🗸							То	otal Rows: 1
	Name	Description	Туре	Activated	Updated By	Policy Version	Last Up	lated		
*	Centralized_Policy	Centralized_Policy	UI Policy Builder	true	admin	03062020T045202769	05 Mar 2	2020 8:52:02	2 PM PST	•••
*									View	
11								- F	Preview	1
									Edit	
									Delete	
									Deactivate	_

Step 2. Input the Policy Name and Description for the new policy and click Copy

Policy Copy	×
Policy Name	
Centralized_Policy_2	
Description	
Centralized_Policy_2	
Copy Cance	3I

**Step 3.** Confirm that the newly created Policy is inactive (column **Activated: false** status) and then select the three dots (...) against the policy and choose **Edit** to add App-Aware routing policy.

sco <sup>1</sup> Cisco vManage						•		<mark>)</mark>	) a	admin <del>v</del>
CONFIGURATION   POLICIES								III C	ustom Opt	tions 👻
Centralized Policy Localized Po	blicy									
Add Policy										0
Q	Search Options 🗸								Total	l Rows: 2
Name	Description	Туре	Activated	Updated By	Policy Version	L	ast Updated			
Centralized_Policy	Centralized_Policy	UI Policy Builder	true	admin	03062020T045202769	C	15 Mar 2020 8	:52:02 PM P	ST	
Centralized_Policy_2	Centralized_Policy_2	UI Policy Builder	false	admin	03062020T045643280	C	15 Mar 2020 8	:56:43 PM P	ST	
								Vie	N	
								Pre	view	
								Edit	, y	
								Del	ete	_
								Act	ivate	
	Signed State       ConFigurAtion   Policies         ConFigurAtion   Policy       Localized Policy         Add Policy       Localized Policy         Add Policy       Localized Policy         Name       Contralized_Policy         Centralized_Policy_2       Localized	Search Option       Add Policy       Add Policy       Add Policy       Add Policy       Add Policy       Search Option       Name       Description       Centralized_Policy       Centralized_Policy_2       Centralized_Policy_2	Vibito       Cisco vManage         CONFIGURATION   POLICIES         Centralized Policy       Localized Policy         Add Policy       Search Options v         Add Policy       Search Options v         Name       Description       Type         Centralized_Policy       Centralized_Policy       Ul Policy Builder         Centralized_Policy_2       Centralized_Policy_2       Ul Policy Builder	Search Options         Search Options ~         Add Policy       Search Options ~         Add Policy       Search Options ~         Name       Description       Type       Activated         Centralized_Policy_2       Centralized_Policy_2       UI Policy Builder       true	Obscription       Search Options         Name       Description       Type       Activated       Updated By         Centralized_Policy       Centralized_Policy_2       Ul Policy Builder       true       admin         Centralized_Policy_2       Centralized_Policy_2       Ul Policy Builder       false       admin	Visition of Control policies         Contriguration   policies         Centralized Policy       Localized Policy         Add Policy         Centralized Policy       Search Options •         Name       Description         Centralized Policy       Centralized Policy         Centralized Policy       Centralized Policy         Centralized Policy       Centralized Policy_2         Visit   Policy Builder       Ture         Centralized Policy_2       Centralized Policy_2         Visit   Policy Builder       Tale         Centralized Policy_2       Visit Policy Builder         Centralized Policy_2       Visit Policy Builder	Image: I	Image:	vielo Cisco vManage	iii) iii) iii) iii) iii) iii) iiii) iii)

**Step 4.** Click **Traffic Rules** tab and choose **Application Aware Routing** and click **Add Policy**, select **Import Existing** option from the drop-down menu.

=	cisco vManage	•	8 4	<u>89</u>	🕜 adr	
::	CONFIGURATION   POLICIES Centralized Policy > Edit Policy					
▫	Policy Application Topology Traffic Rules					
۵	Choose a tab and add Traffic rules under the selected type					
ચ	Application Aware Routing Traffic Data Cflowd					
÷	• Add Policy - (Create an application-aware routing policy)				0	
	Create New Search Options V				Total Ro	ows: 1
	Import Existing Type Description Bioference Count Updated By	Last	Updated			

Select the policy created from the drop-down menu and click **Import**.

Import Existing Ap	oplication Aware Routing Policy	×
Policy	Voice_Video_AAR_Policy2	•
		Import Cancel



≡	cisco vManage					•	Ê	<b>*</b> @	0	admin 👻
::	CONFIGURATION   POLICIES Cent	ralized Policy > Edit Policy								
▫			Policy Application	Topology Traffic Rules						
٠	Choose a tab and add Traffic rules under t	he selected type								
عر	Application Aware Routing Traf	fic Data Cflowd								
ŝ	• Add Policy • (Create an applicat	ion-aware routing policy)								0
	Q	Search Options 🖌								Total Rows: 2
	Name	Туре	Description	Reference Count	Updated By	Last U	pdated			
•••	Voice_Video_AAR_Policy1	App Route	Voice_Video_AAR_Policy1	1	admin	22 Feb	2020 4:09:	17 PM PST		
	Voice_Video_AAR_Policy2	App Route	Voice_Video_AAR_Policy2	0	admin	05 Mar	r 2020 7:48:	06 PM PST		
			Preview Save	Policy Changes CANCEL						

Step 6. Select the Policy Application and select the Application-Aware Routing tab.

Under the imported App-Aware routing policy, click the **New Site List and VPN List** and select the appropriate **Site List** and the **VPN List** from the drop-down menu

=	Cisco vMana	e	•	Ê	<u>*</u>	0	admin 🔫
::	CONFIGURATION	OLICIES Centralized Policy > Edit Policy					
▫		Policy Application         Topology         Traffic Rules					
۰	Add policies to sites and	PNs					
عر	Policy Name	Centralized_Policy_2					
÷	Policy Description	Centralized_Policy_2					
*	Topology Applie Voice_Video_AAR	Ation-Aware Routing Policy2					
	Site List	VPN List Action					
							- 1
							_
		Preview Save Policy Changes CANCEL					

click Add and click Save Policy Changes.

=	cisco VMana	ge	•	Ê	<b>*</b> @	ø	admin 👻
::	CONFIGURATION	POLICIES Centralized Policy > Edit Policy					
▫		Policy Application Topology Traffic Rules					
۰	Add policies to sites and	VPNs					
٩	Policy Name	Centralized_Policy_2					
ĉ	Policy Description	Centralized.Policy.2					
*	Topology Appl	cation-Aware Routing Traffic Data Cflowd					
1	Voice_Video_AAI	LPolicy2					
	Select Site List	te_23 ×					•
	Select VPN List						
	VPN_10 ×						-
					Add	Cancel	
		Preview Save Policy Changes CANCEL					

**Step 7.** Activate the modified Centralized Policy.

Configuring and associating the Application Aware Routing policy does not push the policy to vSmart controller or enforce the policy in the SD-WAN environment. Final step is to activate the policy, which provisions the vSmart controller and enforces the policy.

In vManage, navigate to **Configuration > Policies > Centralized Policy**. Choose the newly configured centralized policy from the list, on the far right-side select the three dots (...) and select **Activate** option from the menu.

	ala da ser ser ser									
	cisco VManage					•	Ê	<b>*</b>	0	admin 👻
8	CONFIGURATION   POLICIES								Custom 0	ptions 👻
	Centralized Policy Localized Policy	licy								
•	Add Policy									0
4	Q	Search Options 🗸							Tot	al Rows: 2
Č.	Name	Description	Туре	Activated	Updated By	Policy Version	Last Update	d		
÷	Centralized_Policy	Centralized_Policy	UI Policy Builder	true	admin	03062020T045202769	05 Mar 2020	0 8:52:02 PN	/ PST	
**	Centralized_Policy_2	Centralized_Policy_2	UI Policy Builder	false	admin	03062020T045643280	05 Mar 2020	) 9:07:29 PN	/ PST	
•									View Preview	
									Сору	
									Edit	
								C	Activate	

Pop-up window would ask for confirmation to push the configuration to all vSmart controllers for enforcement. Click **Activate**.

Activate Policy	×
Policy will be applied to the reachable vSmarts:	
15.15.15.25	
	Activate Cancel

the new policy configuration is pushed to vSmart and the configuration is activated for enforcement.

		Cisco vManage				•	Ê	<b>*</b> @	0	
::	Ê TA:	SK VIEW								
	Push v	Smart Policy   📀 Validation Success 👻					Initi	ated By: admi	n From: 1/	0.119.42.142
~	Total T	ask: 1   Success : 1								
ع										0
÷	Q		Search Options 🗸							Total Rows: 1
	>	Status	Message	Hostname	System IP	Site ID	vManage	IP		
<u></u>	>	Success	Done - Push vSmart Policy	ENT19-vsmart1	15.15.15.25	25	11.11.11	21		
11										

# Operate

With Application-Aware routing deployed and activated, this section covers steps to manage, monitor and troubleshoot the various component in the SD-WAN environment using vManage GUI.

# Process: Monitor the Application-Aware Routing policy

#### **Procedure 1.** View the Application-Aware routing policy configuration

Step 1. View the activated centralized policy

To confirm the centralized policy that contains Application–Aware Routing policy is activated, navigate to **vManage** > **Configuration** > **Policies** > **Centralized Policy** and the **Activated** section should be **true**.

=	Cisco vManage					•	ê <b>4</b> 9 0	admin 🔻
	CONFIGURATION   PO	LICIES					E Custom C	Options 👻
	Centralized Policy Log	calized Policy						
\$	Add Policy							0
4	Q	Sea	rch Options 🗸				То	tal Rows: 1
	Name	Description	Туре	Activated	Updated By	Policy Version	Last Updated	
÷	AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020T002255638	21 Feb 2020 4:22:55 PM PST	
•								

**Step 2.** View the Application-Aware routing policy from the vManage User Interface.

To view the Application-Aware Routing Policy, navigate to **vManage** > **Configuration** > **Policies.** Click the **Custom Options** on the top right corner and select the **Centralized Policy** > **Traffic Policy**.

Cisco vManage						•	Ê	¢® @	) admii	
CONFIGURATION   POLICIES								📖 Ci	istom Options	•
Centralized Policy Localized Policy	blicy					🜐 Centralized I	Policy	🛅 Localiz	ed Policy	
Add Policy						CLI Policy		CLI Policy		
						Lists		Lists		
Q	Search Options 🗸					Topology		Forwarding	Class/QoS	
Name	Description	Туре	Activated	Updated By	Policy Version	Traffic Policy		Access Cor	ntrol Lists	
AAR_Policy	AAR_Policy	UI Policy Builder	true	admin	02222020TC			Route Polic	у	
	ConFigURATION   POLICIES Contralized Policy C Add Policy Q Name AAR_Policy	Inition     Cisco vManage       CONFIGURATION   POLICIES       Centralized Policy       Localized Policy       Add Policy       Q       Search Options        Name       ARLPolicy       ARLPolicy	Initial Cisco vManage       CONFIGURATION   POLICIES       Centralized Policy       0 Add Policy       Q       Name       Description       AAR_Policy       UI Policy Builder	Name     Description     Type     Activated       ARLPolicy     ARLPolicy     UI Policy Builder     true	ConFiguration   Polucies   Contributed Policy   Contributed Policy   Conded Policy     Contributed Policy       <	ConFigURATION   POLICIES   ConfigURATION   POLICIES   Centralized Policy   Localized Policy   Configuration   Policy   Configuration   Policy   Localized Policy   Search Options ~     Search Options ~     Name   Description   ARLPolicy   ARLPolicy   ARLPolicy     View   Policy Builder   true   admin   0222202010	ConFigURATION   POLICIES   Contrailized Policy   Localized Policy   Add Policy   Search Options ~     Name   Description   AR_Policy   AR_Policy   AR_Policy     Mark   AR_Policy     UP locicy Builder   true   admin   02220207	Indic Classical Wainage     CONFIGURATION POLICIES     Contralized Policy     Catalated Policy	Indic Cicco VManage   CONFIGURATION   POLICIES   Centralized Policy   Localized Policy   Add Policy   Search Options     Name   Description   Art.Policy   AR_Policy   AR_Policy     Mark   Mark   Description   Type   Activated   Updated By   Policy Warks   Traffic Policy   Cill Policy   Lists   Traffic Policy   AR_Policy   UI Policy Builder   true   admin   Oczazor	Indic Cicco vManage   CONFIGURATION   POLICIES     Contributed Policy   Catalized Policy   Catalized Policy   Catalized Policy   Catalized Policy   Search Options v     Search Options v     Name   Description   Type   Activated   Updated By   Policy   UPolicy Builder   Tupe   Admin   Occurrence     Route Policy     Cut Policy     Cut Policy   Lists   Topology   Porwarding Class/QoS   ARPolicy     UPolicy Builder     Tupe   Admin   Occurrence     Route Policy

Click the three dots (...) to the right of each table row against the policy and select View from the options

≡	cisco VManage						▲ Ê	<b>*</b> ® (	🕽 admin 🔫
::	CONFIGURATION   POL	LICIES	Centralized Policy > Appliciation Aware Ro	uting Policy					ustom Options 👻
	Choose a tab and add Traffic	rules und	ler the selected type						
-	Application Aware Rout	iting	Traffic Data Cflowd						
	Add Policy      (Create	te an appl	ication-aware routing policy)						0
<b>`</b>	٩		Search Options 🗸						Total Rows: 2
2	Name		Туре	Description	Reference Count	Updated By	Last Updated	ł	
*	AAR_23_222		App Route	AAR_23_222	0	admin	28 Jan 2020	11:07:14 AM PS1	•••
678	Voice_Video_AAR_Policy1		App Route	Voice_Video_AAR_Policy1	1	admin	22 Feb 2020	4:09:17 PM PST	
= :: 	CINCLE CISCO VMANAGE CONFIGURATION   POL Name Voic Description Voic	LICIES ( ce_Video_J	Centralized Policy > Application Aware Ro WR. Policy1 MR. Policy1	uting Policy > View Application Aware Route	Policy		▲ û	£dit Copy	admin 🗸
٩		91	Ann Dauta						Application Doute
÷	App Route		App Route						Application Route
	Default Action	0	Match Conditions			Actions			
			Application/Application Family List:	Audio_Video_Application_List		SLA Class: List	Custom_SLA_Class_1		
11						Preferred Color	mpls		
						Strict	false		
						Backup SLA Preferred Color:	public-internet		
						Log	Enabled		
			^						

Step 3. To verify the Application-Aware routing policy configuration on the vSmart controller

To view the Application-Aware Routing Policy, navigate to vManage, **Tools > SSH Terminal.** Select the vSmart controller and issue **show running-config policy.** 

≡	Cisco vManage			•	Ê	<b>*</b> ®	0	
::	🔧 TOOLS   SSH TERMINA	ıL.						
ᅟ	Device Group	<	15.15.15.25 x					
~	All	÷	Last login: Sat Feb 22 01:26:24 2020 from 100.119.42.47 Welcome to Viptela CLI					
لا ب	Q	~	admin connected from 11.11.11.21 using sah on ENT19-vemart1 ENT19-vemart1# how running-config policy policy					
-	Sort by Reachability \$	te.	sla-class Custom_SLA_Class_1 loss 5					
	ENT19-vmanage 11.11.11.21   Site ID: 21	vManage	latancy 70 jitter 100 I					
•	ENT19-vsmart1 15.15.15.25   Site ID: 25 Reachable		spp-route-policy_VTW_l0_Voice_Video_AAR_Policy1 vpn-list VPR_l0 expenses 1					
	ENT19-vbond 13.13.13.23   Site ID: 23 Reachable	vEdge Cloud vBond	matten source-ip 0.0.0/0 app-list Audio_Video_Application_List i					
	RS01-ISR4431-21 1.1.1.21   Site ID: 111 Reachable	ISR4431	action log backup-sla-preferred-color public-internet					
	RS01-ISR4431-22 1.1.1.22   Site ID: 111 Reachable	ISR4431	sia-clas Custom_SLA_Class_1 preferred-color mpis 1 1 1					
	RS02-ISR4331-18 2.2.2.18   Site ID: 222 Reachable	ISR4331	l lists vyn-list vym_10					
	RS02-ISR4331-19 2.2.2.19   Site ID: 222 Reachable	ISR4331	vp 10 I app-list Audio_Video_Application_List appo_family_andio_video					
	RS03-C1116P-15 3.3.3.15   Site ID: 333 Reachable	C1116-4P	app-family audio_video : site-list Site_222					
	RS05-ASR1001X-04 5.5.5.4   Site ID: 555 Reachable	ASR1001-X	ster_id 222 i site_ids_23 site_id_3					
	RS05-ASR1001X-05 5.5.5.5   Site ID: 555 Reachable	ASR1001-X						
	RS06-ASR1001HX-03 6.6.6.3   Site ID: 666	ASR1001-HX	ENT19-vsmart1#					

### and show running-config apply-policy

≡	Cisco vManage		•	Ê	<b>*</b> ®	0	admin 🔻
	K TOOLS   SSH TERMINAL						
	Device Group	< 15.15.15.25 x					
~	All	c 15.15.15.25 login: admin admin%15.15.15.25's password:					
	Q	Last login: Sun Feb 23 05:04:43 2020 from 11.11.11.21 V Nelcome to Viptela CLI addin connected from 11.11.11.21 using msh on ENT19-vemart1					
	Sort by Reachability \$	EXT19-vsmart1#					
	ENT19-vmanage 11.11.11.21   Site ID: 21	vManage Description: Apply network policy Possible completions: site-list Site list					
•	ENT19-vsmart1 15.15.15.25   Site ID: 25 Reachable	VErmain         I         Output modifiers <cr>         CrP         RNT9-Summing-config apply-policy</cr>					
	ENT19-vbond 13.13.13.23   Site ID: 23 Reachable	vEdge Cloud site-list Site_222 app-route-policy_VPN_10_Voice_Video_AAR_Policy1					
	RS01-ISR4431-21 1.1.1.21   Site ID: 111 Reachable	ISR4431 aito-list Site_J3 app-route-policy_VPM_10_Voice_Video_AAR_Policy1					
	RS01-ISR4431-22	ISR4431 INTI9-vsmart10					

**Step 4.** View the Application-Aware routing policy configured on the WAN Edge device.

To view the Application-Aware Routing Policy configured on the WAN Edge device, navigate to **vManage** > **Tools > SSH Terminal.** Select the WAN Edge device and issue **show sdwan policy from-vsmart** on IOS-XE SD-WAN platform



and show policy from-vsmart on Viptela platform.



#### Procedure 2. View the SLA configuration on the WAN Edge device

Step 1. View the SLA configured on the WAN Edge device.

To view the SLA configured, navigate to vManage, **Tools > SSH Terminal.** Select the WAN Edge device and issue **sh sdwan app-route sla-class** on IOS-XE SD-WAN platform **sh app-route sla-class** on vipteal platform.

≡	cisco Cisco vManage					•	Ê	<b>*</b>	0	admin 🔻
	K TOOLS   SSH TERMINAL									
	Device Group	<	15.15.15.25 🛪 2.2.2.19	×						
~	All	٠	2.2.2.19 login: admin admin@2.2.2.19's password:							
~ بر	۹	~	Password:							
	Sort by Reachability 🖨	t=	DS02_TSD4331_19#sh edua							
*	1.1.1.21   Site ID: 111 Reachable		RS02-ISR4331-19#sh sdwan ap RS02-ISR4331-19#sh sdwan app-							
	RS01-ISR4431-22 1.1.1.22   Site ID: 111 Reachable	ISR4431	RS02-ISR4331-19#sh sdwan app- RS02-ISR4331-19#sh sdwan app- INDEX NAME	route sl route sla-cla LOSS LATENC	ss Y JITTER					
	RS02-ISR4331-18 2.2.2.18   Site ID: 222 Reachable	ISR4331	0all_tunnels 1 Custom_SLA_Class_1	0 0 5 70	0 100					
	RS02-ISR4331-19 2.2.2.19   Site ID: 222 Reachable	ISR4331	RS02-ISR4331-19#							

# Process: Monitor the WAN transport path characteristics

#### **Procedure 1.** View the WAN transport path characteristics across the SD-WAN environment

SD-WAN transport tunnel characteristics across the SD-WAN environment or specific to the WAN Edge can be monitored from the vManage.

Step 2. Monitor transports health characteristics across the SD-WAN environment.

To view the tunnel characteristics across the SD-WAN infrastructure. Navigate to **vManage > Dashboard > Main Dashboard > Transport Health** widget.



**Step 3.** Expand the widget by clicking the **square icon** in the top right corner of the Transport Health widget and select the **Type** option to view the chart **By Loss, By Latency or by Jitter** values and view the transport health over the maximum of past 7 days.



## **Procedure 2.** View the path characteristics for the WAN Edge device

**Step 1.** Monitor WAN transport TLOC path characteristics for the WAN Edge device.

To view the tunnel characteristics on the WAN Edge device, navigate to vManage, **Monitor > Network > WAN -**Edge. select the WAN Edge device.

≡	Cisco vManage										۵	8 🎣	Ø	admin 🔫
::														
	WAN - Edge Colocation C	Clusters												
	VPN GROUP	VPN SEGME	NT											
۵	Select VPN Group	All segm	ienta											
∢ #	Device Group All +	٩		Search Options 👻									T	otal Rows: 14
**	Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID↑	BFD	Control	Version	Up Sin	se.	Device	Groups
-	ENT19-vmanage	11.11.11.21	vManage	24b0ba05-b599-45d9-a00a-3dee8	0	reachable	21	-	12	19.2.099	15 Jan	2020 4:34:00 PM PST	"No gr	oups"
w	8 RS21-vEdge1000-33	21.21.21.33	vEdge 1000	110G621194126J	0	reachable	21	17	2	19.2.099	25 Jan	2020 1:15:00 PM PST	"No gr	oups"
	8 RS21-vEdge1000-34	21.21.21.34	vEdge 1000	110G408180039	0	reachable	21	16 (17)	2	19.2.099	25 Jan	2020 1:15:00 PM PST	"No gr	oups"
	ENT19-vbond	13.13.13.23	vEdge Cloud (vBo	0a0e0ce1-da1a-4f4d-ac6d-56983	0	reachable	23	-	-	19.2.099	15 Jan	2020 4:34:00 PM PST	"No gr	oups"
	BRS23-vEdge2000-29	23.23.23.29	vEdge 2000	260E134323003AM	0	reachable	23	19	2	19.2.099	25 Jan	2020 1:24:00 PM PST	"No gr	oups"

Step 2. click WAN > TLOC from the left panel options for the device.

Select the **Chart options** and choose **Loss percentage** or **Latency/Jitter** option. By default, the value is shown for 24hours, but can be changed.

Cisco vManage					▲ Ê	" <u>@</u>	🧿 admin 👻
MONITOR Network >	WAN - TLOC						
Select Device 🝷	RS23-vEdge2000-29   23.23.23.29 Site ID: 23	Device Model: vEdge 2000 🚯					
Applications	Chart Options *				F Real Time 1h	3h 6h 12h [	4h 7days Custom 🕶
Interface	Loss					Legend	
	Percentage					mpls	
TCP Optimization	C Latency/Jitter	*******				public-inte	ernet
WAN Throughput	age 30 %						
Flows	Percent		1				
Top Talkers	S 20 %						
WAN	10 %						
TLOC							
Tunnel	0 Apr 05, 20:00 Apr 05, 22:00	Apr 06, 00:00 Apr 06, 02:00 Apr 06,	04:00 Apr 06, 06:00 Apr 06, 08:00 Apr	06, 10:00 Apr 06, 12:00 Apr 06, 14:00	Apr 06, 16:00		
Security Monitoring	2 Rows Selected						00
Firewall	Q	Search Options 🗸					Total Rows: 2
Intrusion Prevention	🔸 Down (0) 🥝 Partial (0) 🛧 Up (2)						
URL Filtering	Local Color	State	Jitter (ms)	Loss (%)	Late	ncy (ms)	
Advanced Malware	M mpls	1	0.00	0.00	0.00		
Protection	public-internet	<b>^</b>	0.01	23.03	0.69		
	Cisco vManage         MONITOR Network >         Salect Device -         Applications         Interface         TCP Optimization         WAN Throughput         Flows         Top Talkers         WAN         TLOC         Security Monitoring         Firewall         Intrusion Prevention         URL Filtering         Advanced Malware	Image: Cisco vManage         MONITOR Network > WAN - TLOC         Select Device *       R523-vEdge2000-29 (23.23.23.29)         Applications       © Chart Options -         Interface       Image: Chart Options -         VAN       Image: Chart Options -         WAN Throughput       Image: Chart Options -         Flows       Image: Chart Options -         Top Talkers       Image: Chart Options -         WAN       Image: Chart Options -         Tunnel       Image: Chart Options -         Security Monitoring       Image: Chart Options -         Firewall       Image: Chart Options -         Intrusion Prevention       Image: Chart Options -         Ukl. Filtering       Advanced Malware         Protection       Image: Chart Options -	Implications       Implications         Interface       Implications         WAN       Implications         Interface       Implications         Top Talkers       Implications         Intrusion Prevention       Implication         Intrusion Prevention       Implication         URL Filtering       Implication         Advanced Malware       Implication         Protection       Implication	ctube/c       Cisco VManage         MONITOR       Network > WAN - TLOC         Select Device Y       R523-sEdge2000-29 [23.23.23.25]         Select Device Y       R523-sEdge2000-29 [23.23.23.27]         Device Model: VEdge 2000 •       •         Applications       •         Interface       •         Percentage       •         Cisco VManage       •         WAN Throughput       •         Top Takers       •         VAN       •         Top Takers       •         VAN       •         Tunel       •         Security Monitoring       •         Firewall       •         Intrusion Prevention       •         Vick. Filtering       •         Advanced Malware       •         Protection       •         •       •         •       •         •       •         •       •         •       •         •       •         •       •         •       •         •       •         •       •         •       •         •<	Cisco vManage           MONITOR Network > WAN-TLOC           Select Device ·         F523-#56gbc2000-29 [22 22 22 29]         Ste ID 23         Device Model: vEdge 2000         Image: Control of the control of	Cisco Manage         Image: Cisco Manage	Cisco Visco WA-Tico   Select Device I Residence I   Reprice Residence I   Perfector Residence I   TCP Optimization Residence I   WAN Rows   Top Takers Image I   Image I Image I   Top Takers Image I   Image I<

## Procedure 3. View the WAN transport tunnel characteristics for the WAN Edge device

Step 1. Monitor WAN transport Tunnel characteristics for the WAN Edge device

To view the tunnel characteristics on the WAN Edge device, navigate to vManage, **Monitor > Network > WAN -**Edge. click on the WAN Edge device.

=	cisco vManage										۵	ê 🍋	0	admin 👻
-	WAN - Edge Colocation (	Clusters												
-	VPN GROUP	VPN SEGME	INT											
\$	Select VPN Group	All segn	nents											
≺ €	Device Group All +	٩		Search Options 🗸									Tot	al Rows: 14
**	Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID+	BFD	Control	Version	Up Sin	ce	Device G	roups
-	ENT19-vmanage	11.11.11.21	vManage	24b0ba05-b599-45d9-a00a-3dee8	0	reachable	21	-	12	19.2.099	15 Jan	2020 4:34:00 PM PST	"No grou	ps"
w	🔀 RS21-vEdge1000-33	21.21.21.33	vEdge 1000	110G621194126J	0	reachable	21	17	2	19.2.099	25 Jan	2020 1:15:00 PM PST	"No grou	ps"
	RS21-vEdge1000-34	21.21.21.34	vEdge 1000	110G408180039	0	reachable	21	16 (17)	2	19.2.099	25 Jan	2020 1:15:00 PM PST	"No grou	ps"
	ENT19-vbond	13.13.13.23	vEdge Cloud (vBo	0a0e0ce1-da1a-4f4d-ac6d-56983	0	reachable	23	-	-	19.2.099	15 Jan	2020 4:34:00 PM PST	"No grou	ps"
	B RS23-vEdge2000-29	23.23.23.29	vEdge 2000	260E134323003AM	0	reachable	23	19	2	19.2.099	25 Jan	2020 1:24:00 PM PST	"No grou	ps"



≡	cisco VManage				▲ Ê	<b>"</b> 2	0	admin 🔫
	MONITOR Network >	System Status						
	Select Device 👻	RS23-vEdge2000-29   23.23.23.29 Site ID: 23 Device Model: vEdge 2000 ()						
	Applications	🕑 Reboot	4	Crash				
\$	Interface							
٩	TCP Optimization	(c) Module	۲	Power Supply (Total 1)		0 8	1 📀	
<b>2</b>	WAN Throughput	8 Temperature Sensors	0	Fans (Total 4)		0	1	
<u> </u>	Flows			Tray 1		ø	õ	
•	Top Talkers	↓ USB	8	Tray 2		0	0	
	WAN			Tray 3			-	
	TLOC	CPU & Memory			FReal Time 1h 3h	6h 12h 2	h 7days	Custom 👻
	1200	100 %						
	Tunnel							

Select the Tunnel Endpoints from the list and view the path characteristics – **Jitter, Loss, Latency** for all transports (mpls, public-internet).

cisco Cisco vManage								● Ê	<b>*</b> ® Ø	
	WAN - Tunnel									
Select Device 🝷	RS23-vEdge2000-29   23.23.23.29 Site ID: 23 Device Model: vEdge 2000	0								
Applications	🖬 Chart Options 👻						🔻 Re	eal Time 1h 3	h 6h 12h <mark>24h</mark> 7d	lays Custom
Interface	75 %								Legend	
	ige								RS23-vEdge2000	)-29:mpls-RS0 s[IPSEC]
TCP Optimization	11 50 %								RS23-vEdge2000	)-29:public-
WAN Throughput	2 S 25 %						/		internet-RS02-ISF internet[IPSEC]	R4331-19:publ
Flows	2					1				
Top Talkers	0	••••	••••	••••	••••	•••••	••••			
Top Tainers	ate									
WAN	ery R.									
TLOC	Recov									
Tunnel	Loss									
Couvrity Monitoring	E C									
Security Monitoring	Feb 21, 20:00 Feb 21, 22:00 Feb 22, 00:00 Feb 22, 02:00 Feb 2	22, 04:00 Feb 2	2, 06:00 Fel	22, 08:00 Feb	22, 10:00 Feb	22, 12:00 Feb 22, 14:00	Feb 22, 16:00 Fel	b 22, 18:00		
Firewall										
Intrusion Prevention	2 Rows Selected									0e
URL Filtering	Q Search Opt	ions 🗸							Tot	tal Rows: 19
Advanced Melware	↓ Down (0) 🕓 Init (0) 个 Up (19)									
Protection	V Tunnel Endpoints	Protocol	State	Jitter (ms)	Loss (%)	FEC Loss Recovery (%)	Latency (ms)	QoE Score	Total Tx Bytes	Total Rx
Umbrella DNS Re-direct	✓ public-internet									
	RS23-vEdge2000-29:public-internet-RS06-ASR1001HX-03	IPSEC	$\uparrow$	0.20	8.44	N/A	11.69	9.00	0 B	0 B
Control Connections	RS23-vEdge2000-29:public-internet-RS05-ASR1001X-04:p	IPSEC	$\uparrow$	0.19	8.41	N/A	11.51	9.00	0 B	0 B
System Status	RS23-vEdge2000-29:public-internet-RS05-ASR1001X-05:p	. IPSEC	$\uparrow$	0.19	8.34	N/A	11.65	9.00	0 B	0 B
Events	RS23-vEdge2000-29:public-internet-RS03-C1116P-15:pub	IPSEC	$\uparrow$	0.20	8.39	N/A	11.73	9.00	0 B	0 B
	RS23-vEdge2000-29:public-internet-RS02-ISR4331-18:pu	IPSEC	$\uparrow$	0.19	8.43	N/A	11.63	9.00	0 B	0 B
ACL Logs	RS23-vEdge2000-29:public-internet-RS02-ISR4331-19:pu	IPSEC	$\uparrow$	0.19	8.39	N/A	11.80	9.00	0 B	0 B
Traublasheating	RS23-vEdge2000-29:public-internet-RS01-ISR4431-22:pu	IPSEC	*	0.20	8.48	N/A	11.79	9.00	0 B	0 B

By default, the value is shown for 24hours, but can be changed.

The chart can be changed to view the **Latency/Jitter** path characteristics by selecting the appropriate option form the **Chart Options** option as shown below.



# Process: Monitor the Application-Aware Routing Statistics

**Procedure 1.** View the Application-Aware routing statistics across the SD-WAN environment

Application Aware statistics can be monitored for each WAN transport in the SD-WAN environment from vManage GUI.

Step 1. Monitor the Application-Aware Routing across the SD-WAN environment.

To view the tunnel characteristics across the SD-WAN infrastructure, navigate to vManage >Dashboard > Main Dashboard > Application-Aware Routing widget.

≡	cisco vManage										•	Ê	<b>≜</b> ®	Ø	admin 🔻
:	Dashboard	SHBOARD													
▫	Main Dashboard			11 ↑			1↑		<b></b> 1 <b>o</b>		Reboot	0	Ø	Warning	0
\$	VPN Dashboard	1		WAN Edge - 11			vBond - 1		vManag	e - 1	Last 24 hrs	0		invalid	
٩	Security				Site H	lealth (Total 7)	)			Transpo	ort Interface Dis	ribution			
÷	Control Up			11	0	Full WAN Co	nnectivity		4 sites	< 10 M	bps				94
*	Partial			0	0	Partial WAN	Connectivity		3 sites	100 M	bps - 500 Mbps				0
	Control Down			0	0	No WAN Cor	nnectivity		0 sites	> 500	Vbps				0
											`	/iew Perce	nt Utilization		
	WAN Edge Inventory				WAN	Edge Health (1	Fotal 11)			Transpo	ort Health			Type: By Loss	• <del>•</del> = 0
	Total			14		$\frown$	$\frown$			100 %					
	Authorized			14		8)	3		0	50 %					
	Deployed			11		$\checkmark$									
	Staging			0		Normal	Warning		Error	0	••••••	••••	••••		
	Top Applications			∓ 0	Appli	cation-Aware F	Routing							Туре: Ву	Loss 💠 🖂
						Tunnel Endp	oints	Avg.	Latency (ms)	A	/g. Loss (%)		Avg. Jitte	er (ms)	
					~	RS05-ASR10	01X-04:public-internet-RS21-vE.	. 0.33	7	34	1.586		0		
		No data to disp	play		~	RS05-ASR10	01X-04:public-internet-RS21-vE.	. 0.34		34	.226		0		
					~	RS05-ASR10	01X-04:public-internet-RS23-vE.	. 0.33	3	34	1.084		0		

**Step 2.** expand the widget by clicking the square icon in the top right corner of the Application-Aware Routing widget and select the **Chart options** to view the **Loss Percentage, Latency, Jitter** as far as past 7 days on the WAN transports.

Application-Aware Routing					×
🖪 Chart Options 👻				1h 3h 6	ih 12h <mark>24h</mark> 7days
Loss Percentage/FEC Loss Recovery Rate				Legend	
C Latency/Jitter				RS05-ASR10 internet-RS2 34:public-int	101X-04:public- 1-vEdge1000- ernet
				RS05-ASR10 internet-RS2 29:public-int	101X-04:public- 3-vEdge2000- ernet
ss Recover Rate				RS05-ASR10 internet-RS2 33:public-int	101X-05:public- 1-vEdge1000- ernet
ې ۲۰۰۵ کې Apr 05, 21:00 Apr 06, 00:00 Apr 06, 03:00 Apr 06, 06	5:00 Apr 06, 09	1:00 Apr 06, 12	2:00 Apr 06, 15:00	RS06-ASR10 internet-RS2 34:public-int	101HX-03:public- 1-vEdge1000- ernet
10 Rows Selected					0
Q Search Option	ns 🗸				Total Rows: 25
✓ Tunnel Endpoints	Jitter (ms)	Loss (%)	FEC Loss Recovery (%)	Latency (ms)	QoE Score
✓ public-internet					
RS21-vEdge1000-33:public-internet-RS01-ISR4431-21:pu	0.01	29.32	N/A	0.83	6.00
RS06-ASR1001HX-03:public-internet-RS21-vEdge1000-34	0.00	32.47	N/A	0.36	5.00
RS21-vEdge1000-33:public-internet-RS02-ISR4331-18:pu	0.01	29.25	N/A	0.81	6.00
RS23-vEdge2000-29:public-internet-RS02-ISR4331-18:pu	0.01	28.70	N/A	0.86	6.00
	0.00	00.57		0.00	5.00

### Procedure 2. View the Application-Aware routing statistics for the WAN Edge device

Step 1. Monitor the Application-Aware Routing statistics specific for the WAN Edge health.

To view the tunnel characteristics across the SD-WAN infrastructure, navigate to vManage > Dashboard > Main Dashboard > Application-Aware Routing widget.

Expand the widget by clicking the square icon in the top right corner of the Application-Aware Routing widget and select the **Chart options** to view the **Loss Percentage**, **Latency**, **Jitter**. Search the WAN Edge device in the search options and select the transports to view in the chart



Step 2. View the App-route statistics on the WAN Edge device.

To view the App-route statistics, navigate to **vManage** > **Tools** > **SSH Terminal.** Select the WAN Edge device and issue **show sdwan app-route stats** on IOS-XE SD-WAN platform and **show app-route stats** on vipteal platform.

Image:																				
Image: Control Signer Transmit         15151525 x 2.22.19 x 222.237 x           Image: Control Signer Transmit         15151525 x 2.22.19 x 222.237 x           Image: Control Signer Transmit         15151525 x 2.22.19 x 222.237 x           Image: Control Signer Transmit         15151525 x 2.22.19 x 222.237 x           Image: Control Signer Transmit         Image: Control Signer Transmit           Image: Contramati         Image: Control Signer Transmit <th></th> <th>cisco VManage</th> <th></th> <th>•</th> <th>Ê</th> <th><b>*</b></th> <th>0</th> <th></th>		cisco VManage														•	Ê	<b>*</b>	0	
Device Group         I 1515125 x         2.22.219 x         2.22.22.37 x           A         I         I 1515125 x         2.22.19 x         2.22.22.37 x           A         I         I 1515125 x         2.22.19 x         2.22.21.37 x           C         I         I 1515125 x         2.22.19 x         2.22.21.37 x           C         I         I 1515125 x         2.22.19 x         2.22.21.37 x           C         I         I 1515125 x         2.22.19 x         2.22.21.37 x         I 1515125 x         2.22.19 x           C         I         I 1515125 x         2.22.19 x         I 1515125 x         2.22.21 x         I 1515125 x         2.22.21 x           D11.22.1 Simulation (I         I 151512 x         2.22.19 x         I 1515125 x<	::	K TOOLS   SSH TERMINAL																		
Al       •       No. 1000000000000000000000000000000000000		Device Group	<	15.15.15.25	×	2.2.2.19	× 23	.23.23.29	×											
Q.	_	All	٠	RS23-vEdge2000	-29# s	how app-ro	oute stats	s remote-s	ystem-ip	ip 2.2.2.	2.19									
Gerl V Mashhadiry C       Incl exclore       public - taktrack         In 1.1.21 [Brendball       Incl exclore       public - taktrack         R801-1868441-22       IIII A21 [Brendball       IIII A21 [Brendball         R801-1868441-22       IIII A21 [Brendball       IIII A21 [Brendball         R802-1868431-18       IIII A21 [Brendball       IIII A21 [Brendball         R802-1868431-19       IIIII A21 [Brendball       IIII A21 [Brendball         R802-1868431-19       IIII A21 [Brendball       IIII A21 [Brendball         R802-1868431-19       IIIII A21 [Brendball       IIIII A21 [Brendball         R802-1868431-18       IIIII A21 [Brendball       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	<b>\$</b>			app-route stat remote-system	istics -ip 2.	10.5.207. 2.2.19	110 10.5	.207.38 ip	sec 1236	866 12366	66									
Bits // Beachabity @ IE         Beachabity @ IE         Beachabity @ IE         Beachabity @ IE           11121 // Beachabit         Interview         6	٩	Q	~	local-color remote-color	pu pu	blic-inter blic-inter	net net													
1.1.1.21 [se lb :111       maximude       maximude       maximude         8.00.1-804431-22       (SD44)       (SD44)       maximude       maximude         8.00.1-804431-22       (SD44)       maximude       Maximude       Maximude       Maximude         8.00.1-804431-22       (SD44)       maximude       Maximude       Maximude       Maximude         8.00.1-804431-16       (SD44)       (SD44)       Maximude       Maximude       Maximude         2.2.2.19 [SB40]       (SD44)       (SD44)       Maximude       Maximude       Maximude         2.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       Maximude         2.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)         2.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)         3.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)         3.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)         3.2.2.19 [SB40]       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44)       (SD44) <td< td=""><td><b>A</b></td><td>Sort by Reachability \$</td><td>te.</td><td>mean-loss mean-latency</td><td>49 0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	<b>A</b>	Sort by Reachability \$	te.	mean-loss mean-latency	49 0															
Republic Astronomy       Special Security       Special Security       Special Security       Special Security         TOTAL       AVEBARE       AVEBARE       AVEBARE       Special Security       Special Security         Response       Special Security       Special Security       Special Security       Special Security       Special Security       Special Security         Response       Special Security		1.1.1.21   Site ID: 111 Reachable		mean-jitter	0															
Note:         Note: <th< td=""><td>*</td><td>RS01-ISR4431-22</td><td>ISR4431</td><td>514-01455-1H4</td><td>CA V</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>	*	RS01-ISR4431-22	ISR4431	514-01455-1H4	CA V															
BSO2-ISR433-14       (ISR43)         2.2.18 Is UP: D22       ISR433         Reschable       ISR433         Paschable       ISR443         Paschable		Reachable		INDEX PACKETS	LOSS	LATENCY	JITTER	TK DATA PKTS	PKTS	~										
Reschable       1       56       278       0       0       0       0         Reschable       5       56       20       0       0       0       0         Reschable       5       56       20       0       0       0       0         Reschable       C1116-P       5       56       25       0       0       0       0         Reschable       C1116-P       5       56       25       0       0       0       0         Reschable       C1116-P       5       56       10.5.20B.JB [pisse: 12346 12366       10.5.20B.JB [pisse: 12346 12366         Reschable       C1116-P       pp-roote statistics       10.5.20B.JB [pisse: 12346 12366       10.5.20B.JB [pisse: 12346 12366         Reschable       C1116-P       ps-roote statistics       10.5.20B.JB [pisse: 12346 12366       10.5.20B.JB [pisse: 12346 12366         Reschable       Cost = cost = psiss = roote = psis		RS02-ISR4331-18 2.2.2.18   Site ID: 222	ISR4331	0 596	302															
R502-ISRA331-19       ISRA33       3       3.56       3.03       0       0       0       0         2.2.2.19       ISBED 222       0       0       0       0       0       0         R633-C118-75       0.556       2.25       0       0       0       0       0         R633-S11001X-04       ASR1001X-04       ASR1001X-05       ASR100X-05 <td></td> <td>Reachable</td> <td></td> <td>1 596 2 596</td> <td>278 284</td> <td></td>		Reachable		1 596 2 596	278 284															
Reschable       5       56       29       0       0       0         Ro30-C116P-15 Reschable       C1164P       app-coute statistics 10.5.208.66 10.5.208.38 jpsec 12346 12366 remote-system-1p 2.2.2.3         Ro55-ASR1001X-05 S 5.5.5 1 Site ID:55 Reschable       ASR1001X-05 Reschable       ASR1001X-07 Reschable       ASR1001X-07 RESCHABLE ASR1000-07 RESCHABLE ASR1001X-07 RESCHABLE ASR1000-07 RESCHABLE ASR1000-07 RES		RS02-ISR4331-19 2.2.2.19   Site ID: 222	ISR4331	3 596 4 596	303 319															
R3.3.15       Stel D: 33 Reschable       Cifferen Stel D: 33 Reschable       ASR1001-X Reschable       ASR10-X Reschable       ASR10-X Reschable       ASR10-X Reschable		Reachable	01116.40	5 596	295															
Nethoday     ASR1001X-04 Sto55.41     ASR1001X-05 Sto55.41     AVERAGE AVERAGE AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto56.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE X DATA TIOEX PACKETS LOSS LATENCY JITTER PXTS PKTS Sto60.0     D TOTAL     AVERAGE		3.3.3.15   Site ID: 333	C1110-4P	app-route stat	istics	10.5.208.	66 10.5.	208.38 ips	ec 12346	16 12366	6									
S 5.5 4 1 Stel (D: 555       mean-loss       me		RS05-ASR1001X-04	ASR1001-X	local-color	mp	ls														
Rass       ASRI01-X-05       ASR1001-X-05       ASR1001-X-05       ASR1001-X-05       Bean-litter: 0       Bean-litter: 0         S.S.S.S.I StelD.555       Res.       ASR1001-X       Mala-class-index       0,1         Reschable       TOTAL       AVERAGE XVERAGE TX DATA       RX DATA         Reschable       TOTAL       AVERAGE XVERAGE TX DATA       RX DATA         Reschable       TOTAL       AVERAGE XVERAGE TX DATA       RX DATA         Reschable       TNDEX PACKETS Loss LATENCY JITTER       PXTS       PXTS         Reschable       0       556       0       0       0         12.12.12.31 SiteID.21       156       0       0       0       0         21.21.21.31 SiteID.21       VEdge 1000       2       556       0       0       0         21.21.21.31 SiteID.21       VEdge 1000       4       596       0       0       0       0         21.21.21.31 SiteID.21       VEdge 2000-29#       VEdge 2000-29#       NE Site 2-VEdge 2000-29#       NE Site 2-VEdge 2000-29#       NE Site 2-VEdge 2000-29#         21.21.21.21.21.21.21 SiteID.22       VEdge 2000-29#       NE Site 2-VEdge 2000-29#       NE Site 2-VEdge 2000-29#         21.21.21.21.21.21.21.21.21.21.21.21.21.2		5.5.5.4   Site ID: 555 Reachable		mean-loss	mp. 0	15														
S.S.S. S. S.S. S. S. S. S. S. S. S. S. S		RS05-ASR1001X-05	ASR1001-X	mean-latency mean-jitter	0															
RS06-ASR1001HX-03 6.6.3 I Stel D.660       ASR1001+X INDEX       AVERAGE       XVERAGE		5.5.5.5   Site ID: 555 Reachable		sla-class-ind	ex 0,															
6.6.3 I Site ID. 666     0     0     0     0       Rechable     0     596     0     0     0       121.72.13.3 I Site ID. 21     2     596     0     0     0       Rechable     3     596     0     0     0       Rechable     3     596     0     0     0       Rechable     3     596     0     0     0       RS21-vEdge1000-34     vEdge 1000     2     596     0     0     0       121.72.13.4 I Site ID. 21     vEdge 2000-29#     vEdge2000-29#     vEdge2000-29#     vEdge2000-29#       RS23-vEdge2000-29     vEdge2000-29#     RS23-vEdge2000-29#     RS23-vEdge2000-29#		RS06-ASR1001HX-03	ASR1001-HX	TOTAL INDEX PACKETS	LOSS	AVERAGE LATENCY	AVERAGE JITTER	TX DATA PKTS	RX DATJ PKTS	£λ										
RS21-vEdge1000-33       vEdge 1000       1       596       0       0       0         Z1:Z1:Z1:33       Site ID:21       3       596       0       0       0       0         Reachable       3       596       0       0       0       0       0         Rs21-vEdge1000-34       vEdge 1000       4       596       0       0       0       0         Z1:Z1:Z1:A1       Site ID:21       vEdge 1000       4       596       0       0       0       0         Rs21-vEdge2000-29       vEdge 2000       3       596       0       0       0       0         Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z2:Z		6.6.6.3   Site ID: 666 Reachable		 0 596																
Racchable     3     556     0     0     0       Rs21+vEdge1000-34     vEdge 1000     4     556     0     0     0       21.21.21.31.41     Sitel D: 21     Sitel D: 21     Sitel D: 21     Sitel D: 21     Sitel D: 22     Sitel D: 23     NEdge 2000-29#       RS22+vEdge 2000-29     VEdge 2000-29#     RS22+vEdge 2000-29#     RS22+vEdge 2000-29#       RS22+vEdge 2000-29#     RS22+vEdge 2000-29#     RS22+vEdge 2000-29#		RS21-vEdge1000-33	vEdge 1000	1 596	0	0		0												
R521-vEdge1000-34       vEdge 1000       4       556       0       0       0       0         21:21:21:34       (Stel):21       5       56       0       0       0       0         Reschable       823-vEdge2000-39#       R523-vEdge2000-39#       R523-vEdge2000-39#       R523-vEdge2000-39#       R523-vEdge2000-39#         Reschable       823-vEdge2000-39#       R523-vEdge2000-39#       R523-vEdge2000-39#       R523-vEdge2000-39#		Reachable		3 596																
Reschuble         R523-vEdge200-29           R523-vEdge200-29         vEdge200-29           R523-vEdge200-29         R523-vEdge200-29           Reschuble         R523-vEdge200-29           Reschuble         R523-vEdge200-29		RS21-vEdge1000-34	vEdge 1000	4 596 5 596	0			0												
R523+vEdge2000-29         vEdge 2000         R623-vEdge3200-29#           232323239         Sint ID:23         R623-vEdge3200-29#           Reachable         R523-vEdge2000-29#		Reachable		RS23-vEdge2000	-29#															
Reschable 2523-vr2dgo2000-29#		RS23-vEdge2000-29 23.23.23.29   Site ID: 23		RS23-vEdge2000 RS23-vEdge2000	-29# -29#															
		Reachable		RS23-vEdge2000	-29#															

≡	cisco vManage											•	ġ	<b>*</b>	0	admin 👻
	K TOOLS   SSH TERMINAL	-														
ᆸ	Device Group	<	15.15.15.25	×	2.2.2.19	×										
<b>Å</b>	All	÷	RS02-ISR4331-19 app-route stati	stics	wan app-r 10.5.207.	oute stat 38 10.5.2	s remote- 07.110 ip	system-ip sec 12366	23.23.23	.29						
T a	Q	~	remote-system- local-color	ip 23. pub	23.23.29 lic-inter	net										
	Sort by Reachability \$	te.	mean-loss mean-latency	50 0	11C-inter	net										
	ENT19-vmanage 11.11.11.21   Site ID: 21	vManage	mean-jitter sla-class-inde	0 x 0					IPV6 TX	IPV6 RX						
0	ENT19-vsmart1 15.15.15.25   Site ID: 25 Reachable	vSmart	TOTAL INDEX PACKETS	LOSS	AVERAGE LATENCY	AVERAGE JITTER	TX DATA PKTS	RX DATA PKTS	DATA PKTS	DATA PKTS						
	ENT19-vbond 13.13.13.23   Site ID: 23 Reachable	vEdge Cloud vBond	0 663 1 661 2 665 3 666	315 339 344 339												
	RS01-ISR4431-21 1.1.1.21   Site ID: 111 Reachable	ISR4431	4 663 5 663	319 337												
	RS01-ISR4431-22 1.1.1.22   Site ID: 111 Reachable	ISR4431	app-route stati remote-system- local-color remote-color	stics ip 23. mpl mpl	10.5.208. 23.23.29 8	38 10.5.2	08.66 ips	ec 12366	12346							
	RS02-ISR4331-18 2.2.2.18   Site ID: 222 Reachable	ISR4331	mean-latency mean-jitter	0 0 0												
	RS02-ISR4331-19 2.2.2.19   Site ID: 222 Reachable	ISR4331	sla-class-inde TOTAL INDEX PACKETS	x 0,1	AVERAGE	AVERAGE	TX DATA PKTS	RX DATA PKTS	IPV6 TX DATA PKTS	IPV6 RX DATA PKTS						
	RS03-C1116P-15 3.3.3.15   Site ID: 333 Reachable	C1116-4P	0 664 1 665													
	RS05-ASR1001X-04 5.5.5.4   Site ID: 555 Reachable	ASR1001-X	2 661 3 665 4 662 5 662													
	RS05-ASR1001X-05 5.5.5.5   Site ID: 555 Reachable	ASR1001-X	RS02-ISR4331-19	♥ #Conne	ction to	192.168.1	.6 closed	by remot	e host.							
	RS06-ASR1001HX-03 6.6.6.3   Site ID: 666	ASR1001-HX	Connection to 2 Session closed.	.2.2.1	9 closed.											

# Process: Monitor Events – SLA, BFD, App-route changes

## Procedure 1. View the Events - SLA, BFD, App-Route

Application-Aware routing specific events related to SLA changes, BFD events, and App-route events can be monitored across the SD-WAN environment from vManage GUI.

**Step 1.** To view the events on the WAN Edge device, navigate to **vManage > Monitor > Network > WAN - Edge**. click on the specific WAN Edge device.

≡	cisco vManage										۵	ê 🍂	Ø	admin 🔫
	MONITOR   NETWORK													
	WAN - Edge Colocation (	Clusters												
	VPN GROUP	VPN SEGME	NT											
۵	Select VPN Group	✓ All segmination	ients											
∢ ≇	Device Group All +	٩		Search Options 🗸										O C C
**	Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID↑	BFD	Control	Version	Up Sin	ce	Dev	vice Groups
	ENT19-vmanage	11.11.11.21	vManage	24b0ba05-b599-45d9-a00a-3dee8	0	reachable	21	-	12	19.2.099	15 Jan	2020 4:34:00 PM PS	T "No	o groups"
w	BRS21-vEdge1000-33	21.21.21.33	vEdge 1000	110G621194126J	0	reachable	21	17	2	19.2.099	25 Jan	2020 1:15:00 PM PS	T "No	o groups"
	8 RS21-vEdge1000-34	21.21.21.34	vEdge 1000	110G408180039	0	reachable	21	16 (17)	2	19.2.099	25 Jan	2020 1:15:00 PM PS	T "No	o groups"
	ENT19-vbond	13.13.13.23	vEdge Cloud (vBo	0a0e0ce1-da1a-4f4d-ac6d-56983	0	reachable	23	-	-	19.2.099	15 Jan	2020 4:34:00 PM PS	T "No	o groups"
	BRS23-vEdge2000-29	23.23.23.29	vEdge 2000	260E134323003AM	0	reachable	23	19	2	19.2.099	25 Jan	2020 1:24:00 PM PS	T "No	o groups"





**Step 3.** Click **Filter > Filter By > Component.** choose **BFD**, **App-route** from the drop-down options and click **Search**.

≡	cisco vManage	•	Ê	<b>≜</b> 129	0	admin 👻
	MONITOR Network >	Events				
_	Select Device 👻	RS23-vEdge2000-29   23.23.23.29 Site ID: 23 Device Model: vEdge 2000 ()				
	Applications	≂ Filter +	1h	3h 6h 12h	24h 7days	Custom -
\$	Interface	Filter By				
a	interface	Severity Select Severity				
	TCP Optimization		-			
÷	WAN Throughput	Component BFD × App-Route ×		Critical		
÷	Flows	Event name Select Event name		Minor		
1	Top Talkers	Reset All Close				
	WAN					
	TLOC					

Alternatively, you can also filter on Event Name as shown below

≡	Cisco vManage	•	6	€ <b>≜</b>	0	admin 👻
::	MONITOR Network >	Events				
_	Select Device 👻	RS23-vEdge2000-29   23.23.23.29 Site ID: 23 Device Model: vEdge 2000 ()				
<u> </u>	Applications	Filter → Component: BFD, App-Route	1h	n 3h 6h 12h	24h 7days	Custom 👻
\$	Interface	Filter By				
3	TCP Optimization	Severity Select Severity		Legend		
÷	WAN Throughput	Component Select Component		Critical Major		
÷	Flows	Event name bfd-state-change × sla		Minor		
1	Top Talkers	sla-change           Reset All         sla-violation				
	WAN	0 sla-violation-pkt-drop				
	TLOC	ро <sup>0,00</sup> , <b>sla</b> -config				



Step 4. Click the three dots on the right hands side of the event to view more details of the event



## Process: Visualize traffic path selection on the WAN Edge

## Procedure 1. Visualize real-time Application-Aware routing enforcement in vManage

vManage has a very useful tool for network administrators to simulate traffic on the Service side on the Viptela platform and view the traffic path taken on the WAN Edge to confirm the desired policy enforcement.

**Step 1.** Simulate the traffic flow from service side to remote branch service site with App-Aware routing enabled.

In vManage, navigate to **Monitor > Network.** Select the WAN Edge device and click the **Troubleshooting** option from the left-side panel. Click **Traffic** section > **Simulate Flows** 

=	Cisco vManage	e .	📥 📋 🔎 🥝 admin 🕶
	MONITOR Network	> Troubleshooting	
	Select Device 🝷	RS23-vEdge2000-29   23.23.23.29 Site ID: 23 Device Model: vEdge 2000	
-	TCP Optimization		
₽	WAN Throughput		
عر	Flows		
÷	Top Talkers		
*	WAN	Connectivity	Traffic
	TIOC		
	Turnel		
	Coourity Monitoring		
	Security Monitoring		
	Firewall		· · · · · · · · · · · · · · · · · · ·
	Intrusion Prevention		
	URL Filtering	Device Bringup	Tunnel Health
	Advanced Malware Protection	Control Connections(Live View)	App Route Visualization
	Umbrella DNS Re-direct	Ping	Simulate Flows
	Control Connections	Trace Route	
	System Status		
	Events		
	ACL Logs		
	Troubleshooting		
	Real Time		
	Cisco vManage		📥 🖨 💭 🤣 admin ▾
::	MONITOR Network	> Troubleshooting > Simulate Flows	
	Select Device *	KSZS-VE0geZUUU-Z9 Z3.Z3.Z3 29 Site ID: 23 Device Model: VEdge 2000	Troubleshooting -
\$	VPN* VPN - 10	Source/Interface for VPN - 10*         Source IP*         Destination           Ioopback0 - ipv4 - 10.23.23.29         Io.23.23.29         10.23.23.29         10.23.23.29	9 facetime X
4	Advanced Options >		
â			
-			Simulate
Ĩ	Output:		Total next hops: 1   IPSec : 1
		□→ 🔀 23.23.23.29	
		→ mpls	Remote System IP 2.2.2.19
		← mpts	encapsulation IPSec

**Step 2.** View the Tunnel health by navigating to vManage, **Monitor > Network**, select the WAN Edge device and click the **Troubleshooting** option from the left-side panel. Click **Traffic** section > **Tunnel Health** to view the tunnel health (**Loss percentage, Latency, Jitter**) between the WAN Edge device and the selected Remote WAN Edge device.


With Application-Aware Routing policy enabled, the WAN Edge device considers the tunnel health to forward the traffic. In the above example, the public-internet WAN transport has significant loss, Latency and doesn't meet the SLA defined. The WAN Edge is preferring the MPLS transport to forward the service-side traffic as defined in the policy.

## Appendix A: Product List

The following products and software versions are included as part of validation in this deployment guide. This validated set is not inclusive of all possibilities.

## Table 1. Cisco SD-WAN Solution

Functional area	Product	Software version
Cisco SD-WAN controllers	Cisco vManage, Cisco vSmart, and Cisco vBond controllers	19.2.099
Cisco IOS-XE SD-WAN Device	ISR4K, ASR1K	16.12.02r
Cisco vEdge Device	vEdge, vEdge 1000	19.2.099
Server	Hypervisor/vSphere client	VMware ESXi, 6.7.0, 10302608/version 6.7.0.20000

## Feedback

For comments and suggestions about this guide and related guides, join the discussion on <u>Cisco Community</u> at <u>https://cs.co/en-cvds</u>.