Cisco SD-WAN AppQoE Configuration Guide, Cisco IOS XE Release 17.x

First Published: 2020-12-19

Last Modified: 2021-06-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

CONTENTS

CHAPTER 1

Read Me First

Related References

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

User Documentation

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

Communications, Services, and Additional Information

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

Documentation Feedback

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

CHAPTER 2

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

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

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

CHAPTER 3

AppNav-XE for Cisco SD-WAN

Table 1: Feature History

Feature Name	Release Information	Description
AppNav-XE	Cisco IOS XE Release 17.2.1r	This feature lets you configure policy-based redirection of LAN-to-WAN and WAN-to-LAN traffic flows to WAAS nodes for WAN optimization on Cisco IOS XE SD-WAN devices . This feature was already available on Cisco IOS XE platforms and is being extended to Cisco IOS XE SD-WAN platforms in this release.

Overview of AppNav-XE

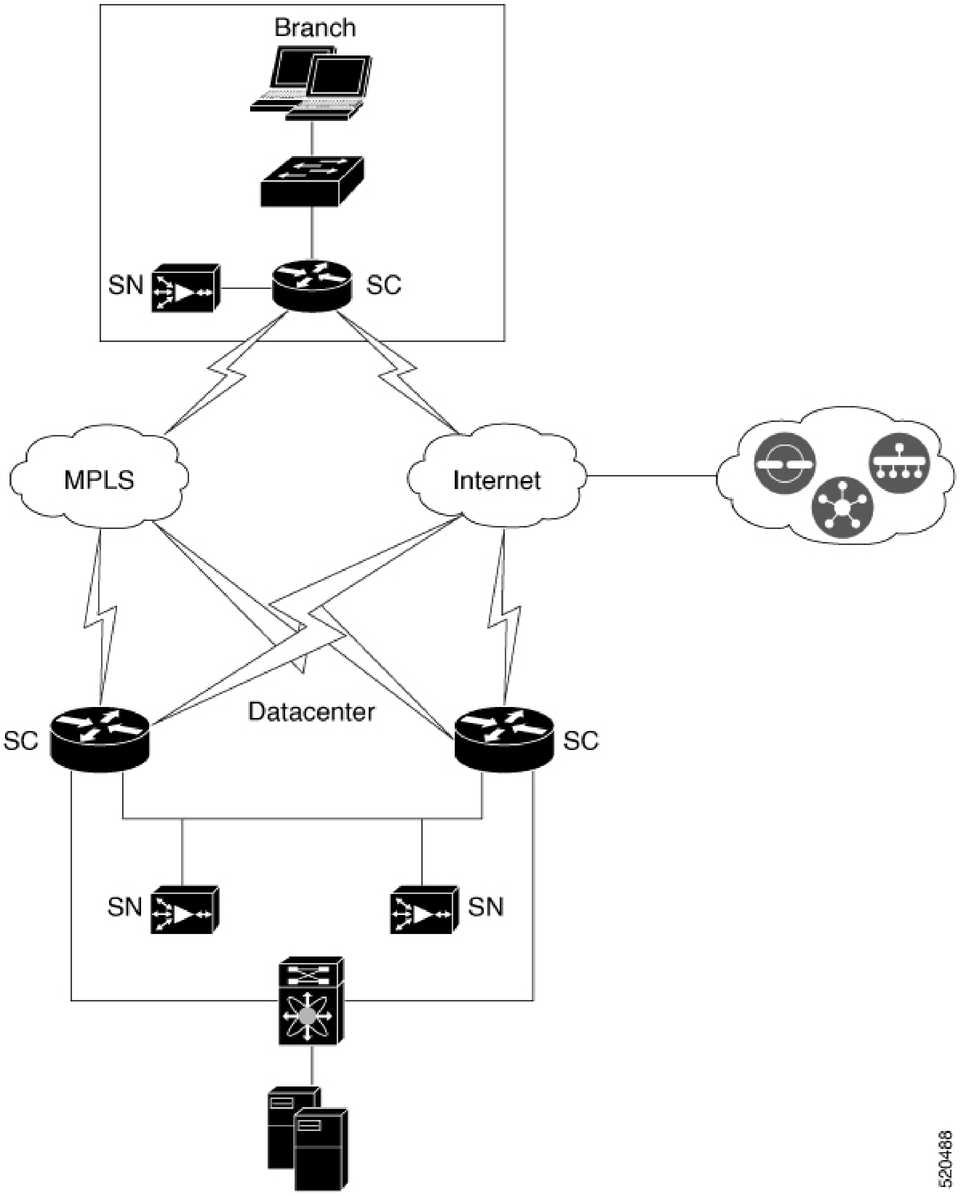
The AppNav-XE feature facilitates intelligent distribution of traffic flows to WAAS devices. WAAS devices are used for WAN optimization.

AppNav-XE reduces dependency on the intercepting router by distributing traffic among WAAS devices for optimization using a class and policy mechanism. You can use WAAS nodes (WNs) to optimize traffic based on sites and/or applications. The AppNav-XE solution can scale up to available capacity by taking into account WAAS device utilization as it distributes traffic among nodes. The solution provides high availability of optimization capacity by monitoring node overload; and by providing configurable failure and overload policies.

Note The AppNav-XE feature was already available on Cisco IOS XE platforms before it was introduced to Cisco SD-WAN in Cisco IOS XE Release 17.2. For more information, see Configuration Guide for AppNav-XE on the Cisco CSR 1000V Series and Cisco ASR 1000 Series.

Topology Example

Figure 1: Example Topology



*SN: Service nodes or WAAS nodes (up to 64)
*SC: A Cisco IOS XE SD-WAN device acting as a service controller (up to 4)

The image above shows an example of Cisco SD-WAN deployment with AppNav-XE. The Cisco IOS XE SD-WAN devices at the data center and branches are enabled with the AppNav-XE feature and form an AppNav cluster with WAAS nodes.

Benefits of AppNav-XE

- Enables enterprises to expand services efficiently and cost-effectively
- Supports the use of flexible policy definitions
- Integrated with Cisco SD-WAN network services, which eliminates the need for any additional hardware
- Intelligently redirects new flows based on the load on each service node. This also includes the load on individual L7 application accelerators
- For flows that don't require any optimization, service nodes can inform the AppNav Controller to directly pass-through the packets, thus minimizing the latency and resource utilization
- Has minimal impact to traffic when adding or removing service nodes
- Supports VRFs, so that the VRF information is preserved when traffic returns from a service node
- Supports optimization of asymmetric flows through AppNav controller groups

Note An asymmetric flow is when the traffic in one direction goes through one AppNav Controller and the return traffic goes through a different AppNav Controller; but both AppNav Controllers redirect the traffic to the same service node.

- Provides inter-router high availability to keep traffic flows uninterrupted, where if one router goes down, the traffic can be re-routed to a different router within the AppNav Controller group.

Components of AppNav-XE

- **AppNav Cluster:** A group of all AppNav controllers and WAAS nodes at a site. Typically, each enterprise site, such as branch and data center, has an AppNav cluster.
- **AppNav Controller:** A device that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more WAAS nodes (WNs) for optimization. The device in this context is a Cisco IOS XE SD-WAN device running AppNav-XE.
- **WAAS Nodes:** Wide Area Application Services (WAAS) nodes or service nodes are WAAS optimization engines or vWAAS instances that optimize and accelerate traffic based on the optimization policies configured on the device.

Note WAAS service nodes are outside the scope of this document.

- **WAAS Central Manager (WCM):** WCM devices host WCM, a Web-based interface that allows you to configure, manage, and monitor AppNav controllers and WAAS nodes in your network. In AppNav-XE for Cisco SD-WAN, WCM communicates with Cisco vManage, which is the NMS used to configure Cisco IOS XE SD-WAN devices. Cisco vManage then pushes the AppNav-XE configuration to the Cisco IOS XE SD-WAN devices. However, WAAS nodes in an AppNav cluster still receive their configuration through WCM. Monitoring of WAAS nodes and AppNav-XE on Cisco IOS XE SD-WAN devices is done directly through WCM.

- **Cisco vManage:** This is the primary management system in Cisco SD-WAN. Therefore, WCM sends the AppNav-XE configuration to Cisco vManage, which in turn pushes it to the AppNav-XE controllers.

Supported Platforms

The following platforms support AppNav-XE for Cisco SD-WAN.

- Cisco 1000 Series Aggregation Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series
- C8500-12X4QC and C8500-12X Series Aggregation Services Routers
- C8300 Series Integrated Services Routers

Managing AppNav-XE in Cisco SD-WAN

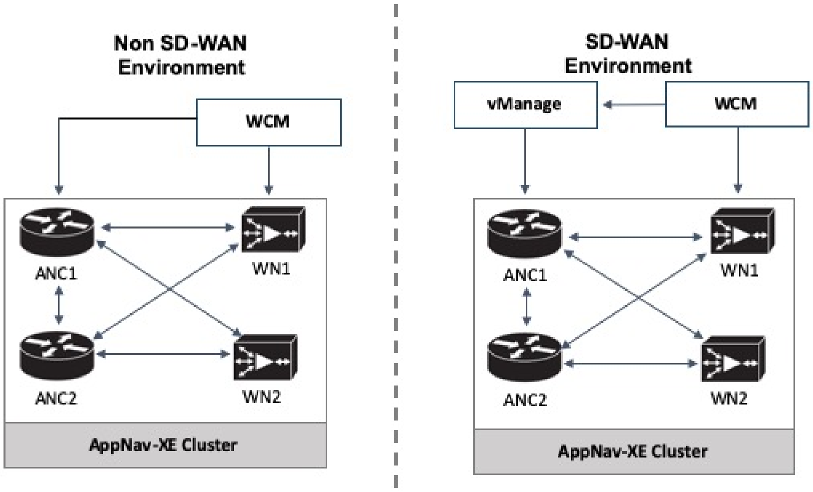
The AppNav-XE feature was already supported on IOS XE platforms. However, starting from Cisco IOS XE Release 17.2, the feature is extended to Cisco IOS XE SD-WAN platforms. Note that for this feature to work, Cisco vManage should be running Cisco SD-WAN Release 20.1.1 or later.

AppNav-XE in SD-WAN versus non-SD-WAN Environments

How AppNav-XE is configured in SD-WAN is different from how it's configured in non-SD-WAN environments. The major difference is the involvement of Cisco vManage, which acts as an intermediary between WCM and AppNav-XE controllers, to push the AppNav policy configuration to Cisco IOS XE SD-WAN devices. Cisco IOS XE SD-WAN devices act as AppNav-XE controllers.

The following image shows the differences in the deployment of AppNav-XE in SD-WAN and non-SD-WAN environments.

Figure 2: Comparison: AppNav-XE in SD-WAN versus non SD-WAN Environments



AppNav-XE in IOS XE: The WCM GUI directly communicates with the AppNav Controller (ANC) and the WAAS Nodes (WN) in the AppNav cluster to push the configuration.

AppNav-XE in IOS XE SD-WAN: The major difference is in terms of how the AppNav policy configuration is pushed to the AppNav Controllers (ANC). Here, the feature is configured through both WCM GUI and Cisco vManage. You continue to configure the AppNav-XE feature in WCM. WCM then sends the configuration to Cisco vManage, which in turn pushes the configuration to AppNav controllers. The communication between WCM and Cisco vManage is achieved through registering WCM as a third-party controller with Cisco vManage. WCM still directly sends the configuration to the WAAS nodes.

Configure AppNax-XE on Cisco IOS XE SD-WAN Devices

Perform the following procedures to configure AppNav-XE on Cisco IOS XE SD-WAN devices.

1. Register WCM in Cisco vManage
2. Attach Cisco IOS XE SD-WAN Device to WCM Partner
3. Register Cisco XE SD-WAN Device with WCM
4. Configure AppNav-XE Cluster for SD-WAN, on page 12

Register WCM in Cisco vManage

This topic describes how to access Cisco WAAS Central Manager (WCM) and register WCM as s third-party controller on Cisco vManage. It also describes how to attach an Cisco IOS XE SD-WAN device to the WCM partner through Cisco vManage.

Access the WCM GUI

To access the WAAS Central Manager GUI, enter the following URL in your web browser:

https:// *WAE_Address* :8443/

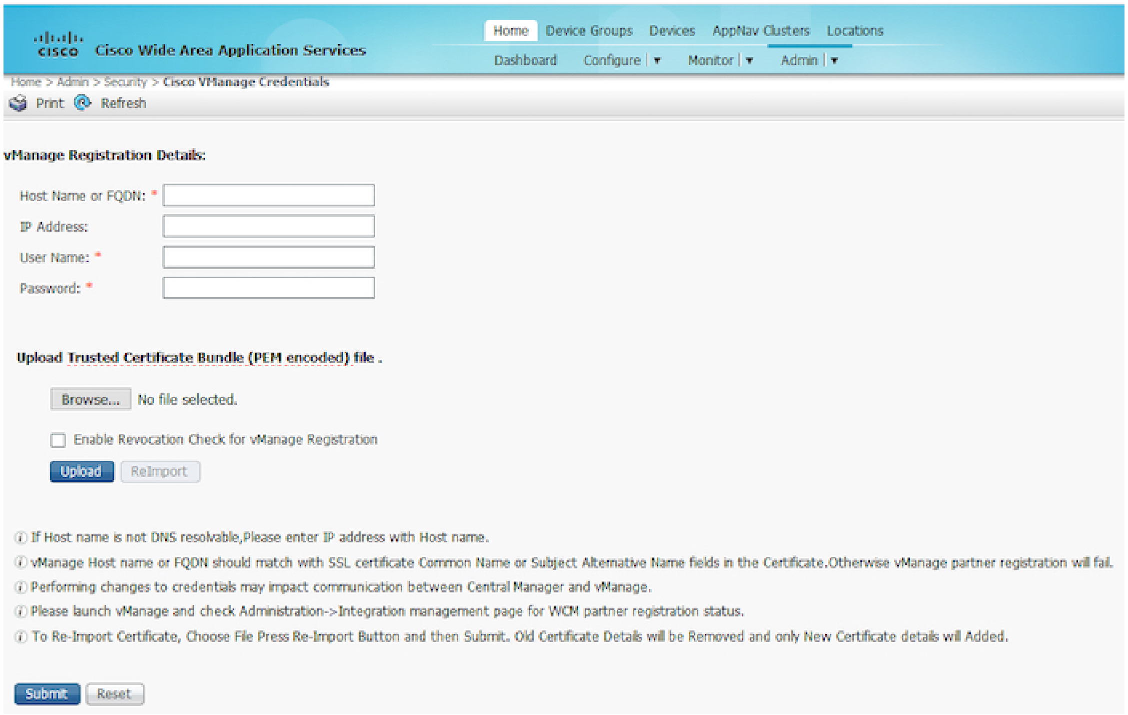
The *WAE_Address* value is the IP address or host name of the WAAS Central Manager device.

The default administrator username is *admin* and the password is *default*.

Integrate WCM with Cisco vManage

1. From the WCM GUI homepage,choose **Admin**.
2. Next, choose **Security** > **Cisco vManage Credentials**.
3. Provide the requested information.

Figure 3: WCM GUI



vManage Registration Details:

Host Name or FQDN: *

IP Address:

User Name: *

Password: *

Upload Trusted Certificate Bundle (PEM encoded) file .

No file selected.

□ Enable Revocation Check for vManage Registration

ⓘ If Host name is not DNS resolvable,Please enter IP address with Host name.

ⓘ vManage Host name or FQDN should match with SSL certificate Common Name or Subject Alternative Name fields in the Certificate.Otherwise vManage partner registration will fail.

ⓘ Performing changes to credentials may impact communication between Central Manager and vManage.

ⓘ Please launch vManage and check Administration->Integration management page for WCM partner registration status.

ⓘ To Re-Import Certificate, Choose File Press Re-Import Button and then Submit. Old Certificate Details will be Removed and only New Certificate details will Added.

To register using a Fully Qualified Domain Name (FQDN), enter the FQDN in the Host Name field. The IP Address field should remain empty.

4. Upload the trusted issuer certificate bundle in PEM format for the Cisco vManage web server certificate.

Note Use the re-import button to re-upload the trusted issuer certificate bundle, which replaces the existing certificate bundle.

5. To enable revocation check of the Cisco vManage web server certificate, choose the **Revocation Check** option.

   Note that only OSCP based revocation check is supported.

6. Click **Submit**.

Once integrated, the WCM partner can be seen from the Cisco vManage menu by choosing **Administration** > **Integration Management**.

Attach Cisco IOS XE SD-WAN Device to WCM Partner

1. From the Cisco vManage menu, choose **Administration** > **Integration Management**.

   You'll see the list of third-party controllers registered on Cisco vManage.

2. For the desired WCM partner, click **...** and choose **Attach Devices**.
3. In the **Available Devices** column on the left, choose a device from the list.
4. Click **Attach**.
5. To configure AppNav-XE on the device, Register Cisco XE SD-WAN Device with WCM next.

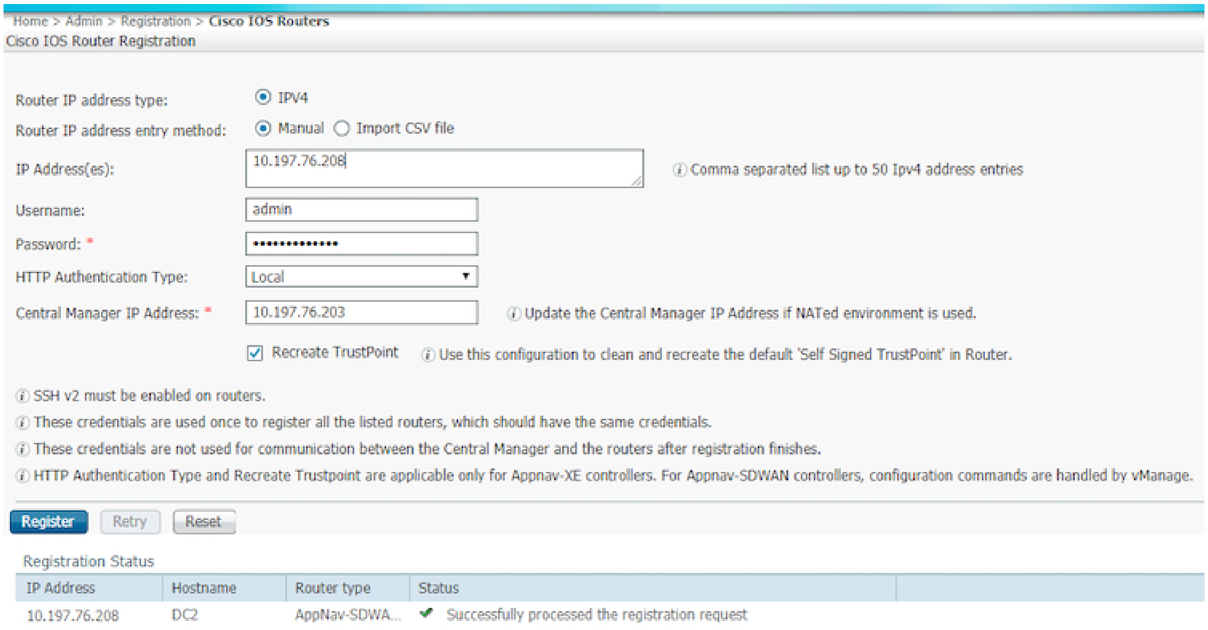
Register Cisco XE SD-WAN Device with WCM

Prerequisites

- The device being registered should be in vManage mode in the Cisco vManage GUI. For more information, see Change Configuration Modes in Cisco vManage
- The device being registered must have HTTPS configuration attached to it. The HTTPS configuration can be attached to the device using the Global Settings template in Cisco vManage.
  1. From Cisco vManage menu, choose **Configuration** > **Templates**.
  2. Click **Feature** then click **Add Template**.
  3. Under the **Basic Information** area in the right pane, choose the **Global Settings** template.
  4. Click **Services**.
  5. For both the fields—HTTP Server and HTTPS Server, from the drop-down list, choose **Global** and choose **On**.

Register the Device on WCM

1. In WCM, navigate to the **Admin** section.
2. Choose **Registration** > **Cisco IOS Routers**.
3. Enter the requested details and click **Register**.



Home > Admin > Registration > Cisco IOS Routers

Cisco IOS Router Registration

Router IP address type: ● IPV4

Router IP address entry method: ● Manual ○ Import CSV file

IP Address(es): 10.197.76.208 — ⓘ Comma separated list up to 50 Ipv4 address entries

Username: admin

Password: * •••••••••••••

HTTP Authentication Type: Local

Central Manager IP Address: * 10.197.76.203 — ⓘ Update the Central Manager IP Address if NATed environment is used.

☑ Recreate TrustPoint — ⓘ Use this configuration to clean and recreate the default 'Self Signed TrustPoint' in Router.

ⓘ SSH v2 must be enabled on routers.

ⓘ These credentials are used once to register all the listed routers, which should have the same credentials.

ⓘ These credentials are not used for communication between the Central Manager and the routers after registration finishes.

ⓘ HTTP Authentication Type and Recreate Trustpoint are applicable only for Appnav-XE controllers. For Appnav-SDWAN controllers, configuration commands are handled by vManage.

Registration Status

IP Address	Hostname	Router type	Status
10.197.76.208	DC2	AppNav-SDWA...	✓ Successfully processed the registration request

The registration status of the device is displayed in the lower part of the screen.

4. Click **Submit**.

Configure AppNav-XE Cluster for SD-WAN

The configuration of AppNav-XE clusters for Cisco SD-WAN environments through WCM remains the same as the configuration for non-Cisco SD-WAN environments, except for a few different steps. Refer to the following links from the AppNav-XE configuration guide. Any difference in configuration for Cisco SD-WAN has been called out with notes.

- Create a Cisco AppNav-XE Cluster with the AppNav Cluster Wizard
- Configure a Class Map on an AppNav-XE Cluster
- Configure AppNav-XE Policy Rules on an AppNav-XE Cluster
- Configure AppNav Controller Settings for an AppNav-XE Device
- Manage AppNav-XE Policies
- Enable Cisco WAAS Service Insertion on AppNav-XE Device Interfaces

Monitor and Troubleshoot AppNav-XE

The AppNav-XE component on your Cisco IOS XE SD-WAN devices can be monitored through CLI on your devices and through the WCM GUI.

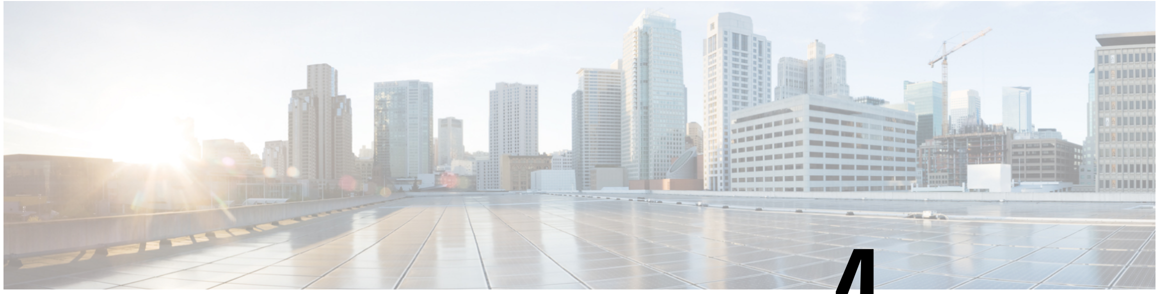
Monitor AppNav-XE

- **Through CLI:** See Monitoring the AppNav-XE Component

- **Through WCM GUI:** See Monitoring an AppNav Cluster

Troubleshoot AppNav-XE

For information on common problems and how to troubleshoot them using various debug commands, see Troubleshooting AppNav-XE.



CHAPTER 4

TCP Optimization

Table 2: Feature History

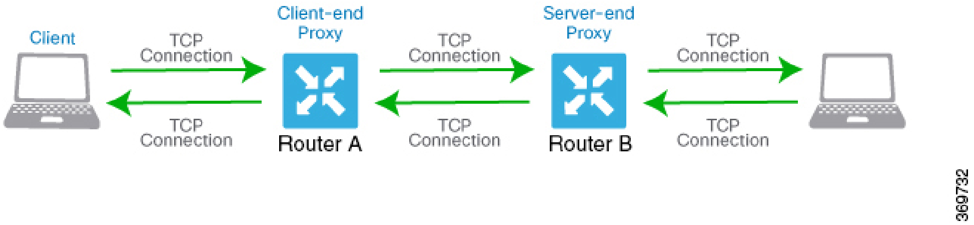
Feature Name	Release Information	Description
TCP Optimization	Cisco IOS XE Release 17.3.1a	TCP optimization support extended to Cisco ISR4221, Cisco ISRv, and Cisco 1000 Series Integrated Services Routers. See Supported Platforms for more information.
	Cisco IOS XE SD-WAN Release 16.12.1d	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput.

TCP optimization fine tunes the processing of TCP data traffic to decrease round-trip latency and improve throughput.

This article describes optimizing TCP traffic in service-side VPNs on Cisco IOS XE SD-WAN devices.

Optimizing TCP traffic is especially useful for improving TCP traffic performance on long-latency links, such as transcontinental links and the high-latency transport links used by VSAT satellite communications systems. TCP optimization can also improve the performance of SaaS applications.

With TCP optimization, a router acts as a TCP proxy between a client that is initiating a TCP flow and a server that is listening for a TCP flow, as illustrated in the following figure:



The figure shows two routers acting as proxies. Router A is the proxy for the client, and is called the client proxy. Router B is the proxy for the server, called the server proxy. Without TCP optimization, the client establishes a TCP connection directly to the server. When you enable TCP optimization on the two routers, Router A terminates the TCP connection from the client and establishes a TCP connection with Router B. Router B then establishes a TCP connection to the server. The two routers cache the TCP traffic in their buffers to ensure that the traffic from the client reaches the server without allowing the TCP connection to time out.

It is recommended that you configure TCP optimization on both the routers, the router closer to the client and the router closer to the server. This configuration is sometimes called a dual-ended proxy. It is possible to configure TCP optimization only on the router closer to the client, a scenario called single-ended proxy, but this configuration is not recommended because the TCP optimization process is compromised. TCP is a bidirectional protocol and operates only when connection-initiation messages (SYNs) are acknowledged by ACK messages in a timely fashion.

If both the client and the server are connected to the same router, no TCP optimization is performed.

To use TCP optimization, first enable the feature on the router. Then define which TCP traffic to optimize. Before you configure TCP optimization, to start with the configuration transaction, you can use the following command such as,

```
ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

Topology and Roles

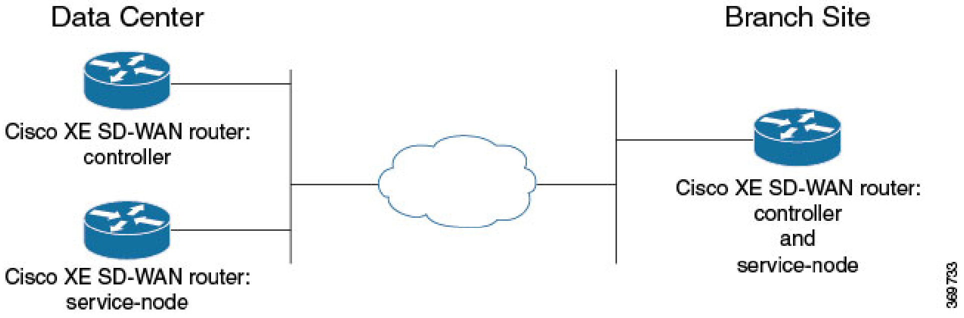
For a branch, the Cisco IOS XE SD-WAN device acts as both controller and service-node.

Data Center

For a data center, the controller and service-node roles are performed by separate Cisco IOS XE SD-WAN devices. This optimizes performance and enables handling more traffic.

The service-node is an external node that has control connections to vManage to receive configurations.

Note The service-node Cisco IOS XE SD-WAN device must have an underlay connection to the controller on the global VRF to establish an appnav tunnel.


Data Center
Branch Site
Cisco XE SD-WAN router: controller
Cisco XE SD-WAN router: service-node
Cisco XE SD-WAN router: controller and service-node
369733

Supported Platforms

Release	Supported Platforms
Cisco IOS XE Release 17.2.1r and later	• Cisco 4331 Integrated Services Router (ISR 4331) • Cisco 4431 Integrated Services Router (ISR 4431) • Cisco 4321 Integrated Services Router (ISR 4321) • Cisco 4351 Integrated Services Router (ISR 4351) • Cisco 4451 Integrated Services Router (ISR 4451) • Cisco 4461 Integrated Services Router (ISR 4461) • Cisco CSR 1000v Cloud Services Router (CSRv)
Cisco IOS XE Release 17.3.1a and later	• Cisco 4221 Integrated Services Router (ISR4221) • Cisco Integrated Services Virtual Router (ISRv) • Cisco 1000 Series Integrated Services Routers **Note** The support is only applicable on Cisco 1000 Series Integrated Services Routers that have a RAM of 8 GB or more. See Cisco 1000 Series Integrated Services Routers Data Sheet for platform specifications.
Cisco IOS XE Release 17.3.2	• Cisco Catalyst 8300 Series Edge Platforms
Cisco IOS XE Release 17.4.1a	• Cisco ISR 1100X Series Integrated Services Routers • Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms

Minimum Resource Requirements

- The platforms must have a minimum of 8 GB of DRAM.
- The platforms must have four or more data cores, with the exception of Cisco 4321 Integrated Services Router (ISR 4321), which is supported in spite of having fewer than four data cores.

Limitations and Restrictions

- TCP optimization in Cisco SD-WAN uses the Bottleneck Bandwidth and Round-trip Propagation Time (BBR) algorithm for congestion control. Because BBR is used, if clients request for Explicit Congestion Notification (ECN), the proxy disables it because it is not supported.

TCP Optimization Configuration Examples

Example: Configure Service Insertion using CLI – Branch Router

This example configures a branch Cisco IOS XE SD-WAN device to act as controller and service-node.

Note By default, subnet 192.168.1.1/30 and 192.0.2.1/30 used for VPG0 and VPG1 (UTD) and 192.168.2.1/24 used for VPG2 (APPQOE) is configured through Cisco vManage. Use any RFC 1918 subnet for Transport and Service VPN configurations other than these netmask.

```
service-insertion appnav-controller-group ACG-APPQOE
 appnav-controller 192.3.3.1
!
service-insertion service-node-group SNG-APPQOE
 service-node 192.3.3.2
!
service-insertion service-context appqoe/1
 appnav-controller-group ACG-APPQOE
 service-node-group      SNG-APPQOE
 enable
 vrf global
!

interface VirtualPortGroup2
 no shutdown
 ip address 192.3.3.1 255.255.255.0
 service-insertion appqoe
exit
```

Example: Configure Service Insertion Using Cisco vManage – Branch Router

For a branch, the Cisco IOS XE SD-WAN device acts as both controller and service-node.

This example configures the branch Cisco IOS XE SD-WAN device as controller and service-node.

Note When enabling the AppQoE feature on a device through Cisco vManage, ensure that you remove any Virtual Port Groups (VPG) that already have **service-insertion appqoe** in their configuration and have an IP address that differs from the one you are pushing through vManage. Enabling AppQoE on a device that has an existing **service-insertion appqoe** configuration on a VPG could lead to a conflict in configurations. This conflict may result in the AppQoE status remaining indeterminate.

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

2. Click **Feature**.
3. Choose a device from one of the device options listed.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Enter a name and description for the template.
6. Click the **Controller** option.
7. Enter the following details for the controller option:
    - Controller IP: Corresponds to the appnav-controller value that would be configured by the service-insertion appnav-controller-group command when configuring by CLI.
    - Internal: Check this check box.
    - Service Node IP: Corresponds to the service-node value that would be configured by the service-insertion service-node-group command when configuring by CLI.
8. Click **Save**.
9. Add the feature template that was created in a previous step, to a device template page. In the AppQoE drop-down menu, choose the name of the feature template. Add the AppQoE template you created in the previous step following the steps below.
    a. From the Cisco vManage menu, choose **Configuration** > **Templates**.
    b. Click **Device**.
    c. From the devices listed in the window, click **...**for the device you want to attach the AppQoE template to. Click **Edit**.
    d. Click **Additional Templates** and under the AppQoE drop-down list, choose the AppQoE template created.
10. Click **Update**.

Example: Configure Service Insertion Using Cisco vManage – Data Center Controller

1. From the Cisco vManage, choose **Configuration** > **Templates**.
2. Click **Feature**.
3. Under **Select Devices**, choose the branch device to configure.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Enter a name and description for the template.
6. Click the **Controller** option.
7. Create a feature template for the Cisco IOS XE SD-WAN device acting as controller. Enter:
    - Controller IP: Corresponds to the appnav-controller value that would be configured by the service-insertion appnav-controller-group command when configuring by CLI.
    - Internal: Leave this option unchecked.

- Service Node IP: Corresponds to the service-node value that would be configured by the service-insertion service-node-group command when configuring by CLI.

8. Click **Save**.
9. Add the feature template that was created in a previous step, to a device template. In the AppQoE drop-down menu, choose the name of the feature template. Add the AppQoE template you created in the previous following the steps below.
   a. From the Cisco vManage menu, choose **Configuration** > **Templates**
   b. Click **Device**.
   c. From the devices listed on the page, select the device you want to attach the AppQoE template to and click the More Options icon (**…**) next to the selected device. Click **Edit**.
   d. Click **Additional Templates** and under the AppQoE drop-down menu, choose the AppQoE template created.
10. Click **Update**.

Example: Configure Service Insertion Using vManage – Data Center Service-Node

Note When enabling the AppQoE feature on a device through vManage, ensure that you remove any Virtual Port Groups (VPG) that already have **service-insertion appqoe** in their configuration and have an IP address that differs from the one you are pushing through vManage. Enabling AppQoE on a device that has an existing **service-insertion appqoe** configuration on a VPG could lead to a conflict in configurations. This conflict may result in the AppQoE status remaining indeterminate.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature**.
3. Under **Select Devices**, choose the branch device to configure.
4. Under **Other Templates** in the right pane, choose **AppQoE**.
5. Click the **Service Node** button.
6. Create a feature template for the Cisco IOS XE SD-WAN device acting as service-node. Enter:
   - Template Name
   - Service Node IP: Corresponds to the appnav-controller value that would be configured by the service-insertion service-node-group command when configuring by CLI.
   - Virtual Port Group IP: Corresponds to the service-node value that would be configured by the interface VirtualPortGroup2 command when configuring by CLI.
7. Click **Save**.
8. Add the feature template that was created in a previous step, to a device template page. In the AppQoE drop-down list, choose the name of the feature template.

9. Click **Create**.

CHAPTER 5

External Service Nodes for AppQoE Services

Table 3: Feature History

Feature Name	Release Information	Description
Support for Multiple, External AppQoE Service Nodes	Cisco IOS XE Release 17.4.1a Cisco vManage Release 20.4.1	This feature allows you to configure multiple AppQoE service nodes that are external to the intercepting edge routers or AppQoE service controllers. It extends AppQoE support to edge routers in which AppQoE can't run as an integrated service node. This feature also allows AppQoE to scale, where integrated AppQoE has limitations on the throughput and number of connections. The ability to configure multiple AppQoE service nodes help meet the scale and throughput requirements of large enterprise sites, such as data centers.
Support for Additional Platforms as Controllers for AppQoE Service Nodes	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	This release extends the service controller role to additional device models—C8500L-8S4X and ASR1006-X.
Support for Automated MTU Setting for Tunnel Adjacency	Cisco IOS XE Release 17.5.1a	This feature enables a programmatic setting of the maximum transmission unit (MTU) size to 1500 for the network connecting the service controllers and service nodes. This automation prevents broken communication due to packet fragmentation that can bring down the throughput requirements.

Supported Devices for AppQoE Controllers and External Service Nodes

Devices Supported as Service Controllers

Release	Supported Devices
Cisco IOS XE Release 17.4.1a and later	• **Cisco ASR 1000 Series Aggregation Services Routers** • ASR1001X • ASR1002X • ASR1001-HX • ASR1002-HX • **Cisco Catalyst 8500 Series Edge Platforms:** • C8500-12X4QC • C8500-12X • Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) **Note** If you configure Cisco Catalyst 8000V as a service controller, you cannot use the same instance as a service node.
Cisco IOS XE Release 17.5.1a and later	• **Cisco Catalyst 8500 Series Edge Platforms** • C8500L-8S4X • **Cisco ASR 1000 Series Aggregation Services Routers** • ASR1006-X

Devices Supported as External Service Nodes

Release	Supported Platforms
Cisco IOS XE Release 17.4.1a and later	• Cisco Catalyst 8000V • **Minimum RAM Requirement:** 16 GB, to be configured as service plane heavy • **Minimum CPU:** 8 Core **Note** If you configure Cisco Catalyst 8000V as a service node, you cannot use the same instance as a service controller.

Note If you configure Cisco Catalyst 8000V as a service node, you cannot use the same instance as a service controller.

Note For information on platforms supported as external service nodes for Data Redundancy Elimination (DRE), see Traffic Optimization with DRE.

Restrictions for External AppQoE Service Nodes

- Only Cisco Catalyst 8000V instances can be configured with the service node role.
- When Cisco Catalyst 8000V is configured as a service node, it can't act as a service controller, even though Cisco Catalyst 8000V supports the service controller role.
- Only one service cluster is supported per site.
- Only one service controller group is supported per site and a service controller group can have up to eight service controllers. A maximum of eight service controllers is supported per site, and each service controller can have up to 64 service nodes.
- Only one service node group is supported per AppQoE cluster.
- VRRP is not supported for service controller to service node connectivity.
- Although handling of asymmetrical flows isn't built into AppQoE, you need to configure flow symmetry for all stateful features in Cisco SD-WAN.
- If a service controller fails, the flows handled by that service controller are reset.
- Ensure that the bootstrap configuration for the Cisco Catalyst 8000V instance being configured as the AppQoE service node is modified as follows:
  - Exclude any controller groups from the TLOC interfaces (**exclude-controller-group** *0*)
  - Ensure that the configuration includes **omp shutdown**

  Note This configuration prevents the AppQoE service node from participating in the SD-WAN data plane. The absence of this modification in the bootstrap configuration leads to generation of alarms indicating that OMP and Control Connections are down in Cisco vManage. However, the alarms are harmless and can be ignored if the recommended configuration is absent from bootstrap configuration.

Information about External AppQoE Service Nodes

Overview of External AppQoE Service Nodes

The support for configuring multiple, external Application Quality of Experience (AppQoE) service nodes provides high availability for TCP and DRE optimization. When AppQoE service nodes are external to the edge router acting as the service controller, the dependency on this intercepting router is reduced. Prior to the release of this feature, AppQoE service instances had to be configured on the service controller itself. You can now configure supported devices with the AppQoE service node role to optimize traffic based on sites and applications. This solution addresses the requirement of larger enterprises to have higher throughput and more number of connections.

Components of AppQoE Solution with External Service Nodes

- **AppQoE Cluster:** An AppQoE controller and a group of AppQoE service nodes at a site.

  Typically, data centers or regional data center sites, which require higher aggregated throughput, have an AppQoE cluster with external service nodes for TCP and DRE optimization.

- **AppQoE Controller:** A supported Cisco IOS XE SD-WAN device that intercepts network traffic. Based on the AppQoE policy, the device distributes that traffic to one or more AppQoE service nodes.

- **AppQoE Service Nodes:** Devices that are configured as AppQoE service nodes are TCP optimization instances that optimize and accelerate traffic. The optimization is based on the configuration in control policies.

  From Cisco IOS XE Release 17.5.1a, the service nodes can also run the DRE feature to eliminate data redundancy and reduce bandwidth usage. For more information, see Traffic Optimization with DRE .

How External Service Nodes and Standalone Controllers Work

With Cisco SD-WAN supporting the creation of external service nodes from Cisco IOS XE Release 17.4.1a, service nodes are decoupled from the intercepting edge router or the service controller. You now have the option to configure supported devices as standalone service controllers and connect them to devices that are configured with the service node role.

Using Cisco vManage device templates, you can configure the following roles on supported devices:

- Service Node
- Service Controller

How Service Controllers and Service Nodes Interact

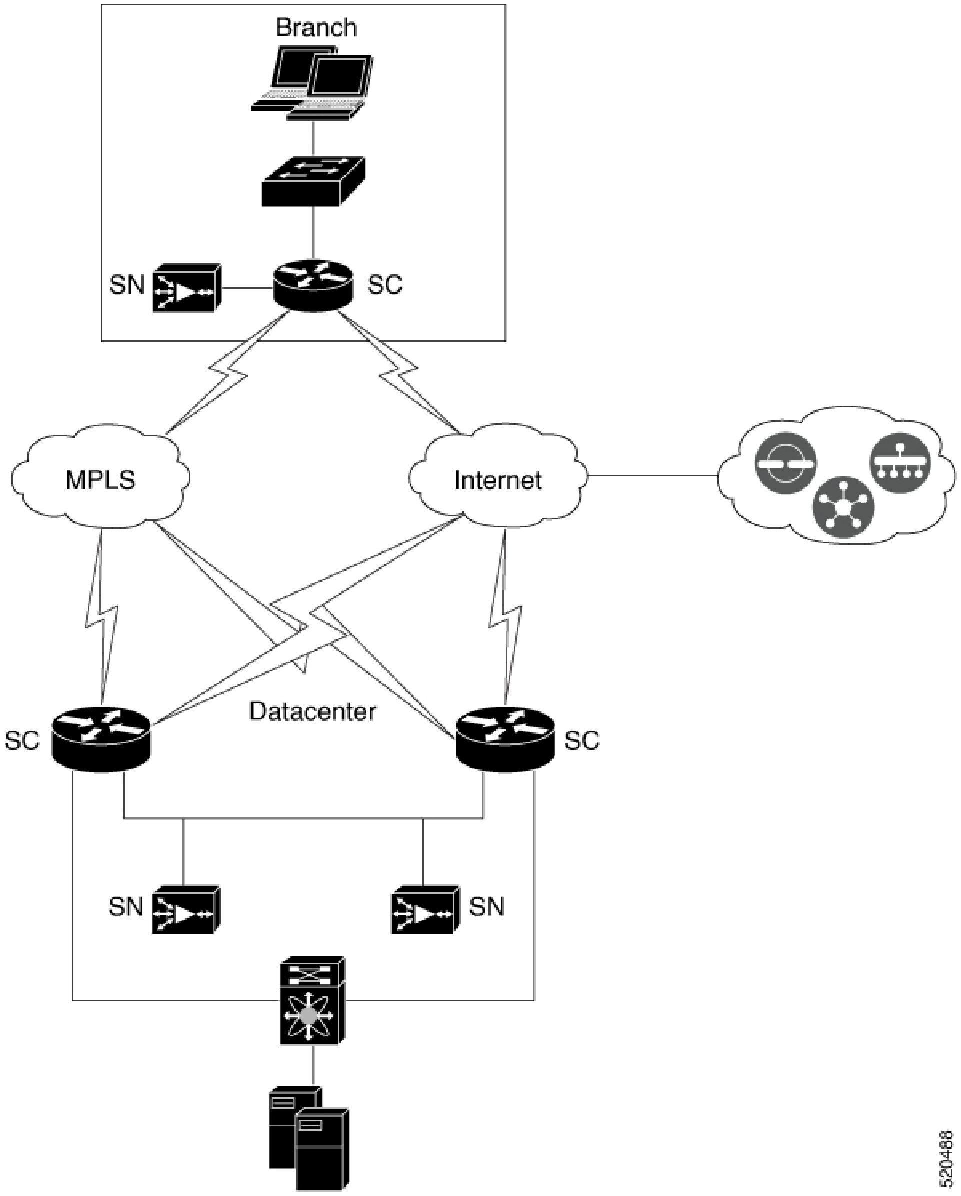
- In Cisco IOS XE Release 17.4.1a, only Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) can be configured with the service node role. When you configure Cisco Catalyst 8000V instances with the service node role, a default AppQoE template is attached to them, which cannot be modified.

- Service nodes in a site and the service controllers that they are connected to form a service cluster.

- Service nodes do not communicate with each other and are not aware of the other service nodes in the cluster.
- Service controllers initiate communication with the service nodes connected to them. This configuration is set up in the AppQoE feature template associated with a device template that has the service controller role defined.
- Service controllers and service nodes can be adjacent to each other, or next or multiple hops away.
- Service controllers communicate with the service nodes through service VPNs. However, service nodes communicate with service controllers through transport VPN or VPN 0.
- Service nodes only respond to the service controller that they are connected with.
- In Cisco vManage, the health of each AppQoE service node is represented by the colors Green or Yellow. Only nodes with Green status are considered for distribution of new flows. Any ongoing flows to service nodes showing as Yellow are redirected.

Sample Topology

Figure 4: Sample Topology with External Service Nodes



*SN: Service node (up to 64 per controller)	
*SC: Service controller (up to 8 per site)	

The image above shows an example of Cisco SD-WAN deployment with service nodes that are external to the service controller. The image shows the deployment at both a branch site and a data center. Cisco IOS XE SD-WAN devices at the data center and branches form an AppQoE cluster with service nodes at their respective sites.

Best Practices and Recommendations

- To ensure that the service nodes have sufficient capacity for AppQoE services, don't configure any other features on devices that have been configured with the service node role.
- When you create an AppQoE cluster containing service controllers and service nodes, ensure that all the cluster members have the same ID as the site.
- Ensure that service controllers and service nodes that form a cluster share the same Cisco SD-WAN site ID. If there’s a mismatch in the site IDs, the service nodes are reported as Yellow on the controller. This leads the service nodes being disregarded from distribution of flows for optimization.
- Ensure that the maximum transmission unit (MTU) size of the network connecting the service controllers and service nodes is uniform across the complete traffic path. Otherwise, it can lead to broken communication due to packet fragmentation.

Configure AppQoE Controllers and Service Nodes

Configure AppQoE Service Nodes

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Under **Device**, click **Create Template** and choose **From Feature Template**.
3. In the **Device Model** field, choose **C8000v**.

   Note Only Cisco Catalyst 8000V instances can be configured as AppQoE service nodes. If you choose any other device, the Service Node option isn’t available in the Device Role field.

4. In the **Device Role** field, choose **Service Node** from the drop-down list.
5. Enter **Template Name** and **Description**.
6. Click **Additional Templates**. In the AppQoE field, notice that the Factory Default AppQoE External Service Node template is attached by default.

   No further configuration is required for devices configured as AppQoE service nodes. Additional configuration for connecting the service nodes to a service node controller is done through the AppQoE controller configuration screens in Cisco vManage.

7. Attach the device template to the device.

Configure AppQoE Service Controller

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Under **Device**, click **Create Template** and choose **From Feature Template**.
3. In the **Device Model** field, choose any one of the devices that support the service controller role. See the Supported Platforms section in this chapter for a complete list of devices that support the service controller role.

4. In the **Device Role** field, choose **SDWAN Edge** from the drop-down list.

   Note The SDWAN cEdge option is only visible for devices that support the service controller role.

5. Enter **Template Name** and **Description**.

6. Click **Additional Templates**. In the AppQoE field, you can either choose an existing AppQoE feature template or create a new one. This procedure includes steps to create a new AppQoE template for the device being configured with the service controller role.

7. Click the drop-down list for the AppQoE field and then click **Create Template.**

8. In the **Template Name** and **Description** fields, enter a name and description for your template respectively.

9. In the **Controller** area, enter the requested details.

   a. **Controller IP address:** Enter the service-side interface IP address of the controller. This is the IP address that the controller uses to communicate with the service nodes connected to it in a service cluster.

   b. **Service VPN:** Specify the service VPN ID in which the LAN-side connections of the service nodes reside. The VPN ID can be anyone from the following ranges: from 1 through 511, or from 513 through 65527.

   c. **Service Node IP 1:** Enter the IP address of the service nodes to enable the service controllers to communicate with the service nodes.

      Note Click + next to the Service Node IP field to add more service nodes. You can add up to 64 service nodes for a single service controller.

      Note From Cisco vManage Release 20.6.1, the AppQoE feature template allows you to configure multiple service node groups and add the external service nodes to such groups. However, if the version of the device that you are configuring as a service controller is lower than Cisco IOS XE Release 17.6.1a, and you use Cisco Cisco vManage Release 20.6.1 to configure the AppQoE template for such device, ensure that you configure only one service node group, even though the template allows you to configure multiple service node groups.

10. Attach the device template to the device.

Configure AppQoE Service Controllers and Nodes Using the CLI

This section provides example CLI configurations to configure TCP optimization using external service nodes and standalone service controllers connected to such service nodes.

Configure an External Service Node

1. Enable TCP optimization.

```
Device# config-transaction
Device(config)# sdwan appqoe tcpopt enable
Device(config-appqoe)# no sslproxy enable
```

2. Create a virtual port group interface.

```
Device(config)# interface VirtualPortGroup virtual-port-group-number
Device(config-if)# service-insertion appqoe
Device(config-if)# ip address ip-address mask
```

3. Create a service node group.

```
Device(config)# service-insertion service-node-group appqoe
service-node-group-name
Device(config-service-insertion-sng)# service-node service-node-ip-address
```

4. Configure the service node as service plane heavy.

```
Device(config)# platform resource service-plane-heavy
```

Note If you configure Cisco Catalyst 8000V as service-plane heavy, you need to reload it to enable the service plane..

Here's the complete configuration example for creating service nodes.

```
config-transaction

 sdwan appqoe tcpopt enable
  no sslproxy enable
  !

 service-insertion service-node-group appqoe SNG-APPQOE

  device-role service-node
  service-node 192.168.2.2
  !

 interface VirtualPortGroup1
  ip address 192.168.2.1 255.255.255.0
  service-insertion appqoe
  !

  interface GigabitEthernet 2
   description SN_LAN_Interface in VPN0
   ip address 192.0.2.1 255.255.255.0
   !

 platform resource service-plane-heavy

 system
```

```
  system-ip 198.51.100.1
  site-id 78200
 !
```

Configure a Service Controller

1. Create a service controller and assign it to a service controller group.

```
Device# config-transaction
Device(config)# service-insertion appnav-controller-group appqoe
appqoe-controller-group-name
Device(config-service-insertion-acg)# appnav-controller controller-ip-address
```

2. Create a service node group and add service nodes to it.

```
Device(config)# service-insertion service-node-group appqoe
service-node-group-name
Device(config-service-insertion-sng)# service-node service-node-ip-address
```

Note You can configure multiple external service nodes in a service node group.

3. Configure service context for the controller and service node groups.

```
Device(config)# service-insertion service-context appqoe/1
Device(config-service-insertion-context)# appnav-controller-group
appqoe-controller-group-name
Device(config-service-insertion-context)# service-node-group service-node-group-name
Device(config-service-insertion-context)# enable
Device(config-service-insertion-context)# vrf default
```

Here's a complete configuration example for creating service controllers.

```
config-transaction

 service-insertion appnav-controller-group appqoe Test-ACgroup
  appnav-controller 198.51.100.1 vrf 200
  !

 service-insertion service-node-group appqoe Test-SNGroup
  service-node 192.0.2.2
  service-node 192.0.2.3
  service-node 192.0.2.4
  service-node 192.0.2.5
  !

 service-insertion service-context appqoe/1
  appnav-controller-group ACG-APPQOE
  service-node-group SNG-APPQOE
  cluster-type service-controller
  enable
  vrf default
  !

  interface GigabitEthernet 1
   description SC_To_SN_LAN_Interface in VPN200
   ip address 192.0.2.1 255.255.255.0
   vrf forwarding 200
   !

  system
   sytem-ip 198.51.100.10
   site-id 78200
   !
```

Monitor AppQoE Service Controllers and Nodes

Verify Device Role

Follow this procedure to verify the device role (service controller or service node) for a device after you configure the role using a device template.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Ensure that you are in the **Device** area .

   A list of available device templates is displayed.
3. Check the **Device Role** column for a device to know its role. **SDWAN Edge** implies that the device is configured as a service controller.

Monitor Traffic on Service Controllers

Alarms and Events

If a cluster isn't formed or is not operational, the device sends a notification to Cisco vManage. You can view such event notifications from the **Monitor** window of Cisco vManage. For some of these events, Cisco vManage also generates alarms. For information on how to view alarms and events for your devices, see Alarms, Events, and Logs

Monitor AppQoE Service Controllers and Nodes Using the CLI

Use the following CLI commands to view the statistics for AppQoE service controllers, service nodes, and clusters.

The following sample output shows the configuration details of service nodes in a service node group:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 10.1.1.1
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020
```

```
Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

The following sample output shows the traffic statistics for service nodes in a service node group:

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
10.1.1.1
10.1.1.2

Aggregate of statistics from all SNs of the SNG:
------------------------------------------------
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

The following sample output shows the configuration details of service controllers in a controller group:

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
10.1.1.100

AppNav Controller : 99.1.1.100
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
Current AC View of AppNav Controller
IP Address
10.1.1.100

Current SN View of AppNav Controller
```

```
IP Address
10.1.1.1
```

CHAPTER 6

Traffic Optimization with DRE

Table 4: Feature History

Feature Name	Release Information	Description
Traffic Optimization with DRE	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	This release extends the DRE functionality to Cisco SD-WAN. DRE is a compression technology that reduces the size of data transmitted over the WAN and enables more effective utilization of the WAN.
DRE Profiles	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	This feature provides the flexibility to use resources for DRE based on your connection requirements by applying profiles such as S, M, L, and XL.
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	This feature lets you deploy Cisco Catalyst 8000V instances, on supported routers, using the UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.

Supported Devices for DRE

Integrated Service Nodes and Controllers

Devices	Release	Memory Requirements
Cisco Catalyst 8300 Series Edge Platforms: • C8300-1N1S-6T • C8300-1N1S-4T2X • C8300-2N2S-6T • C8300-2N2S-4T2X	Cisco IOS XE Release 17.5.1a and later	• RAM: 16 GB • Storage: 600 GB
Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T	Cisco IOS XE Release 17.6.1a and later	• RAM: 16 GB • Storage: 600 GB
Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V)	Cisco IOS XE Release 17.5.1a and later	• RAM: 16 GB • Storage: 600 GB • vCPUs: 8

External Service Nodes and Controllers

Devices	Release	Memory Requirements
Cisco Catalyst 8000V	Cisco IOS XE Release 17.6.1a	• RAM: 32 GB • Storage: 2 TB • vCPUs: 16
	Cisco IOS XE Release 17.5.1a	• RAM: 16 GB • Storage: 600 GB • vCPUs: 8
C8500L-8S4X	Cisco IOS XE Release 17.6.1a	• RAM: 32 GB • Storage: 2 TB
	Cisco IOS XE Release 17.5.1a	• RAM: 16 GB • Storage: 600 GB

Disk Recommendations for DRE

We recommend using solid-state drive (SSD) disks for deploying DRE as well as other AppQoE services.

Configure the following recommended parameters from Cisco Integrated Controller Manager (IMC). Ensure that you configure these before installing the hypervisor because some of the settings may require disk formatting.

Table 5: Recommended Disk Parameters

Parameter	Value
RAID level	RAID10
Read Policy	Always Read Ahead
Disk Cache Policy	Disabled
Write Policy	Write Back Good BBU
Strip Size	256 KB
I/O Cache Policy	Direct

Disk Provisioning Recommendation for Cisco Catalyst 8000V Deployment

While deploying Cisco Catalyst 8000V instances, choose Thick Provision Eager Zeroed as the disk format.

For information on deploying Cisco Catalyst 8000V instances on supported hypervisors, see:

- ESXi
- KVM

Supported DRE Profiles

The following table provides this information:

- Devices that support DRE feature and their default DRE profiles.
- DRE profiles supported on the devices.
- The UTD profile supported along with the DRE profile size configured.
- Minimum resource recommendation for the supported DRE profiles.
- The maximum connections that the DRE profiles provide on the supported devices.
- The FanOut values that correspond to the DRE profiles configured on the devices. FanOut refers to the number of peers that a device can communicate with to form the DRE service.

Table 6: DRE Profiles, Resource Requirements, and Supported Connections and FanOut

Devices and Default DRE Profile	DRE Profiles	Supported UTD Profile	Minimum Deployment Recommendations		Maximum Connections	FanOut
			RAM	Disk		
C8200-1N-4T (S)	S	—	8 GB	120 GB	750	35
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
C8300-2N2S-4T2X (M)	S	S, M	8 GB	120 GB	750	35
	M	S	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256
C8500L-8G4X (M)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22,000	256
	XL	—	32 GB	1600 GB	36,000	256
Cisco Catalyst 8000V—6 core (S)	S	—	8 GB	120 GB	750	35
Cisco Catalyst 8000V—8 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
Cisco Catalyst 8000V—12 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	16 GB	500 GB	10,000	256
Cisco Catalyst 8000V—16 core (S)	S	—	8 GB	120 GB	750	35
	M	—	8 GB	280 GB	5000	70
	L	—	32 GB	500 GB	22000	256
	XL	—	32 GB	1600 GB	36000	256

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

The following table provides this information:

- The memory, disk, and cache allocated based on the DRE profile configured on the supported devices.

Table 7: Profile-wise Resource Allocation

Devices and Default DRE Profile	DRE Profiles	Resource Allocation (GB)		
		Memory	Disk	Cache Size
C8200-1N-4T (S)	S	2	80	60
C8300-2N2S-6T (M) C8300-1N1S-4T2X (M) C8300-1N1S-6T (M)	S	2	80	60
	M	4	250	230
C8300-2N2S-4T2X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
C8500L-8G4X (M)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180
Cisco Catalyst 8000V—6 core (S)	S	2	80	60
Cisco Catalyst 8000V—8 core (S)	S	2	80	60
	M	4	250	230
Cisco Catalyst 8000V—12 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
Cisco Catalyst 8000V—16 core (S)	S	2	80	60
	M	4	250	230
	L	8	480	460
	XL	20	1200	1180

Note UCS E-Series servers only support 6 core, 8 core, and 12 core Cisco Catalyst 8000V instances. For more information, see Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V.

Supported UCS E-Series Server Modules for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Release 17.6.1a, Cisco Catalyst 8000V instances can be deployed on UCS E-Series server modules that reside in Cisco 4000 Series Integrated Services Routers and Cisco Catalyst 8300 Series Edge Platforms.

Device Family	Device Model	Supported UCS-E Module and DRE Profiles
Cisco 4000 Series Integrated Services Routers	Cisco 4461	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4451	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	Cisco 4351	UCS-E160S-M3/K9 (S)
	Cisco 4331	UCS-E160S-M3/K9 (S)
Cisco Catalyst 8300 Series Edge Platforms	C8300-2N2S-4T2X	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	C8300-2N2S-6T	UCS-E180D-M3/K9 (S, M) UCS-E1120D-M3/K9 (S, M, L)
	C8300-1N1S-4T2X	UCS-E160S-M3/K9 (S)
	C8300-1N1S-6T	UCS-E160S-M3/K9 (S)

Restrictions for DRE

- DRE is a dual-side solution. Therefore, flow symmetry is required to configure DRE optimization. DRE isn’t supported for asymmetric flows.
- DRE is supported only if integrated service nodes or external service nodes are deployed at both ends of a Cisco SD-WAN overlay tunnel.
- DRE isn’t supported on devices that are configured as service controllers.
- Starting from Cisco IOS XE Release 17.6.1a the default mode for SSL proxy is single-side. However, because DRE is a dual-side solution, it requires SSL on both, the sending and the receiving end, of the traffic. To optimize SSL performance for this dual-side use case, enable dual-side SSL optimization

using the `dual-side optimization enable` command in Cisco vManage CLI templates. We don’t recommended enabling dual-side SSL if you use GRE tunnels over the WAN.

Restrictions for Installing Cisco Catalyst 8000V on UCS E-Series Servers

Note UCS E-Series Server support is applicable for installing Cisco Catalyst 8000V as an external service node starting from Cisco IOS XE Release 17.6.1a only.

- Only the VMware vSphere ESXi (release 6.7) hypervisor is supported for deploying Cisco Catalyst 8000V instances on UCS-E Series server modules.
- Hyperthreading should be disabled on VMware vSpehere ESXi hypervisor.
- Hyperthreading is not supported for the app-heavy core allocation profile for Cisco Catalyst 8000V deployed on UCS E-Series servers.
- Cisco Catalyst 8000V instances on UCS-E series server modules can only have 6, 8, or 12 cores.
- Cisco Catalyst 8000V instances on UCS-E series server modules should be configured with the app-heavy core allocation profile to enable them to run the DRE service.
- Only one Cisco Catalyst 8000V instance can be installed on a supported UCS E-Series server.
- To change the DRE profile applied to a device, you need to uninstall DRE, reinstall it, and then apply the new DRE profile.

  Note Uninstalling DRE results in loss of cache data.

Information About DRE

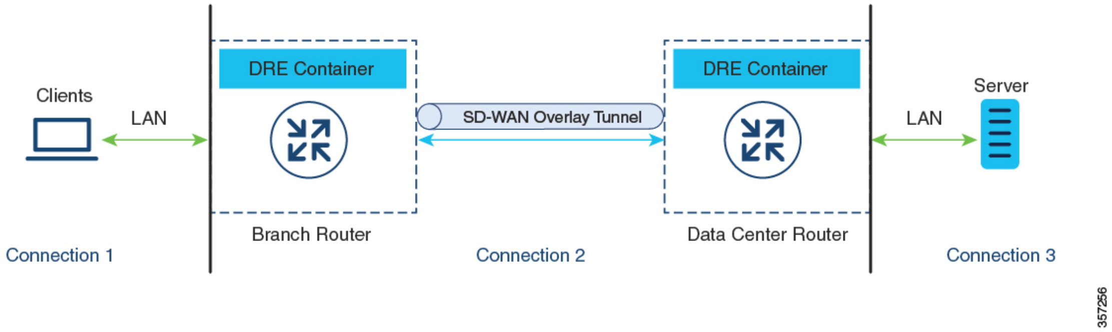
Overview of DRE

Data Redundancy Elimination (DRE) is a compression technology that reduces the size of data transmitted over the WAN. DRE reduces the size of transmitted data by removing redundant information before sending the data stream over the WAN. The DRE compression scheme is based on a shared cache architecture where each peer involved in compression and decompression shares the same redundancy cache. With the integration of DRE with Cisco SD-WAN, DRE replaces repeated data in the stream with a much shorter reference, and then sends the shortened data stream across the SD-WAN overlay. The receiving end uses its local redundancy cache to reconstruct the data stream before passing it along to the destination client or server.

Note Cisco IOS XE SD-WAN devices need to be deployed at both ends of the Cisco SD-WAN overlay tunnel.

How DRE and TCP Optimization Work Together

Figure 5: Interception of TCP Traffic



When DRE is configured, the TCP traffic is intercepted and it's separated into three connections:

Connection Type	Network
Client to the branch Cisco IOS XE SD-WAN device: This connection exists in Local Area Network (LAN)	LAN
Branch router to the data center router	Through Cisco SD-WAN overlay tunnel
Remote branch or data center router to the server	LAN

TCP connections in the Local Area Network (LAN) continue to send the original data. However, TCP connections through the Cisco SD-WAN overlay tunnel send data that is compressed by DRE. The DRE container in the Cisco IOS XE SD-WAN device at one side of the tunnel compresses the data before it's sent over the overlay tunnel. The DRE container in the Cisco IOS XE SD-WAN device at the other side of the tunnel decompresses the data before it's sent to the server at the remote branch or data center side.

Components of DRE

DRE Cache: DRE cache uses secondary storage so that it can store a large amount of data. DRE cache is stored on both sides of the WAN and is used by edge devices to decompress the data. DRE cache in both devices (branch and data center) is synchronized, which means that if a chunk signature is present on one side, the other side has it too.

DRE Compression: DRE uses the Lempel-Ziv-Welch (LZW) compression algorithm for compressing data. DRE operates on large streams of data, typically tens to hundreds of bytes or more, and maintains a much larger compression history.

Overview of DRE Profiles

DRE profiles is a feature introduced in Cisco IOS XE Release 17.6.1a. This feature provides the flexibility to allocate resources to the DRE service based on the size of your branches and the number of connections required. DRE profiles are combinations of resource requirements and allocations that enable resource assignment based on your connection requirements.

The following DRE profiles are supported:

- Small (S)
- Medium (M)
- Large (L)
- Extra-large (XL)

To see the profiles supported on the devices that support the DRE feature, see the *Supported DRE Profiles* section in this chapter.

UCS-E Series Server Support for Deploying Cisco Catalyst 8000V

Starting from Cisco IOS XE Release 17.6.1a, Cisco Catalyst 8000V instances can be configured as external service nodes on supported UCS E-Series server modules. These server modules reside in Cisco 4000 Series Integrated Services Routers (Cisco 4000 Series ISR) and Cisco Catalyst 8000 Series Edge Platforms. These routers come with integrated service nodes. However, you can use supported UCS E-Series servers to deploy Cisco Catalyst 8000V instances on these routers, therefore enabling them to act as hybrid clusters with integrated service nodes and external service nodes. This capability ensures that AppQoE services such as DRE, that require higher CPU, can run on routers that otherwise have lower CPU and RAM.

How Cisco Catalyst 8000V Works on Cisco UCS E-Series Servers

- You can install VMware vSphere ESXi 6.7 hypervisors on UCS-E series server modules that reside in Cisco 4000 Series ISR and Cisco Catalyst 8000 Series Edge Platforms.
- You can then install Cisco Catalyst 8000V on these servers.
- The installed Cisco Catalyst 8000V instances should be configured with the app-heavy profile. This ensures that more cores are allocated to the service plane. The app-heavy profile separates service plane and data plane cores, therefore improving service plane performance.

Configure DRE

Upload DRE Container Image to the Software Repository

Prerequisite

Download the DRE container image from Cisco software downloads page.

Upload the Container Image to Cisco vManage

1. From the Cisco vManage menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.
3. Under **Upload Virtual Image**, choose **vManage**.
4. Browse to the downloaded container image on your local machine, and then click **Upload**.

   When the upload is complete, the image appears in the **Virtual Images** window.

Upgrade DRE Container Virtual Image

To upgrade the container image, see Upgrade Software Image on a Device.

Enable DRE Optimization

Configure AppQoE Template for DRE

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature** and then click **Add Template**.
3. From the **Selected Devices** list, choose a device that is supported for DRE.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose on of the following device roles:
   - **Controller:** Choose **Controller** if you want to configure the device as a controller with an integrated service node. For devices that support an integrated service node, the **Enable** check-box is available. This option is grayed out for devices that don't support the integrated service node functionality.
   - **Service Node:** Choose the **Service Node** option if you want to configure the device as an external service node. The **External Service Node** check box is enabled by default.

     The **Service Node** option is not visible if the device that you chose cannot be configured as an external service node.
7. Under **Advanced**, enable **DRE Optimization**.
8. **Note** The Resource Profile field is applicable for DRE profiles. The DRE profiles feature was introduced in Cisco IOS XE Release 17.6.1a. Therefore, this option is not available in previous releases.

   (Optional) In the **Resource Profile** field, choose **Global** from the drop-down list. Next, choose a profile size from the options available.

   If you don't configure the **Resource Profile**, the default DRE profile size for the device is applied. For more information on the default profiles, see Supported DRE Profiles.
9. (Optional) To optimize HTTPS, FTPS, or any other encrypted traffic, enable **SSL Decryption**.

   Note If you enable **SSL Decryption**, you must configure an SSL/TLS decryption security policy so that the TLS service can decrypt the traffic before it is sent to the DRE container, and then encrypted again after the traffic is optimized.
10. Click **Save**.

Create Security Policy for SSL Decryption

This procedure applies if you enable SSL decryption at the time of configuring the AppQoE feature template to enable DRE optimization.

Configure CA for SSL Proxy

To configure certificate authority for SSL proxy, see Configure CA for SSL/TLS Proxy.

Configure Security Policy for SSL Decryption

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. Choose **Application Quality of Experience** and click **Proceed**.
4. Click **Add TLS/SSL Decryption Policy** and choose **Create New**.
5. Click **Enable SSL Decryption**. Alternatively, toggle the **SSL Decryption** option to enable it.
6. Enter **Policy Name** and other requested details.
7. Click **Save TLS/SSL Decryption Policy**. Your new policy appears in the window.
8. Click **Next**.
9. Enter **Security Policy Name** and **Security Policy Description**.
10. To view the CLI configuration for the policy, click **Preview**. Otherwise, click **Save**.

Update Device Template

For the DRE configuration to take effect, attach the AppQoE policy with DRE enabled, to the device template of the device for which you created the AppQoE policy with DRE.

1. To create a new device template or update an existing one, see Create a Device Template from Feature Templates
2. In the **Additional Templates** area, for **AppQoE**, choose the template you created in the Configure AppQoE Template for DRE section.

Note To deactivate the DRE service, detach the AppQoE template from the device template.

Create a Centralized Policy for TCP and DRE Optimization

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Under **Centralized Policy**, click **Add Policy**.

Note For more information, see Configure Centralized Policies Using Cisco vManage.

3. In the policy configuration wizard, click **Next** until you are on the **Configure Traffic Rules** window.
4. Click **Traffic Data**, and then click **Add Policy**.
5. Enter a name and description for your policy.
6. Click **Sequence Type** and from the **Add Data Policy** dialog box, choose **Custom**.
7. Click **Add Sequence Rule**.
8. Under the **Match** option, you can choose any match conditions that are applicable to a data policy, such as, Source Data Prefix, Application/Application Family List, and so on.
9. Under the **Actions** option, choose **Accept**. Choose **TCP Optimization** and **DRE Optimization** from the options.

   Note Not all actions are available for all match conditions. The actions available to you depend on the match conditions you choose. For more information, see Configure Traffic Rules.

10. Click **Save Match And Actions**.
11. Click **Save Data Policy**.
12. Apply the centralized data policy to the edge devices at the sites between which DRE optimization should be triggered for traffic flows.
13. Activate the centralized policy.

Configure Cisco Catalyst 8000V on UCS-E Series Server Modules for DRE Optimization

From Cisco IOS XE Release 17.6.1a, Cisco Catalyst 8000V instances can be installed as external service nodes on supported UCS E-Series servers that reside in specific router models. This functionality enables the routers to act as hybrid clusters with integrated as well as external service nodes.

Configuration Workflow

1. Configure the UCS E-Series server on the supported router.
2. Deploy Cisco Catalyst 8000V on the supported UCS E-Series server.
3. In Cisco vManage, configure AppQoE feature template for Cisco Catalyst 8000V instances on UCS E-Series servers.
4. In Cisco vManage, configure the AppQoE feature template for the service controllers, and add additional configuration using Cisco vManage CLI template and CLI Add-on feature template.

Configure UCS E-Series Server

Before You Begin

Insert the UCS E-Series server module into the supported device and connect two interfaces (TE2 and TE3) from the front panel. For more information, see UCS-E Series Servers Hardware Installation Guide.

Configure UCS E-Series Server on the Supported Router

The following is sample configuration to enable UCS E-Series server on a supported router:

```
Device(config)# ucse subslot 1/0
Device(config-ucse)# imc access-port shared-lom <ge1/te2/te3>
Device(config-ucse)# imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x
Device(config-ucse)# exit
Device(config)# interface ucse1/0/0
Device(config-if)# ip address x.x.x.1 255.255.255.0
```

Deploy Cisco Catalyst 8000V on UCS E-Series Server

Before You Begin

- Install the hypervisor on the UCS-E server module.
- Download the Cisco Catalyst 8000V 17.6.1 OVA file from the Cisco software download page for Cisco IOS XE Release 17.6.1a, and install it..

Configure IP Addresses for Cisco Catalyst 8000V

The following is a sample for configuring IP addresses for Cisco Catalyst 8000V on the UCS E-Series server:

```
Device(config)# interface GigabitEthernet1
Device(config-if)# description Mgmt
Device(config-if)# ip addeess x.x.x.x x.x.x.x
Device(config)# int GigabitEthernet2
Device(config-if)# description WAN-CONTROLLER
Device(config-if)# ip address x.x.x.x x.x.x.x
Device(config-if)# exit
Device(config)# int GigabitEthernet3
Device(config-if)# description UCSE-INTF
Device(config-if)# ip addeess x.x.x.x x.x.x.x
```

Configure AppQoE Feature Template for Cisco Catalyst 8000V Instances

Before You Begin

Cisco Catalyst 8000V instances on UCS E-Series servers should be configured with the app-heavy resource allocation profile. This profile allows the Cisco Catalyst 8000V instances to participate in DRE optimization.

The following example shows how to configure a device as app-heavy using the Cisco vManage CLI Add-on feature template:

```
Device(config)# platform resource app-heavy
```

Enable DRE Optimization for Cisco Catalyst 8000V Instances

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature** and then click **Add Template**.
3. From the **Selected Devices** list, choose **C8000v**.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Choose the **Service Node** option.
7. Under the **Advanced** section, enable **DRE Optimization**.
8. Click **Save**.

Configure the Controller Cluster Types

Add UCS E-Series Server Configuration in Cisco vManage

In Cisco vManage, create a CLI Add-on feature template and update it with UCS E-Series server configuration.

The following is sample configuration for UCS E-Series servers that can be added to the CLI Add-on feature template:

```
ucse subslot 1/0
imc access-port shared-lom te2
imc ip address 10.x.x.x 255.x.x.x default-gateway 10.x.x.x

interface ucse1/0/0
vrf forwarding 5
```

Option 1: Configure Service Controller as the Cluster Type

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature** and then click **Add Template**.
3. In the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. Leave the **Integrated Service Node** check box unchecked.
7. In the **Controller IP address** field, enter the IP address of the controller.

   Alternatively, choose **Default** from the drop-down list. The AppQoE controller address is chosen by default.
8. In the **Service VPN** field, enter the service VPN number.

   Alternatively, choose **Default** from the drop-down list. The AppQoE service VPN is chosen by default.
9. In the **Service Nodes** area, click **Add Service Nodes** to add service nodes to the AppQoE service node group.

10. Click **Save**.

11. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

    - CLI Add-on feature template with the UCS E-Series server configuration
    - AppQoE feature template

    For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as the integrated service node separately. For more information, see Enable DRE Optimization.

Option 2: Configure Hybrid as the Cluster Type

Routers that have Cisco Catalyst 8000V instances deployed on their UCS E-Series servers can be configured with cluster types as service-controllers or hybrid.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature** and then click **Add Template**.
3. From the **Selected Devices** list, choose the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server.
4. Under **Other Templates**, click **AppQoE**.
5. Enter **Template Name** and **Description**.
6. For the **Integrated Service Node** field, check the **Enable** check box.
7. Click **Save**.
8. Create a CLI template to add the cluster-type hybrid configuration.

   The following is a sample configuration to configure the cluster type as hybrid on the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

```
interface VirtualPortGroup2
 vrf forwarding 5
 ip address 192.168.2.1 255.255.255.0

interface ucse1/0/0
 vrf forwarding 5
 ip address 10.40.17.1 255.255.255.0
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
service-insertion service-node-group appqoe SNG-APPQOE1
 service-node 10.40.17.5
!
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 10.40.17.1 vrf 5

service-insertion service-context appqoe/1
 cluster-type hybrid
 appnav-controller-group ACG-APPQOE
 service-node-group SNG-APPQOE
 service-node-group SNG-APPQOE1
 vrf global
 enable
```

9. Attach the following to the device template of the router that has Cisco Catalyst 8000V deployed on its UCS E-Series server:

   - AppQoE feature template
   - CLI Add-on feature template with the UCS E-Series server configuration
   - CLI template with the hybrid cluster configuration

   For the DRE service to be enabled, bring up DRE on the Cisco Catalyst 8000V instance configured as integrated service node separately. For more information, see Enable DRE Optimization.

Configure DRE Using the CLI

Install DRE Container Package

To install the DRE container package, use the following command:

```
app-hosting install appid < name > package bootflash:<name>.tar
```

Configure Virtual Port Group and Map it to DRE

The following example shows how to configure a virtual port group and map it to the DRE service, and then start the DRE service:

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre


Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Configure Virtual Port Group and Map it to DRE, and Assign a DRE Profile

Note The DRE Profiles feature is available starting from Cisco IOS XE Release 17.6.1a only. This feature is not applicable to releases before Cisco IOS XE Release 17.6.1a.

The following example shows how to configure a virtual port group, map it to the DRE service and assign a DRE profile to the device. This example shows the small (S) profile being assigned.

```
Device(config)# interface VirtualPortGroup 0

Device(config-if)# no shutdown

Device(config-if)# ip address 192.0.2.1 255.255.255.252

Device(config-if)# app-hosting appid dre
Device(config-app-hosting)# app-resource profile-package small
```

```
Device(config-app-hosting)# app-vnic gateway0 virtualportgroup 0 guest-interface 1
Device(config-app-hosting-gateway)# guest-ipaddress 192.0.2.2 netmask 255.255.255.252
Device(config-app-hosting-gateway)# start
```

Activate DRE Service

The following example shows how to activate DRE service for the application named Bangalore:

```
Device# app-hosting activate appid Bangalore
```

Note Use the **app-hosting activate appid** command if you've already configured the DRE application, but haven't enabled it. Alternatively, you can use the **start** command in application hosting gateway configuration mode, as shown in the example in the preceding section.

Uninstall DRE

Follow these steps to deactivate and uninstall the DRE service.

1. Use the following command in privileged EXEC mode to stop the DRE service.

   ```
   Device# app-hosting stop appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be stopped.

2. Use the following command in privileged EXEC mode to deactivate the DRE service.

   ```
   Device# app-hosting deactivate appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be deactivated.

3. Use the following command in privileged EXEC mode to uninstall the DRE service.

   ```
   Device# app-hosting uninstall appid Bangalore
   ```

   In this example Bangalore is the name of the DRE application to be uninstalled.

Monitor DRE

You can monitor the traffic or applications optimized by DRE using Cisco vManage.

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.

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

2. Click the hostname of the device you want to monitor.

3. Under **Service**, choose **AppQoE DRE Optimization**.

4. Choose **Optimized Traffic** or **Application**, depending on what you want to monitor.

5. Choose **Controller** or **Service Node**.

If the chosen device has an integrated service node, you can view the data for either the controller role or the service node role. If the chosen device is an external AppQoE service node, you can view the monitoring data for the external service node, as well as the controller that it's connected to.

Chart and Table View Options

The monitoring data for your selected device displays in the form of a chart, followed by a table. You can view the data in form of a graph or bar chart by toggling between the two options.

- From the **Chart Options** drop-down list, you can view the data by **Bytes** or **Percentage Reduction**.
- You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.

Monitor and Troubleshoot DRE Using CLI

DRE Optimization Status

The following is a sample output of the **show sdwan appqoe dreopt status** command:

```
Device# show sdwan appqoe dreopt status

DRE ID                                            : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                        : 18:27:43

Health status                                     : GREEN

Health status change reason                       : None

Last health status change time                    : 18:25:29

Last health status notification sent time         : 1 second

DRE cache status                                  : Active

Disk cache usage                                  : 91%

Disk latency                                      : 16 ms

Active alarms:

  None


Configuration:

  Profile type                                : Default

  Maximum connections                         : 750

  Maximum fanout                              : 35

  Disk size                                   : 400 GB

  Memory size                                 : 4096 MB
  CPU cores                                  : 1
  Disk encryption                            : ON
```

To view the status in more detail, use the **show sdwan appqoe dreopt status detail** command.

```
Device# show sdwan appqoe dreopt statistics detail
Total connections                  : 325071
Max concurrent connections         : 704
Current active connections         : 0
Total connection resets            : 297319
Total original bytes               : 6280 GB
Total optimized bytes              : 2831 GB
Overall reduction ratio            : 54%
Disk size used                     : 93%
Cache details:
  Cache status                       : Active
  Cache Size                         : 406573 MB
  Cache used                         : 93%
  Oldest data in cache               : 17:13:53:40
  Replaced(last hour): size          : 0 MB
  Cache created at                   : 27:14:13:43
  Evicted cache in loading cache     : 149610430464
Connection reset reasons:
  Socket write failures                               : 0
  Socket read failures                                : 0
  DRE decode failures                                 : 0
  DRE encode failures                                 : 0
  Connection init failures                            : 0
  WAN unexpected close                                : 297319
  Buffer allocation or manipulation failed            : 0
  Peer received reset from end host                   : 0
  DRE connection state out of sync                    : 0
  Memory allocation failed for buffer heads           : 0
  Other reasons                                       : 0
Connection Statistics:
  Alloc                                               : 325071

  Free                                                : 325071

Overall EBP stats:

  Data EBP received                                   : 1921181978

  Data EBP freed                                      : 1921181978

  Data EBP allocated                                  : 218881701

  Data EBP sent                                       : 218881701

  Data EBP send failed                                : 0

  Data EBP no flow context                            : 0

  Data EBP requested more than max size               : 46714730
```

DRE Auto-bypass Status

The following example shows the auto-bypass status of DRE optimization.

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
Update   Entry Age
------------------------------------------------------------------------------------------

      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

DRE Optimization Statistics

The following example shows DRE optimization statistics.

```
Device# show sdwan appqoe dreopt statistics

Total connections                  : 3714

Max concurrent connections         : 552

Current active connections         : 0

Total connection resets            : 1081

Total original bytes               : 360 GB

Total optimized bytes              : 164 GB

Overall reduction ratio            : 54%

Disk size used                     : 91%

Cache details:

  Cache status                       : Active

  Cache Size                         : 407098 MB

  Cache used                         : 91%
  Oldest data in cache              : 03:02:07:55

  Replaced(last hour): size         : 0 MB
```

The following example shows DRE optimization statistics for a peer device.

```
Device# show sdwan appqoe dreopt statistics peer

  Peer No.  System IP          Hostname    Active connections    Cummulative connections

---------------------------------------------------------------------------------------

         0  209.165.201.1       dreopt                     0                       3714
```

DRE Decryption Status

The following example shows how to send a decryption request to DRE and verify if the request was successfully received.

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT

1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

---------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

---------------------------------------------------

SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

---------------------------------------------------

DECRYPTION:

---------------------------------------------------

BLK NAME        :  No of Oper  | Success | Failure

---------------------------------------------------

SIGNATURE BLOCK |     188616     188616          0

SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

---------------------------------------------------
```

Troubleshoot DRE

The following sample output displays the statistics for the auto discovery of peer devices. When connections are not optimized by DRE, run this command and share the output with Cisco Technical Support.

```
Device# show sdwan appqoe ad-statistics

==========================================================

              Auto-Discovery Statistics

==========================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99

 [Core] AD Negotiation Start                 : 10375

 [Core] AD Negotiation Done                  : 10329

 [Core] Rcvd ACK w/o AD options              : 0

 [Core] AOIM sync Needed                     : 0
```

The following sample output displays the statistics for one time exchange of information between peer devices.

```
Device# show sdwan appqoe aoim-statistics

==========================================================

              AOIM Statistics

==========================================================

 Total Number Of Peer Syncs      : 1

 Current Number Of Peer Syncs in Progress      : 0

 Number Of Peer Re-Syncs Needed      : 1

 Total Passthrough Connections Due to Peer Version Mismatch   : 0

 AOIM DB Size (Bytes): 4194304


 LOCAL AO Statistics

----------------------------------------

 Number Of AOs      : 2
 AO             Version   Registered

 SSL             1.2        Y

 DRE             0.23       Y


 PEER Statistics
----------------------------------------

 Number Of Peers      : 1

 Peer ID: 203.203.203.11

 Peer Num AOs      : 2

 AO             Version   InCompatible

 SSL             1.2        N

 DRE             0.23       N
```

The following example shows how to clear DRE cache. Clearing cache restarts the DRE service.

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```

CHAPTER 7

AppQoE Verification and Troubleshooting

Table 8: Feature History

Feature Name	Release Information	Description
Enhanced Troubleshooting for AppQoE	Cisco IOS XE Release 17.6.1a	This release introduces additional show commands to verify and troubleshoot issues in AppQoE features. A few existing show commands for AppQoE have also been enhanced. - show sdwan appqoe error recent - show sdwan appqoe status - show sdwan appqoe flow closed (command modified to include the keyword error) - show sslproxy status (command output modified)

show Commands for AppQoE

Use the following commands to verify the configuration of various AppQoE features and troubleshoot common issues:

- show sdwan appqoe
- show sdwan appqoe dreopt
- show sdwan appqoe dreopt statistics
- show sdwan appqoe error recent
- show sdwan appqoe status
- show sdwan appqoe flow closed
- show sdwan appqoe flow flow-id
- show sdwan appqoe flow vpn-id

- show sslproxy status