TCP Optimization

Table 1: Feature History

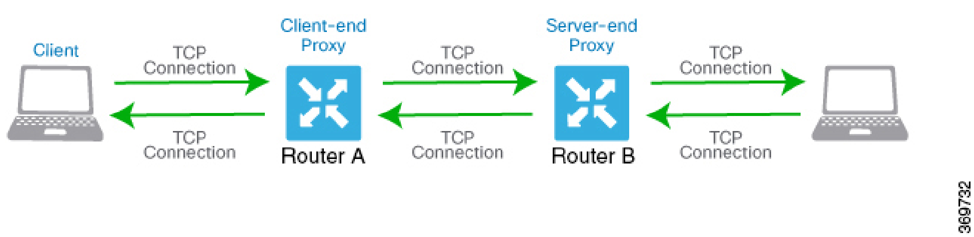
Feature Name	Release Information	Description
TCP Optimization	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	TCP optimization support extended to Cisco 1000 Series Integrated Services Routers (ISRs) and Cisco 4000 Series Integrated Services Routers (ISRs). See Supported Platforms for more information.
	Cisco IOS XE Catalyst 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 Catalyst 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
```

Note The toptalker feature is supported exclusively on Cisco vEdge devices. For Cisco IOS XE Catalyst SD-WAN devices, use the AppQoE TCP optimization options.

Topology and Roles

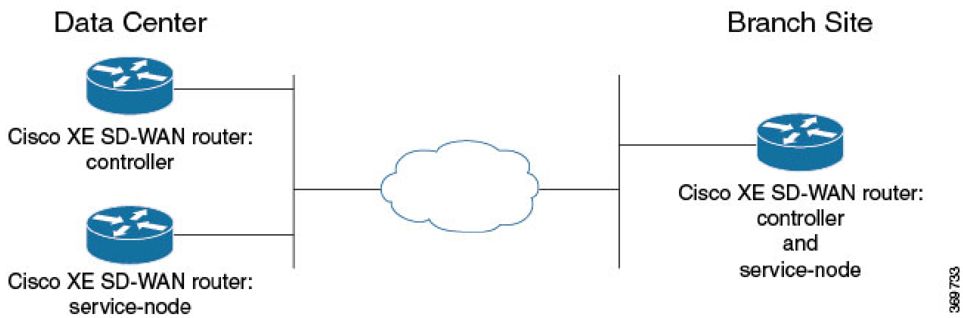
For a branch, the Cisco IOS XE Catalyst SD-WAN device acts as both controller and service-node.

Data Center

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

The service-node is an external node that has control connections to Cisco SD-WAN Manager to receive configurations.

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



Supported Platforms

Integrated Service Nodes

Devices	Release
• 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 17.2.1r 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 17.3.1a and later
• Cisco ISR 1100X Series Integrated Services Routers • Cisco Catalyst 8000V	Cisco IOS XE Release 17.4.1a

Devices	Release
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
Cisco Catalyst 8200 Series Edge Platforms: • C8200-1N-4T	Cisco IOS XE Release 17.6.1a and later
Cisco 8100 Series Secure Routers: • C8161-G2 • C8151-G2 Only the above Cisco 8100 Series Secure Router variants support 8GB DRAM, which allows them to support TCP Optimization. See Cisco 8100 Series Secure Routers Data Sheet for platform specifications.	Cisco IOS XE Release 17.18.1a and later
Cisco 8200 Series Secure Routers: • C8231-E-G2 • C8235-E-G2	Cisco IOS XE Release 17.18.1a and later
Cisco 8200 Series Secure Routers: • C8231-G2 • C8235-G2 C8231 and C8235 do not support SSL proxy.	Cisco IOS XE Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8375-E-G2	Cisco IOS XE Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8300 Series Secure Routers: • C8351-G2 • C8355-G2	Cisco IOS XE Release 17.18.1a and later

Devices	Release
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE Release 17.15.3 and later
Cisco 8100 Series Secure Routers: • C8131-G2 • C8151-CVAI-G2 • C8151-CVAP-G2 Only the above Cisco 8100 Series Secure Router variants support 8GB DRAM, which allows them to support TCP Optimization. See Cisco 8100 Series Secure Routers Data Sheet for platform specifications.	Cisco IOS XE Catalyst SD-WAN Release 26.1.1

Service Controllers

Supported Devices	Release

• 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
Note
If you configure Cisco Catalyst 8000V as a service controller, you cannot use the same instance as a service node.
	Cisco IOS XE SD-WAN Release 17.4.1a and later

• Cisco Catalyst 8500 Series Edge Platforms
  • C8500L-8S4X
• Cisco ASR 1000 Series Aggregation Services Routers
  • ASR1006-X
	Cisco IOS XE SD-WAN Release 17.5.1a and later

Supported Devices	Release
Cisco Catalyst 8500 Series Edge Platforms • C8500-20X6C	Cisco IOS XE SD-WAN Release 17.10.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later
Cisco 8500 Series Secure Routers: • C8570-G2 • C8550-G2	Cisco IOS XE SD-WAN Release 17.15.4a Cisco IOS XE Catalyst SD-WAN Release 17.18.1a and later

External Service Nodes

Devices	Release
Cisco Catalyst 8000V	Cisco IOS XE SD-WAN Release 17.4.1a and later
C8500L-8S4X C8500L supports SSL Proxy function when used as external service node for AppQoE.	Cisco IOS XE SD-WAN Release 17.5.1a and later
Cisco 8400 Series Secure Routers: • C8475-G2 • C8455-G2	Cisco IOS XE SD-WAN Release 17.15.3a and later releases of Cisco IOS XE Catalyst SD-WAN Release 17.15.x Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

TCP optimization is not supported on DNS traffic and C8200L platforms.

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

Minimum Resource Requirements

- The platforms must have a minimum of 16 GB of DRAM.
- The Cisco CSR1000V and Cisco Catalyst 8000V platforms must have eight data cores.

Limitations and Restrictions

- TCP optimization in Cisco Catalyst 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 is not supported for Cisco Catalyst 8000V when deployed on Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) on CSP devices.
- Packet Duplication cannot be enabled with AppQoe on the same connection.

TCP Optimization Configuration Examples

Example: Configure Service Insertion using CLI – Branch Router

This example configures a branch Cisco IOS XE Catalyst 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 SD-WAN Manager. 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 SD-WAN Manager – Branch Router

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

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

> **Note** When enabling the AppQoE feature on a device through Cisco SD-WAN Manager, 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 Cisco SD-WAN Manager. 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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

> **Note** In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**.

   > **Note** In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **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 SD-WAN Manager – Data Center Controller

1. From the Cisco SD-WAN Manager, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

> **Note** In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **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 Catalyst 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 SD-WAN Manager menu, choose **Configuration** > **Templates**
   b. Click **Device Templates**.

> **Note** In Cisco vManage Release 20.7.1 and earlier releases **Device Templates** is called **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 UsingCisco SD-WAN Manager – Data Center Service-Node

> **Note** When enabling the AppQoE feature on a device through Cisco SD-WAN Manager, 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 Cisco SD-WAN Manager. 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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

> **Note** In Cisco vManage Release 20.7.1 and earlier releases **Feature Templates** is called **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 Catalyst 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**.

Monitor TCP Optimization

To view the AppQoE data on Cisco SD-WAN Manager, ensure that you:

- Synchronize the controller and device time by configuring Network Time Protocol (NTP). You can also set the clock manually using the **clock set** command.
- Add the following commands to the device configuration:
  - **policy ip visibility features multi-sn enable**
  - **policy ip visibility features sslproxy enable** (for SSL traffic)

From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. Enable **On-demand Troubleshooting** to view the dashboards. The dashboard screens do not display real-time information. You can also retrieve the DPI statistics by selecting the device from the drop-down menu and choosing the **Data Type** as **DPI**.

You can monitor the traffic or applications optimized by TCP optimizaton using Cisco SD-WAN Manager.

From Cisco vManage Release 20.9.x, you can use **On-Demand Troubleshooting** to monitor the traffic or applications optimized by TCP optimizaton.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier releases: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click the hostname of the device you want to monitor.
3. Under **On-Demand Troubleshooting**, choose **AppQoE TCP Optimization**.
4. Choose **Redirected Traffic**, **Passthrough Traffic** or **Application**, depending on what you want to monitor.
5. Choose **Service Nodes**, **Service Node Groups** or **Control Components.**.

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 **Filters**drop-down list, you can view the data by **Bytes** or **Flow**.
- From the **Filters**drop-down list, you can choose the typr of traffic you want to view.
- You can filter the data for a specified time range: (1h, 3h, 6h, and so on), or click **Custom** to define a time range.