Cisco SD-WAN QoS Overview

Cisco SD-WAN QoS on IOS-XE devices

This white paper presents an overview of the Cisco® Software-Defined WAN (SD-WAN) Quality of Service (QoS) on Cisco IOS® XE routers. It is a good introduction to QoS for those who want to run SD-WAN on selected Cisco Integrated Services Routers (ISRs), Aggregation Services Routers (ASRs), and Enterprise Network Compute Systems (ENCS).

This document describes Cisco's approach to implementing QoS with SD-WAN. SD-WAN is the latest innovation for integrating with enterprises, business, and organizations across the world. The new wave of SD-WAN technologies allows governments and businesses to provide critical application support without additional hassle.

This document does not cover the basic functionality of Cisco SD-WAN. It is purely focused on SD-WAN QoS on XE SD-WAN.

XE SD-WAN is nothing but SD-WAN software integrated on IOS-XE image on Cisco Routers.

To learn more about the overall Cisco SD-WAN solution, please visit www.cisco.com/go/sdwan.

Prerequisites

Before using this document, Cisco recommends that you have knowledge of these topics:

- Cisco SD-WAN solution
- Traditional QoS and policy structure components used

The information here is based on the following software and hardware:

- Cisco edge hardware devices
- Cisco edge software (VM)
- Cisco SD-WAN controllers (vManage, vSmart, vBond)

This document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

© 2019 Cisco and/or its affiliates. All rights reserved.
Solution overview

The SD-WAN approach uses centralized WAN controllers to host and manage all adjacencies with nodes in the network. It provides flexibility in the creation and enforcement of policies. Since each device peers only with controllers for connectivity and control plane policies in order to pass data traffic between service nodes, these can be dynamically adjusted based on overall network conditions.

As shown in Figure 1, each router advertises its local information to the controller. This allows data flow to be easily manipulated by the central controller through the use of policies enforced at every local router.

Figure 1. An SD-WAN configuration

In this example, R1 and R4 have no pairwise adjacency, just the data plane path. Therefore, the central controller easily controls and modifies traffic flow. For example, it can control all the prefixes from R1 that are advertised to R4 via R3.

This approach dramatically reduces the volume of data plane policies that need to be implemented at each router.

SD-WAN is an overlay network, which can help administrators identify critical traffic and give it special treatment throughout the network.
Cisco SD-WAN QoS

In the SD-WAN overlay network, the QoS process begins with an examination of the packets that enter at the edge of the network. Each of the WAN edge routers in the network must be configured to provision QoS. Once the SD-WAN overlay network and the control plane connections are up and running, the data traffic flows automatically over the IPsec connections between WAN edge routers. The default data packet forwarding flow can be modified when centralized data policy or localized data policy is created and applied.

The centralized data policy gives the ability to manage the traffic path, which is routed through the network. The traffic can be controlled (permitted or blocked) based on the address, port, and Differentiated Services Code Point (DSCP) fields in the packet's IP header.

The localized data policy can control the flow of data traffic into and out of a router’s interfaces and enables features such as QoS. The policies can be activated if you apply the access lists either in the outbound direction or in the inbound direction.

Figure 2. SD-WAN QoS components

SD-WAN QoS components

SD-WAN interface or data policy
SD-WAN QoS class-map and rewrite rule
Cisco IOS XE QoS policy map for queuing

SD-WAN interface or data policy

• These policies have an action called “fwd-class.”
• On the device, up to 64 fwd-classes are supported.

Note:
There are some restrictions for subinterface QoS:
• The interface shaper should be mandatory (MUST be 2-level QoS on the subinterface).
• The QoS policy on the subinterface and main interface are mutually exclusive.
SD-WAN QoS class-map and rewrite rule

QoS class-maps
- These provide a mapping from the fwd-class to an output queue.
- The output queue will be stored as “QoS-Group” for the next stage.
- Currently, class-maps are configured at a global level only.

Rewrite rules
- These provide a mapping from the fwd-class to a DSCP or Class of Service (CoS) value that needs to be written to the packet.
- Up to 16 rewrite rule-maps can be configured, and each interface can have a specific rewrite rule-map binding.

Cisco IOS XE QoS policy-map for queueing
- For queueing purposes, Cisco IOS XE QoS policies are reused.
- vManage maps Viptela QoS-map configurations to Cisco IOS XE policy-map configurations.
- In XE SD-WAN, the QoS configuration is limited to only eight classes and the match happening on the QoS-group values (0 to 7). This is how we tie the second-stage output to Cisco IOS XE QoS.

Queueing and IPsec

IPsec supports split anti-replay drop windows for different classes of traffic.

In regular Cisco IOS XE, there are 16 windows based on DSCP values. It is left up to the user to ensure that the correct queues are used based upon these DSCP values.

In XE SD-WAN, the actual queue is used by IPsec to choose the window. This eliminates misconfiguration possibilities.

Queueing details

Queueing policies are two levels deep:
- Shaper at the interface level.
- Per-class queues.

Queue 0
- Always priority or Low-Latency Queuing (LLQ).
- Used for Bidirectional Forwarding Detection (BFD) and SD-WAN control traffic.

Queue 2
- Maps to class default in Cisco IOS XE and uses nonclassified traffic.
- Queue 2 is class-default.
- We don’t support policer with PLP remarking, or remarking based on PLP high;
- Up to 64 rewrite-rule entries supported per rule;

With respect to inner/outer DSCP header remarking, however

We support max of 64 forwarding-class per device, this means that we can have max up to 64 rewrite rule based on default PLP low per forward-class in rewrite-rule given that we don’t support PLP high.
The life of a packet has the following stages:

- During ingress, the packet goes through the port policing and then is classified based on Data Policy (DPI), Access Control List (ACL), and 5-tuple and is associated with a queue.
- During egress, packet flow is matched based on the ACL and then goes through policing, rewrite rules, shaping, and queueing.

**Policing**

The diagram illustrates the processes involved in policing, classification, and queuing.
• Single-rate policer
  - Forwards traffic conforming to the policer rate.
  - Drops traffic exceeding the policer rate.
  - Has a configurable burst rate.

• Ingress and egress policing
  - Interface/VLAN based.
  - Access list classification.
  - Flow policing, match on 5-tuple.

• Data policy classification (ingress only)
  - Flow policing, match on 5-tuple.
  - Application policing, match on DPI.

Marking and re-marking
Figure 5. Marking and re-marking

- Classification
  - Flow, match on 5-tuple (ACL, DPI).
  - Application, match on DPI.

- Ingress interface marks and re-marks inner DSCP bits
  - Copied to encapsulation DSCP bits.

- Egress marks and re-marks outer encapsulation DSCP bits
  - Inner DSCP bits not modified.
  - Transport network QoS.

Shaping
Figure 6. Shaping

- Tokens
- Rate
- Token bucket
- Shape
- Queuing

© 2019 Cisco and/or its affiliates. All rights reserved.
- **Shaper**
  - Forwards traffic conforming to shaper rate.
  - Queues traffic exceeding shaper rate.
  - Uses Weighted Round-Robin (WRR).

- **Egress**
  - Only shaping.
  - Interface based.

### Queuing

**Figure 7. Queuing**

- **Classification**
  - Flow, match on 5-tuple (ACL, DPI).
  - Application, match on DPI.
- **Per-egress interface queuing**
  - Q0 is LLQ.
  - Edge control traffic (DTLS/TLS, BFD, routing protocols) goes into Q0.
  - Not subjected to LLQ policer.
- **Scheduling for Q1 through Q7 is WRR**
- **Drop is RED or taildrop**
  - RED drop profiles are linear, that is, X% queue depth results in X% drop probability.
# vEdge vs. XE SD-WAN QoS

<table>
<thead>
<tr>
<th></th>
<th>vEdge</th>
<th>XE SD-WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data policy</strong></td>
<td>policy data-policy p1 vpn-list v1</td>
<td>policy data-policy p1 vpn-list v1</td>
</tr>
<tr>
<td></td>
<td>sequence 10</td>
<td>sequence 10</td>
</tr>
<tr>
<td></td>
<td>match dscp 1</td>
<td>match dscp 1</td>
</tr>
<tr>
<td></td>
<td>action accept set forwarding-class c1</td>
<td>action accept set forwarding-class c1</td>
</tr>
<tr>
<td><strong>Class</strong></td>
<td>policy class-map class c0 queue 0</td>
<td>policy class-map</td>
</tr>
<tr>
<td></td>
<td></td>
<td>class c0 queue 0</td>
</tr>
<tr>
<td></td>
<td>!NOTE: THE CLASSES IN IOS CLASS-MAP CORRESPOND TO QUEUES AND NOT</td>
<td>!! NOTE: THE CLASSES IN IOS CLASS-MAP CORRESPOND TO QUEUES AND NOT</td>
</tr>
<tr>
<td></td>
<td>SD-WAN CLASSES</td>
<td>SD-WAN CLASSES</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>vpn vpn-id</td>
<td>policy map shape_interface-name</td>
</tr>
<tr>
<td></td>
<td>interface interface-name</td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>qos-map map1</td>
<td>shape average rate-in-bps</td>
</tr>
<tr>
<td></td>
<td>rewrite-rule rewrite1</td>
<td>service-policy output</td>
</tr>
<tr>
<td></td>
<td>shaping-rate rate-in-kbps</td>
<td>shape_interface-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>! qos scheduler configuration translated to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cisco policy-map</td>
</tr>
<tr>
<td><strong>QoS scheduler</strong></td>
<td>policy qos-scheduler qos0</td>
<td>policy-map map1</td>
</tr>
<tr>
<td></td>
<td>class queue0</td>
<td>class queue0</td>
</tr>
<tr>
<td></td>
<td>scheduling liq</td>
<td>priority percent 20</td>
</tr>
<tr>
<td></td>
<td>bandwidth percent 20</td>
<td>class queue1</td>
</tr>
<tr>
<td></td>
<td>buffer-percent 20</td>
<td>bandwidth percent 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>random-detect</td>
</tr>
<tr>
<td></td>
<td>drops red-drop</td>
<td>class queue3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>bandwidth percent 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>random-detect</td>
</tr>
<tr>
<td></td>
<td>qos-scheduler qos1</td>
<td>class class-default</td>
</tr>
<tr>
<td></td>
<td>class queue1</td>
<td>//Replace queue2 with</td>
</tr>
<tr>
<td></td>
<td>bandwidth-percent 10</td>
<td>class-default to match viptela behavior</td>
</tr>
<tr>
<td></td>
<td>buffer-percent 10</td>
<td>bandwidth percent 20</td>
</tr>
<tr>
<td></td>
<td>drops red-drop</td>
<td>random-detect</td>
</tr>
<tr>
<td></td>
<td>qos-scheduler qos2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>class queue2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bandwidth-percent 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>buffer-percent 20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>drops red-drop</td>
<td></td>
</tr>
<tr>
<td></td>
<td>qos-scheduler qos3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>class queue3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bandwidth-percent 50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>buffer-percent 20</td>
<td></td>
</tr>
</tbody>
</table>
Configure Rewrite Rule:
This example shows how to configure the rewrite rule to overwrite the DSCP field of the outer IP header. Here the rewrite rule “transport” overwrites the DSCP value for forwarding classes based on the drop profile. Since all classes are configured with RED drop, they can have one of two profiles: high drop or low drop. The rewrite rule is applied only on the egress interface, so on the way out, packets classified as “af1” and a Packet Loss Priority (PLP) level of low are marked with a DSCP value of 3 in the IP header field, while “af1” packets with a PLP level of high are marked with 4. Similarly, “af2” packets with a PLP level of low are marked with a DSCP value of 5, while “af2” packets with a PLP level of high are marked with 6, and so on.

```
policy
rewrite-rule transport
 class af1 low dscp 3
 class af1 high dscp 4
 class af2 low dscp 5
 class af2 high dscp 6
 class af3 low dscp 7
 class af3 high dscp 8
 class be low dscp 1
 class be high dscp 2
!
```

Apply the Queue Map and Rewrite Rule on an Interface
This example applies the queue map “test” and the rewrite rule “transport” to the egress interface ge0/0 in VPN 0. (Note that you cannot apply QOS maps to VLAN interfaces, also called sub-interfaces.) Queue maps and rewrite rules are applied only on outgoing traffic.

```
vpn 0
interface ge0/0
 ip address 10.1.15.15/24
tunnel-interface
 preference 10
 weight 10
 color lte
 allow-service dhcp
 allow-service dns
 allow-service icmp
 no allow-service sshd
 no allow-service ntp
 no allow-service stun
!

 no shutdown
 qos-map test
 rewrite-rule transport
!
```

© 2019 Cisco and/or its affiliates. All rights reserved.
TLOC Extension – Use Case:

The box XE SD-WAN 1 has a wan interface which needs to be extended via XE SD-WAN 2. The terms we will see are as follows:

- Extended wan interface – the wan interface of the box 1 is directly connected to an interface on box 2.
- Extended interface – the interface connected directly to XE SD-WAN box 1. Traffic from this interface would be extended to a wan interface on box 1. The data from this interface would also undergo NAT before being sent out.

QoS deployment workflow

In the Dashboard, go to Configuration -> Policies -> Localised Policy -> Add Policy -> Class Map.

- Add class-map from vManage policy builder.
- Associate classes with queues.
Adding QoS-map/policy-map from vManage policy builder, continued.

- Associate class queue with bandwidth buffer scheduling type, drop type, and forwarding class.

In order to configure the re-write rule: select Add Rewrite policy
The Rewrite rules will be as below: where you can notice the class name, priority, DSCP value, etc.

Policy configuration preview will be as below:
Adding ACL to classify packets in a certain class:

Packets can be classified based on the DSCP, packet length, and 5-tuple.

Final policy preview

Select Preview to see the final QoS policy.
The following is a preview of the QoS configuration.

Go to Configuration -> Templates -> Edit Device Template -> Additional Templates.

- Attach the policy to the template.
- Attach the template to the device.
Applying QoS-map/policy-map to an interface

- Go to Feature -> Template -> VPN Interface Ethernet -> ACL/QoS.
- Attach the feature template to the interface of the device.

Summary

It is easy to understand how Cisco SD-WAN QoS as a solution threatens the traditional MPLS WANs out there, as this solution can deliver QoS levels that match over the Internet with the use of dynamic methods. Cisco SD-WAN dynamically selects the most cost-effective assortment of private links and public Internet connections. With SD-WAN, applications are not at the mercy of standard bandwidth, but instead the connection that’s most applicable to each app is selected.