Configure QOS (Filter, Marking and Classifying) on Nexus 9000

Contents

Introduction

This document describes how to configure and verify Quality of Service (Filter, Marking and Classifying) on Nexus 9000 switches.

Background Information

Marking and classifying traffic in Quality of Service (QoS) is crucial for network performance and ensuring that critical applications receive the necessary level of service.

Summary of its uses:

1. **Traffic Differentiation**: Networks carry various types of traffic, including voice, video, data, and real-time applications. Marking and classifying traffic allow network administrators to differentiate between these types based on their importance, sensitivity to delay, and bandwidth requirements.

2. **Resource Allocation**: By classifying traffic, network devices can allocate resources such as bandwidth, buffer space, and processing power more effectively. Critical applications can be prioritized over less time-sensitive traffic, ensuring that they receive the necessary resources to function optimally.

3. **QoS Guarantees**: Marking and classifying traffic enable the implementation of QoS policies that enforce service level agreements (SLAs) and guarantee certain performance metrics for specific applications or user groups. This ensures a consistent quality of experience for end-users, minimizing the impact of congestion or network issues.

4. **Congestion Management**: In times of network congestion, QoS mechanisms prioritize traffic based on its classification, ensuring that critical applications continue to function smoothly while non-essential traffic possibly experiences delays or is dropped. This helps maintain network stability and prevents degradation of service for important applications.

5. **Optimized Network Utilization**: By intelligently managing traffic through QoS mechanisms, network resources are utilized more efficiently. Unused bandwidth can be dynamically allocated to high-priority applications, maximizing the overall performance of the network.

6. **Enhanced User Experience**: Marking and classifying traffic based on its importance to users or the business allows organizations to deliver a better user experience. Critical applications such as VoIP or video conferencing receive priority treatment, resulting in clearer calls, smoother video streams, and improved productivity.

7. **Security and Compliance**: QoS can also be used to enforce security policies by prioritizing traffic from trusted sources or applying traffic shaping to limit bandwidth for certain types of traffic, such as peer-to-peer file sharing or streaming services. Additionally, QoS mechanisms can help organizations meet compliance requirements by ensuring the prioritization and protection of sensitive data flows.

Overall, marking and classifying traffic in QoS are essential components of network management, enabling organizations to optimize performance, ensure reliable service delivery, and meet the diverse requirements of modern applications and users.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

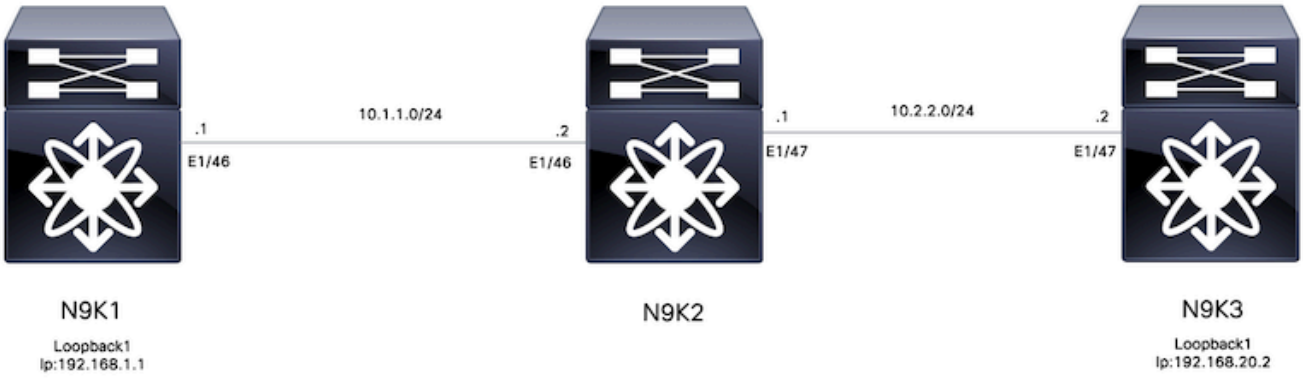
- NXOS Platform
- QoS
- Elam understanding
- Access lists (ACL)

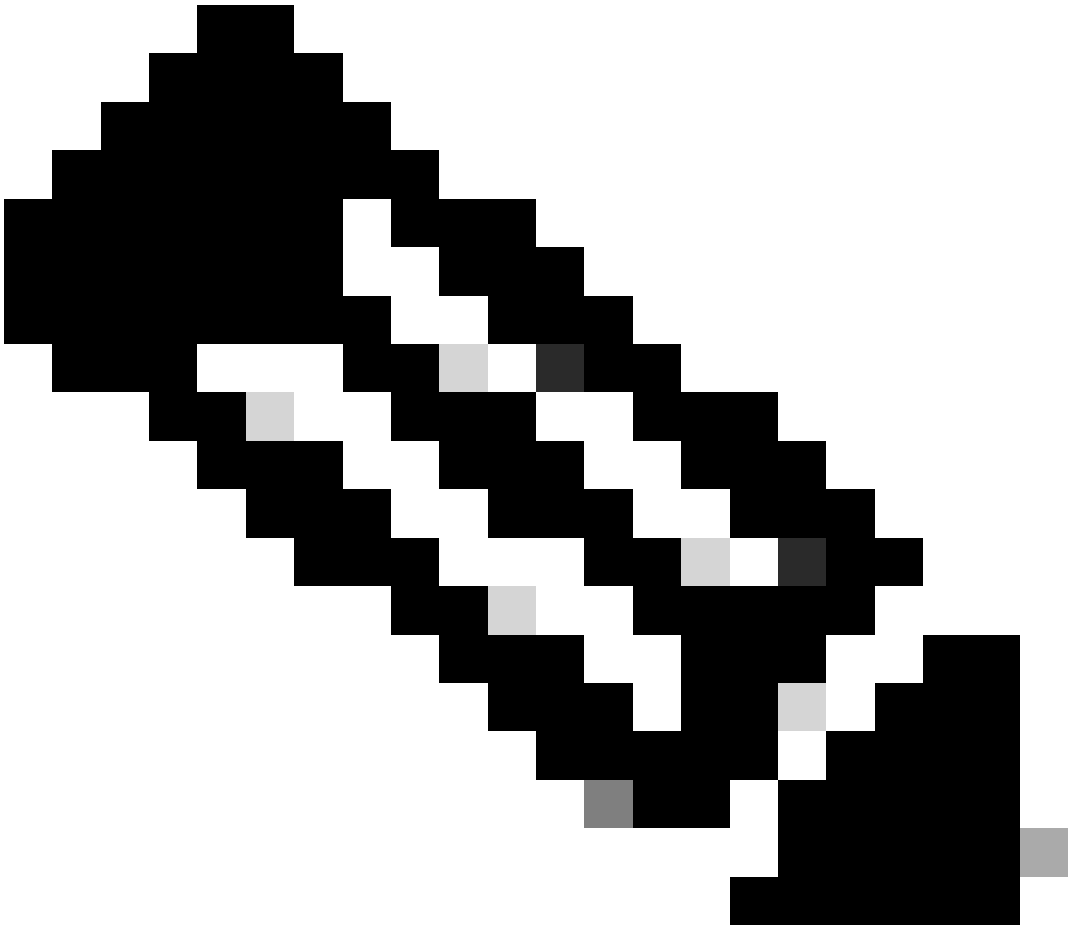
Components Used

Name	Platform	Version
N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

The information in this document was created from the 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.

Topology





Note: For this example N9K2 is the device configured for Filter, Marking and Classifying. N9K1 and N9K3 emulate hosts source and destination.

Filtering

Filtering for Quality of Service (QoS) is essential for ensuring efficient network resource utilization and prioritizing critical traffic. In summary, filtering for QoS is paramount for optimizing network performance, enhancing security, meeting compliance requirements, and delivering a superior quality of experience for end-users. By effectively managing and controlling traffic flows, organizations can ensure the efficient utilization of network resources while maintaining the integrity and security of their networks.

For this example traffic from 192.168.1.1 to 192.168.2 are filtered, new entries can be added to the access-list to have more control of the traffic.

Configure

	Command or Action	**Purpose**
Step 1	N9K2# configure terminal	Enters configuration mode.
Step 2	N9K2(config)# ip access-list marking-acl	Creates ACL to filter traffic.
Step 3	N9K2(config-acl)# permit ip host 192.168.1.1 host 192.168.20.2	Specify IPs that are filtered
Step 4	N9K2(config-acl)# class-map type qos marking-class	Create Class-map for QoS marking
Step 5	N9K2(config-cmap-qos)# match access-group name marking-acl	Match ACL created on step 2

Marking and Classifying

Marking and classifying traffic for Quality of Service (QoS) is fundamental for optimizing network performance, ensuring efficient resource allocation, and enhancing user experience, marking and classifying traffic for QoS are essential practices for optimizing network performance, ensuring efficient resource utilization, and delivering a consistent quality of experience for users. By effectively managing and prioritizing traffic flows, organizations can maximize the value of their network infrastructure while maintaining the integrity and security of their digital assets.

For this example traffic that is already filtered is marked with DSCP value of 5 and is Classified on QoS group 7.

Configure

	Command or Action	**Purpose**
Step 1	N9K2# configure terminal	Enters configuration mode.
Step 2	N9K2(config)# policy-map type qos ingress-classify	Creates policy-map to classify and mark traffic
Step 3	N9K2(config-pmap-qos)# class marking-class	Attach marking class to created policy-map
Step 4	N9K2(config-pmap-c-qos)# set dscp 5	Sets DSCP value of 5 to all traffic matching marking class

Step 5	N9K2(config-pmap-c-qos)# set qos-group 7	Classify traffic matching marking class to QoS group 7
Step 6	N9K2(config-pmap-c-qos)# interface ethernet 1/46	Ener interface configuration
Step 7	N9K2(config-ip)# service-policy type qos input ingress-classify	Apply service policy to ingress interface

Summary steps

1. configure terminal
2. ip access-list marking-acl
3. permit ip host 192.168.1.1 host 192.168.20.2
4. class-map type qos marking-class
5. match access-group name marking-acl
6. policy-map type qos ingress-classify
7. class marking-class
8. set qos-group 7
9. interface ethernet 1/46
10. service-policy type qos input ingress-classify

Verify

Verify Marking

In order to verify if marking was performed correctly a packet capture needs to be performed.

For this example this can be achieve performing a SPAN capture on interface e1/47 (egress interface) on N9K2 or performing a ELAM capture on interface e1/47 (ingress interface) on N9K3.

	Command or Action	**Purpose**
Step 1	N9K3# show hardware internal tah interface e1/47 | include ignore-case asic|slice|srcid Asic: 0 **Asic: 0** AsicPort: 54 **SrcId: 28** **Slice: 1**	Identifies ASIC, Slice and source ID from interface where marked traffic is received.
Step 2	N9K3(TAH-elam-insel6)# attach module 1	Attach to module where front port resides.
Step 3	module-1# debug platform internal tah elam asic 0	Starts ELAM configuration on ASIC 0.
Step 4	module-1(TAH-elam)# trigger init **asic 0 slice 1** use-src-id **28**	Set trigger parameters using Asic=0, Slice=1 and SrcId=28 taken from step 1.
Step 5	module-1(TAH-elam-insel6)# set outer ipv4 src_ip 192.168.1.1 dst_ip 192.168.20.2	Set filters to capture specif traffic .
Step 6	module-1(TAH-elam-insel6)# start	Starts capture.

Step 7	<#root> module-1(TAH-elam-insel6)# report SUGARBOWL ELAM REPORT SUMMARY slot - 1, asic - 0, slice - 1 ========================== Incoming Interface: Eth1/47 <Snipped> Packet Type: IPv4 Dst MAC address: 84:3D:C6:3A:6A:BF Src MAC address: 74:A2:E6:C6:28:FF Sup hit: 1, Sup Idx: 2750 Dst IPv4 address: 192.168.20.2 Src IPv4 address: 192.168.1.1 Ver = 4, **DSCP = 5** , Don't Fragment = 0 Proto = 1, TTL = 254, More Fragments = 0 Hdr len = 20, Pkt len = 84, Checksum = 0x9b89 L4 Protocol : 1 ICMP type : 8 ICMP code : 0	Displays capture, DSCP value of 5 can be observed (Highlighted)

Verify Classifying

Queueing information of the egress interface can be reviewed to verify if traffic is classified correctly.

For this example 5 packets were sent from 192.168.1.1 to 192.168.2, as observed 5 packets are displayed in the TX direction for QoS group 7 confirming that Classify is done correctly.

	Command or Action	**Purpose**
Step 1	<#root>	Traffic matching Marking

	N9K2(config-if)# show queuing interface **e1/47** slot 1 ======= Egress Queuing for Ethernet1/47 [System] -- <Snipped> +---+ | **QOS GROUP 7** | +---+ | | Unicast |Multicast | +---+ | **Tx Pkts | 5** | 0| | Tx Byts | 510| 0| | WRED/AFD & Tail Drop Pkts | 0| 0| | WRED/AFD & Tail Drop Byts | 0| 0| | Q Depth Byts | 0| 0| | WD & Tail Drop Pkts | 0| 0| +---+	class is classified on **QoS group 7**.