在Nexus 9000上配置QOS（过滤、标记和分类）

目录

简介

本文档介绍如何配置和验证Nexus 9000交换机的服务质量（过滤、标记和分类）。

背景信息

服务质量(QoS)对流量进行标记和分类对于网络性能和确保关键应用获得必要的服务水平至关重要。

其使用摘要：

1. 流量差异：网络传输各种类型的流量，包括语音、视频、数据和实时应用。通过对流量进行标记和分类，网络管理员可以根据其重要性、对延迟的敏感性以及带宽要求来区分这些类型。

2. 资源分配：通过对流量进行分类，网络设备可以更有效地分配带宽、缓冲区空间和处理能力等资源。可将关键应用的优先级置于对时间不太敏感的流量之上，确保它们获得必要的资源以最佳方式运行。

3. QoS保证：对流量进行标记和分类有助于实施QoS策略，这些策略可强制执行服务级别协议(SLA)并确保特定应用或用户组的某些性能指标。这样可确保最终用户获得一致的体验质量，将拥塞或网络问题的影响降至最低。

4. 拥塞管理：在网络拥塞时，QoS机制会根据其分类确定流量的优先级，确保关键应用继续平稳运行，而非关键流量可能遇到延迟或被丢弃。这有助于保持网络稳定性，并防止重要应用的服务降级。

5. 优化网络利用率：通过QoS机制智能地管理流量，可以更有效地利用网络资源。未使用的带宽可以动态分配给高优先级应用，从而最大程度提高网络的整体性能。

6. 增强用户体验：根据流量对用户或业务的重要性对其标记和分类，使组织能够提供更好的用户体验。VoIP或视频会议等关键应用会得到优先处理，从而使呼叫更清晰、视频流更流畅，并提高工作效率。

7. 安全性和合规性：QoS还可用于实施安全策略，方法是对来自受信任源的流量进行优先级排序，或者应用流量整形来限制某些流量类型的带宽，例如点对点文件共享或流服务。此外，QoS机制还可以确保敏感数据流的优先级和保护性，从而帮助组织满足合规性要求。

总体而言，标记和分类QoS中的流量是网络管理的重要组成部分，可让组织优化性能、确保可靠的服务交付并满足现代应用和用户的不同要求。

先决条件

要求

Cisco 建议您了解以下主题：

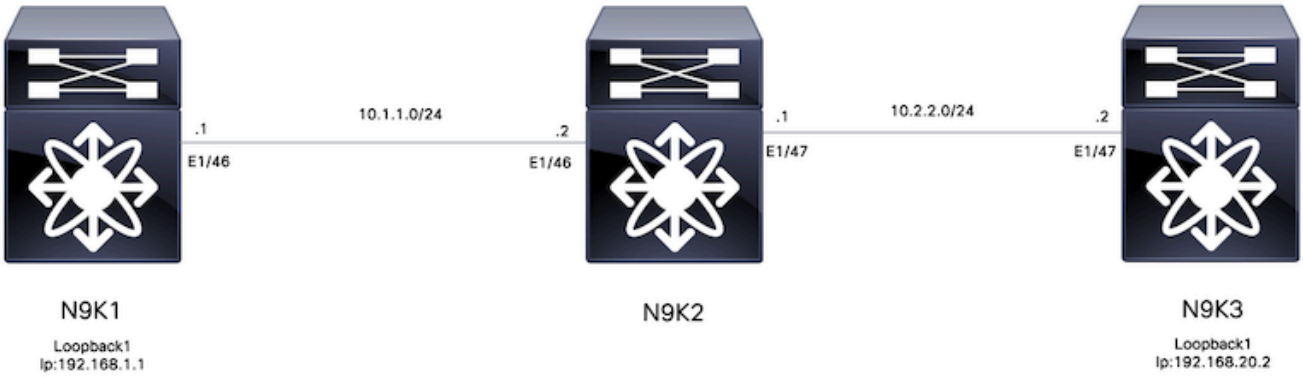
- NXOS平台
- QoS
- Elam了解
- 访问列表(ACL)

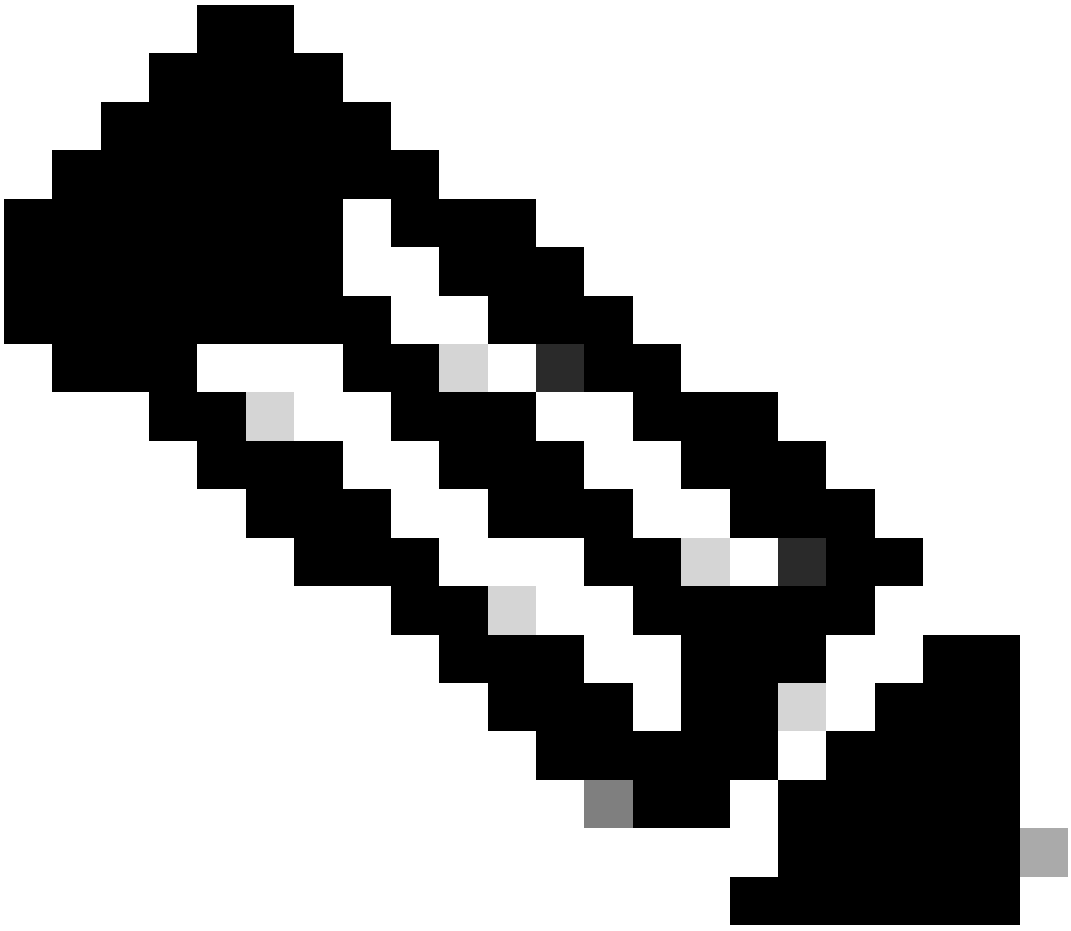
使用的组件

名称	Platform	version
N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

拓扑





注意：对于此示例，N9K2是为过滤、标记和分类配置的设备。N9K1和N9K3模拟主机源和目标。

过滤

服务质量(QoS)过滤对于确保高效的网络资源利用和优先处理关键流量至关重要。 总之，QoS过滤对于优化网络性能、增强安全性、满足合规性要求以及为最终用户提供卓越的体验质量至关重要。通过有效管理和控制流量，组织可以确保网络资源的高效利用，同时维护网络的完整性和安全性。

对于本示例，过滤从192.168.1.1到192.168.2的流量，可以将新条目添加到访问列表中，以更好地控制流量。

配置

	命令或操作	目的
第 1 步	N9K2#配置终端	进入配置模式。
步骤 2	N9K2(config)# ip access-list marking-acl	创建ACL以过滤流量。
步骤 3	N9K2(config-acl)# permit ip host 192.168.1.1 host 192.168.20.2	指定过滤的IP
步骤 4	N9K2(config-acl)# class-map type qos marking-class	创建用于QoS标记的类映射
步骤 5	N9K2(config-cmap-qos)# match access-group name marking-acl	匹配第2步中创建的ACL

标记和分类

根据服务质量(QoS)标记和分类流量是优化网络性能、确保高效资源分配和增强用户体验的基础，为QoS标记和分类流量是优化网络性能、确保高效资源利用以及为用户提供一致体验质量的基本实践。通过有效管理和优先处理流量，组织可以在保持数字资产的完整性和安全性的同时，最大程度地提高其网络基础设施的价值。

对于此示例，已过滤的流量使用DSCP值5进行标记，并在QoS组7上进行分类。

配置

	命令或操作	目的
第 1 步	N9K2#配置终端	进入配置模式。
步骤 2	N9K2(config)# policy-map type qos ingress-classify	创建策略映射以分类和标记流量
步骤 3	N9K2(config-pmap-qos)# class marking-class	将标记类附加到创建的策略映射
步骤 4	N9K2(config-pmap-c-qos)# set dscp 5	将DSCP值5设置为匹配标记类的所有流量
步骤 5	N9K2(config-pmap-c-qos)# set	将流量匹配标记类分类到QoS组

	qos-group 7	7
步骤 6	N9K2(config-pmap-c-qos)# interface ethernet 1/46	输入接口配置
步骤 7	N9K2(config-ip)# service-policy type qos input ingress-classify	将服务策略应用于入口接口

汇总步骤

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

验证

验证标记

为了验证标记是否正确执行，需要执行数据包捕获。

对于此示例，可以在N9K2的接口e1/47（出口接口）上执行SPAN捕获，或在N9K3的接口e1/47（入口接口）上执行ELAM捕获。

	命令或操作	目的
第 1 步	N9K3# show hardware internal tah interface e1/47 | include ignore-case asic|slice|srcid Asic：0 Asic：0 AsicPort：54 源Id：28 切片：1	从接收标记流量的接口标识ASIC、切片和源ID。
步骤 2	N9K3(TAH-elam-insel6)#连接模块1	连接到前端口所在的模块。
步骤 3	module-1# debug platform internal tah elam asic 0	启动ASIC 0上的ELAM配置。
步骤 4	module-1 (TAH-elam)# trigger init asic 0 slice 1 use-src-id 28	使用步骤1中的Asic=0、Slice=1和SrcId=28设置触发器参数。
步骤 5	module-1(TAH-elam-insel6)# set outer ipv4 src_ip	设置过滤器以捕获特定流

	192.168.1.1 dst_ip 192.168.20.2	量。
步骤 6	module-1(TAH-elam-insel6)# start	开始捕获。
步骤 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	显示捕获，可观察DSCP值5（突出显示）

验证分类

可以检查出口接口的排队信息，以验证流量是否正确分类。

在本例中，从192.168.1.1到192.168.2发送了5个数据包，正如观察到的5个数据包在QoS组7的TX方向上显示，并确认分类已正确完成。

	命令或操作	目的

第 1 步	<#root> 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| +---+	与标记类匹配的流量按QoS组7分类。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。