Configurar QOS (Filter, Marking and Classifying, filtragem, marcação e classificação) no Nexus 9000

Contents

Introdução

Este documento descreve como configurar e verificar a Qualidade de Serviço (Filtrar, Marcar e Classificar) em switches Nexus 9000.

Informações de Apoio

Marcar e classificar o tráfego na Qualidade de Serviço (QoS) é crucial para o desempenho da rede e garantir que os aplicativos críticos recebam o nível de serviço necessário.

Resumo das suas utilizações:

1. Diferenciação de tráfego: as redes transportam vários tipos de tráfego, incluindo voz, vídeo, dados e aplicativos em tempo real. A marcação e a classificação do tráfego permitem que os administradores de rede diferenciem esses tipos com base em sua importância, sensibilidade ao atraso e requisitos de largura de banda.

2. Alocação de recursos: ao classificar o tráfego, os dispositivos de rede podem alocar recursos como largura de banda, espaço em buffer e potência de processamento de forma mais eficaz. Os aplicativos críticos podem ser priorizados em relação ao tráfego menos

sensível ao tempo, garantindo que recebam os recursos necessários para funcionar da melhor forma possível.

3. Garantias de QoS: a marcação e a classificação do tráfego permitem a implementação de políticas de QoS que aplicam acordos de nível de serviço (SLAs) e garantem determinadas métricas de desempenho para aplicativos específicos ou grupos de usuários. Isso garante uma qualidade consistente de experiência para os usuários finais, minimizando o impacto de problemas de congestionamento ou de rede.

4. Gerenciamento de congestionamento: em tempos de congestionamento de rede, os mecanismos de QoS priorizam o tráfego com base em sua classificação, garantindo que aplicativos críticos continuem a funcionar sem problemas, enquanto o tráfego não essencial possivelmente sofre atrasos ou é descartado. Isso ajuda a manter a estabilidade da rede e evita a degradação do serviço para aplicativos importantes.

5. Utilização otimizada da rede: ao gerenciar o tráfego de forma inteligente por meio de mecanismos de QoS, os recursos da rede são utilizados com mais eficiência. A largura de banda não utilizada pode ser alocada dinamicamente para aplicativos de alta prioridade, maximizando o desempenho geral da rede.

6. Experiência do usuário aprimorada: marcar e classificar o tráfego com base em sua importância para os usuários ou para a empresa permite que as organizações ofereçam uma melhor experiência ao usuário. Aplicativos essenciais como VoIP ou videoconferência recebem tratamento prioritário, resultando em chamadas mais claras, fluxos de vídeo mais suaves e maior produtividade.

7. Segurança e conformidade: a QoS também pode ser usada para aplicar políticas de segurança, priorizando o tráfego de fontes confiáveis ou aplicando modelagem de tráfego para limitar a largura de banda para determinados tipos de tráfego, como compartilhamento de arquivos ponto a ponto ou serviços de transmissão. Além disso, os mecanismos de QoS podem ajudar as organizações a atender aos requisitos de conformidade, garantindo a priorização e a proteção de fluxos de dados confidenciais.

Em geral, a marcação e a classificação do tráfego em QoS são componentes essenciais do gerenciamento de rede, permitindo que as organizações otimizem o desempenho, garantam a entrega confiável de serviços e atendam aos diversos requisitos de aplicativos e usuários modernos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Plataforma NXOS
- qos
- Compreensão de Elam

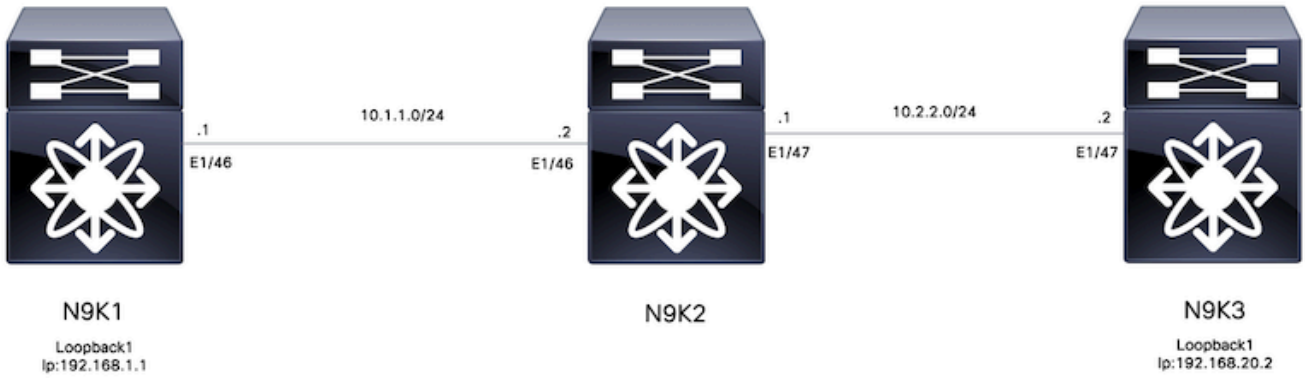
- Listas de acesso (ACL)

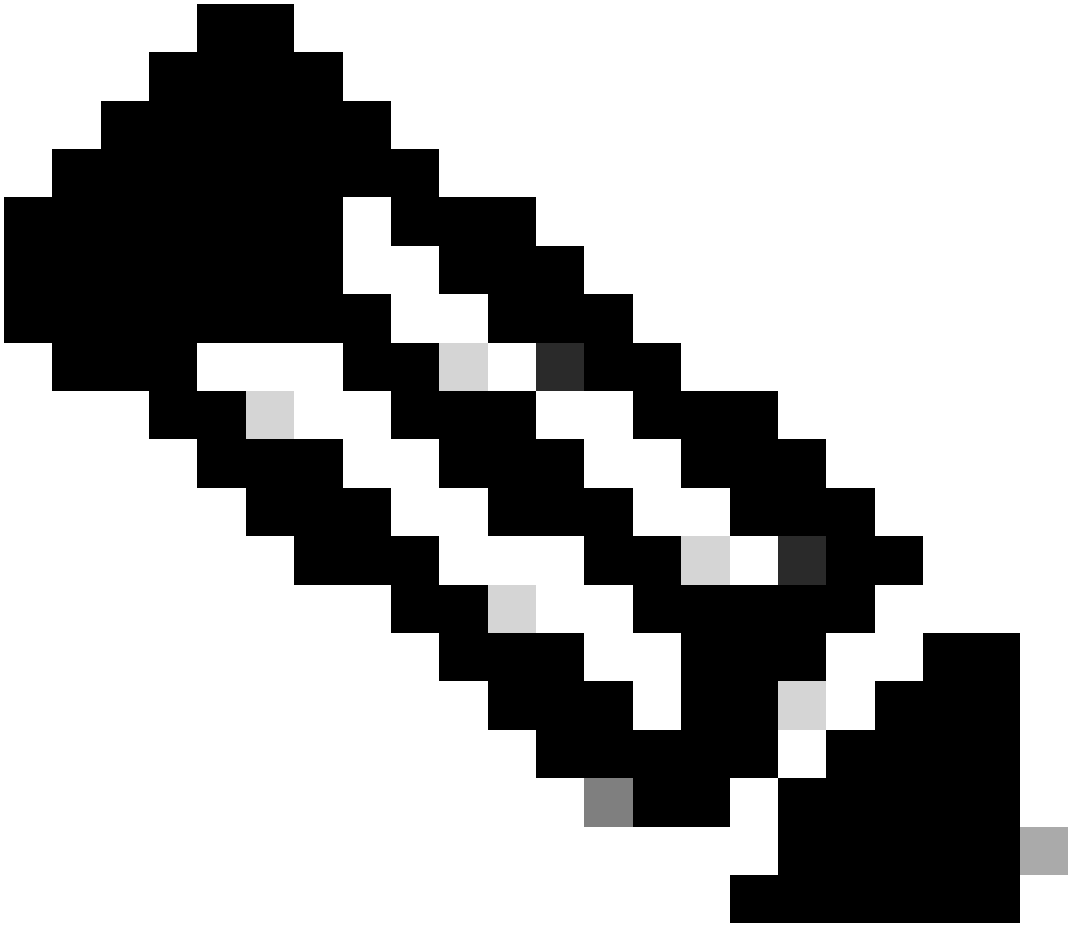
Componentes Utilizados

Nome	Platform	Versão
N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia





Observação: neste exemplo, N9K2 é o dispositivo configurado para Filtrar, Marcar e Classificar. O N9K1 e o N9K3 emulam a origem e o destino dos hosts.

Filtrando

A filtragem para Qualidade de Serviço (QoS) é essencial para garantir a utilização eficiente dos recursos da rede e priorizar o tráfego crítico. Em resumo, a filtragem para QoS é fundamental para otimizar o desempenho da rede, aprimorar a segurança, atender aos requisitos de conformidade e fornecer uma qualidade superior de experiência para os usuários finais. Gerenciando e controlando efetivamente os fluxos de tráfego, as organizações podem garantir a utilização eficiente dos recursos de rede enquanto mantêm a integridade e a segurança de suas redes.

Para este exemplo, o tráfego de 192.168.1.1 a 192.168.2 é filtrado, novas entradas podem ser adicionadas à lista de acesso para ter mais controle do tráfego.

Configurar

	Comando ou Ação	Propósito
Passo 1	N9K2# configure terminal	Entra no modo de configuração.
Passo 2	N9K2(config)# ip access-list marking-acl	Cria uma ACL para filtrar o tráfego.
Etapa 3	N9K2(config-acl)# permit ip host 192.168.1.1 host 192.168.20.2	Especificar IPs filtrados
Passo 4	N9K2(config-acl)# class-map type qos marking-class	Criar um mapa de classes para marcação de QoS
Etapa 5	N9K2(config-cmap-qos)# match access-group name marking-acl	Faça a correspondência da ACL criada na etapa 2

Marcação e classificação

Marcar e classificar o tráfego para Qualidade de Serviço (QoS) é fundamental para otimizar o desempenho da rede, garantir a alocação eficiente de recursos e aprimorar a experiência do usuário. Marcar e classificar o tráfego para QoS são práticas essenciais para otimizar o desempenho da rede, garantir a utilização eficiente de recursos e fornecer uma qualidade consistente de experiência para os usuários. Gerenciando e priorizando com eficiência os fluxos de tráfego, as organizações podem maximizar o valor de sua infraestrutura de rede enquanto mantêm a integridade e a segurança de seus ativos digitais.

Para este exemplo, o tráfego que já está filtrado é marcado com o valor de DSCP 5 e é classificado no grupo de QoS 7.

Configurar

	Comando ou Ação	Propósito
Passo 1	N9K2# configure terminal	Entra no modo de configuração.
Passo 2	N9K2(config)# policy-map type qos ingress-classify	Cria um mapa de políticas para classificar e marcar o tráfego
Etapa 3	N9K2(config-pmap-qos)# class marking-class	Anexar classe de marcação ao mapa de políticas criado
Passo 4	N9K2(config-pmap-c-qos)# set dscp 5	Define o valor de DSCP como 5 para todas as classes de marcação de correspondência de tráfego
Etapa 5	N9K2(config-pmap-c-qos)# set	Classificar a classe de

	qos-group 7	marcação de correspondência de tráfego para o grupo de QoS 7
Etapa 6	N9K2(config-pmap-c-qos)# interface ethernet 1/46	Inserir configuração de interface
Etapa 7	N9K2(config-ip)# service-policy type qos input ingress-classify	Aplicar política de serviço à interface de entrada

Etapas de resumo

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

Verificar

Verificar Marcação

Para verificar se a marcação foi executada corretamente, é necessário executar uma captura de pacote.

Para este exemplo, isso pode ser obtido executando uma captura de SPAN na interface e1/47 (interface de saída) no N9K2 ou executando uma captura de ELAM na interface e1/47 (interface de entrada) no N9K3.

	Comando ou Ação	Propósito
Passo 1	N9K3# show hardware internal tah interface e1/47 | include ignore-case asic|slice|srcid Asic: 0 Asic: 0 AsicPort: 54 Id de orig.: 28 Fatia: 1	Identifica ASIC, Fatia e ID de origem da interface onde o tráfego marcado é recebido.
Passo 2	N9K3(TAH-elam-insel6)# attach module 1	Conecte ao módulo onde a porta frontal reside.
Etapa 3	module-1# debug platform internal tah elam asic 0	Inicia a configuração do ELAM no ASIC 0.

Passo 4	module-1(TAH-elam)# trigger init asic 0 slice 1 use-src-id 28	Defina os parâmetros de acionamento usando Asic=0, Slice=1 e SrcId=28 obtidos da etapa 1.
Etapa 5	module-1(TAH-elam-insel6)# set outer ipv4 src_ip 192.168.1.1 dst_ip 192.168.20.2	Defina filtros para capturar tráfego específico .
Etapa 6	module-1(TAH-elam-insel6)# start	Inicia a captura.
Etapa 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	Exibe a captura; o valor de DSCP de 5 pode ser observado (destacado)

Verificar classificação

As informações de enfileiramento da interface de saída podem ser analisadas para verificar se o tráfego está classificado corretamente.

Neste exemplo, 5 pacotes foram enviados de 192.168.1.1 a 192.168.2, conforme observado, 5 pacotes são exibidos na direção TX para o grupo de QoS 7 confirmando que a classificação foi feita corretamente.

	Comando ou Ação	Propósito
Passo 1	<#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| +---+	A classe de Marcação de correspondência de tráfego é classificada no grupo de QoS 7.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.