

QOS (filter, markering en classificatie) configureren op Nexus 9000

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Topologie](#)

[Filtering](#)

[Configureren](#)

[Markering en classificatie](#)

[Configureren](#)

[Samenvatting stappen](#)

[Verifiëren](#)

[Controleer de markering](#)

[Controleer de classificatie](#)

Inleiding

Dit document beschrijft hoe u Quality of Service (filter, markering en classificatie) kunt configureren en controleren op Nexus 9000 switches.

Achtergrondinformatie

Het markeren en classificeren van verkeer in Quality of Service (QoS) is essentieel voor netwerkprestaties en om ervoor te zorgen dat kritieke toepassingen het benodigde serviceniveau ontvangen.

Samenvatting van het gebruik ervan:

1. Traffic Differentiation: netwerken dragen verschillende soorten verkeer over, zoals spraak, video, gegevens en realtime toepassingen. Door verkeer te markeren en te classificeren kunnen netwerkbeheerders onderscheid maken tussen deze typen op basis van hun belang, gevoeligheid voor vertraging en bandbreedtevereisten.
2. Resource Allocation: door verkeer te classificeren, kunnen netwerkapparaten bronnen zoals bandbreedte, bufferruimte, en verwerkingscapaciteit effectiever toewijzen. Kritieke toepassingen kunnen voorrang krijgen over minder tijdgevoelig verkeer en ervoor zorgen dat ze de benodigde bronnen ontvangen om optimaal te functioneren.

3. QoS-garanties: door verkeer te markeren en te classificeren kunt u QoS-beleid implementeren dat overeenkomsten op serviceniveau (SLA's) afdwingt en bepaalde prestatie maatstaven voor specifieke toepassingen of gebruikersgroepen garandeert. Dit garandeert een consistente ervaringskwaliteit voor eindgebruikers, waardoor de gevolgen van stremmingen of netwerkproblemen worden geminimaliseerd.
4. Congestiebeheer: in tijden van netwerkcongestie prioriteren QoS-mechanismen verkeer op basis van de classificatie ervan, om ervoor te zorgen dat kritieke toepassingen soepel blijven functioneren terwijl niet-essentieel verkeer mogelijk vertragingen ondervindt of wordt weggelaten. Dit helpt netwerkstabiliteit te handhaven en voorkomt achteruitgang van de service voor belangrijke toepassingen.
5. Geoptimaliseerd netwerkgebruik: door verkeer intelligent te beheren via QoS-mechanismen, worden netwerkbronnen efficiënter gebruikt. Ongebruikte bandbreedte kan dynamisch worden toegewezen aan toepassingen met een hoge prioriteit en de algehele prestaties van het netwerk worden gemaximaliseerd.
6. Uitgebreide gebruikerservaring: Het markeren en classificeren van verkeer op basis van zijn belang voor gebruikers of het bedrijf stelt organisaties in staat om een betere gebruikerservaring te leveren. Kritieke toepassingen zoals VoIP of videoconferencing krijgen prioriteit, wat resulteert in duidelijkere gesprekken, vloeiender videostreamen en een verbeterde productiviteit.
7. Beveiliging en naleving: QoS kan ook worden gebruikt om beveiligingsbeleid af te dwingen door prioriteit te geven aan verkeer van vertrouwde bronnen of door traffic shaping toe te passen om de bandbreedte voor bepaalde soorten verkeer te beperken, zoals het delen van peer-to-peer bestanden of streaming services. Bovendien kunnen QoS-mechanismen organisaties helpen aan de nalevingsvereisten te voldoen door te zorgen voor prioritering en bescherming van gevoelige gegevensstromen.

Over het algemeen zijn het markeren en classificeren van verkeer in QoS essentiële componenten van netwerkbeheer, waardoor organisaties de prestaties kunnen optimaliseren, betrouwbare servicelevering kunnen waarborgen en kunnen voldoen aan de diverse eisen van moderne toepassingen en gebruikers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

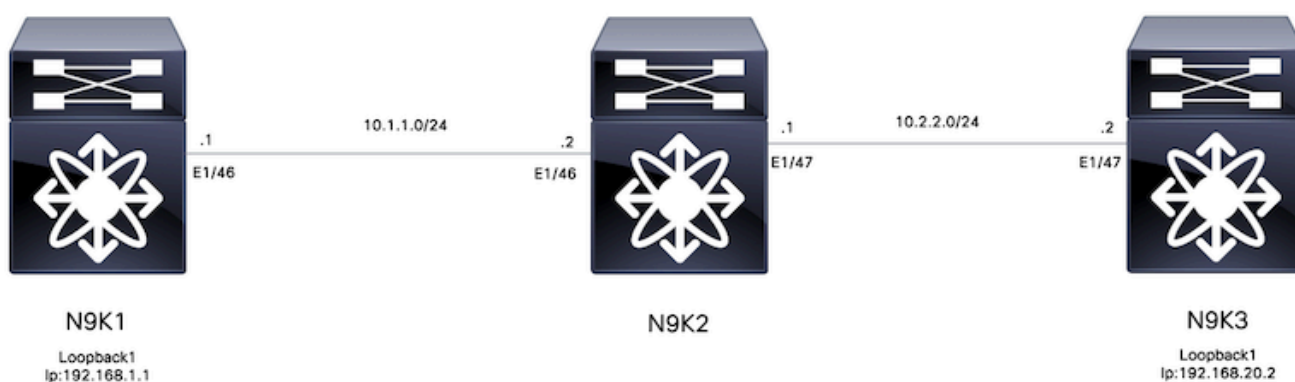
- NXOS-platform
- QoS
- Elam understanding
- Toeganglijsten (ACL)

Gebruikte componenten

Naam	Platform	Versie
N9K1	N9K-C93108TC-EX	9.3(10)
N9K2	N9K-C93108TC-EX	9.3(10)
N9K3	N9K-C93108TC-EX	9.3(10)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Topologie





Opmerking: In dit voorbeeld is N9K2 het apparaat dat is geconfigureerd voor filteren, markering en classificatie. N9K1 en N9K3 emuleren hostbron en -bestemming.

Filtering

Filtering voor Quality of Service (QoS) is essentieel om een efficiënt gebruik van netwerkbronnen te garanderen en prioriteit te geven aan kritisch verkeer. Samengevat is filteren voor QoS van cruciaal belang voor het optimaliseren van netwerkprestaties, het verbeteren van de beveiliging, het voldoen aan nalevingsvereisten en het leveren van een superieure ervaringskwaliteit voor eindgebruikers. Door verkeersstromen effectief te beheren en te controleren kunnen organisaties een efficiënt gebruik van netwerkresources waarborgen zonder de integriteit en beveiliging van hun netwerken in het gedrang te brengen.

Dit voorbeeldverkeer van 192.168.1.1 tot 192.168.2 wordt gefiltreerd, kunnen nieuwe ingangen aan de toegang-lijst worden toegevoegd om meer controle van het verkeer te hebben.

Configureren

	Opdracht of handeling	Doel
Stap 1	N9K2# terminal configureren	Hiermee gaat u de configuratiemodus in.
Stap 2	N9K2 (configuratie)# IP-toegangslijst markering-acl	Maakt ACL om verkeer te filteren.
Stap 3	N9K2 (config-acl)# laat IP-host 192.168.1.1 host 192.168.20.2 toe	IP's opgeven die worden gefilterd
Stap 4	N9K2(config-acl)# class-map type qos markering-klasse	Class-map voor QoS-markering maken
Stap 5	N9K2(config-cmap-qos)# overeenkomende naam van toegangsgroep markering-acl	Overeenkomende ACL gemaakt in stap 2

Markering en classificatie

Het markeren en classificeren van verkeer voor Quality of Service (QoS) is essentieel voor het optimaliseren van netwerkprestaties, het garanderen van een efficiënte toewijzing van bronnen en het verbeteren van de gebruikerservaring, het markeren en classificeren van verkeer voor QoS zijn essentiële praktijken voor het optimaliseren van netwerkprestaties, het verzekeren van een efficiënt gebruik van bronnen en het leveren van een consistente kwaliteit van ervaring voor gebruikers. Door verkeersstromen effectief te beheren en prioriteren, kunnen organisaties de waarde van hun netwerkinfrastructuur maximaliseren terwijl ze de integriteit en beveiliging van hun digitale bedrijfsmiddelen behouden.

Dit voorbeeldverkeer dat al is gefilterd, wordt gemarkeerd met DSCP-waarde 5 en wordt geclassificeerd in QoS-groep 7.

Configureren

	Opdracht of handeling	Doel
Stap 1	N9K2# terminal configureren	Hiermee gaat u de configuratiemodus in.
Stap 2	N9K2(config)# beleidsmaptype qos indringing-classificeren	Maakt beleidskaart om verkeer te classificeren en te markeren
Stap 3	N9K2(config-pmap-qos)# class markering-klasse	Hang markeringsklasse aan gemaakte beleidskaart
Stap 4	N9K2(config-pmap-c-qos)# ingesteld DSCP 5	Stel DSCP-waarde van 5 in op alle traffic matching-markeringsklasse

Stap 5	N9K2(config-pmap-c-qos)# ingestelde qos-groep 7	Classificeren van traffic matching-markeringsklasse met QoS-groep 7
Stap 6	N9K2(config-pmap-c-qos)# interface Ethernet 1/46	Voer interfaceconfiguratie in
Stap 7	N9K2 (configuratie-ip)# type voor servicebeleid qos ingangsclassificatie	Servicebeleid toepassen op toegangsinterface

Samenvatting stappen

1. configureer terminal
2. IP-toegangslijst markering-acl
3. vergunning ip host 192.168.1.1 host 192.168.20.2
4. klasse-kaart type qos markering-klasse
5. match access-group name markering-acl
6. qos ingress-classificeren
7. klasse-aanduidingen
8. reeks qos-groep 7
9. interface-Ethernet 1/46
10. type servicebeleid qos ingangen-classificeren

Verifiëren

Controleer de markering

Om te verifiëren of de markering correct is uitgevoerd, moet een pakketopname worden uitgevoerd.

Dit kan bijvoorbeeld worden bereikt door een SPAN-opname uit te voeren op interface e1/47 (uitgaande interface) op N9K2 of door een ELAM-opname uit te voeren op interface e1/47 (ingangside interface) op N9K3.

	Opdracht of handeling	Doel
Stap 1	N9K3# toont hardware interne tah interface e1/47 negecase asic slice srcid toevoegen Aziatisch: 0 Aziatisch: 0 AsicPort: 54 SRCid: 28 Segment: 1	Identificeert ASIC, Slice en bron-ID vanuit de interface waar gemarkeerd verkeer wordt ontvangen.
Stap 2	N9K3(TAH-elam-insel6)# koppelingsmodule 1	Bevestig deze aan de module waar de voorpoort zich bevindt.

Stap 3	module-1# debug platform interne tah elam asic 0	Start ELAM-configuratie op ASIC 0.
Stap 4	module-1 (TAH-elam)# trigger in asic 0 slice 1 use-src-id 28	Stel triggerparameters in met Asic=0, Slice=1 en SrcId=28 uit stap 1.
Stap 5	module-1 (TAH-elam-insel6)# router ipv4 src_ip 192.168.1.1 dst_ip 192.168.20.2	Filters instellen om specifiek verkeer op te nemen .
Stap 6	module-1 (TAH-elam-insel6)# start	Begint te vangen.
Stap 7	<pre> <#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 </pre>	Hier wordt DSCP-waarde van 5 weergegeven (gemarkeerd)

Controleer de classificatie

De informatie van de wachtrij van de uitgangsinterface kan worden bekeken om te verifiëren als het verkeer correct wordt geclassificeerd.

5 pakketten werden verzonden van 192.168.1.1 naar 192.168.2, zoals 5 pakketten worden weergegeven in de TX richting voor QoS groep 7 bevestigend dat de classificatie correct wordt uitgevoerd.

	Opdracht of handeling	Doel
Stap 1	<pre> <#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 +-----+ </pre>	Traffic matching markering klasse is geclassificeerd op QoS groep 7.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.