Configurer QoS sur GRE de tunnel

Table des matières

Introduction

Ce document décrit comment configurer et dépanner QoS sur tunnel GRE dans le modèle Nexus 9300 (EX-FX-GX).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- QoS
- Tunnel GRE
- Nexus 9000

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Matériel : N9K-C9336C-FX2
- Version : 9.3(8)

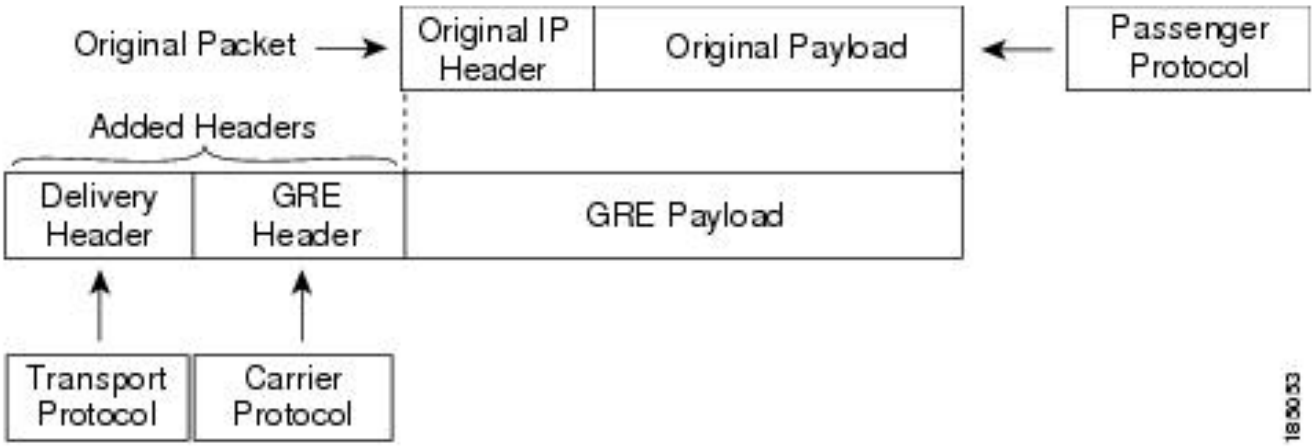
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Vous pouvez utiliser l'encapsulation de routage générique (GRE) comme protocole opérateur pour divers protocoles de transport de passagers.

Vous voyez dans l'image que les composants du tunnel IP pour un tunnel GRE. Le paquet de protocole passager d'origine devient la charge utile GRE et le périphérique ajoute un en-tête GRE au paquet.

Le périphérique ajoute ensuite l'en-tête du protocole de transport au paquet et le transmet.



Le trafic est traité en fonction de la façon dont vous le classifiez et des stratégies que vous créez et appliquez aux classes de trafic.

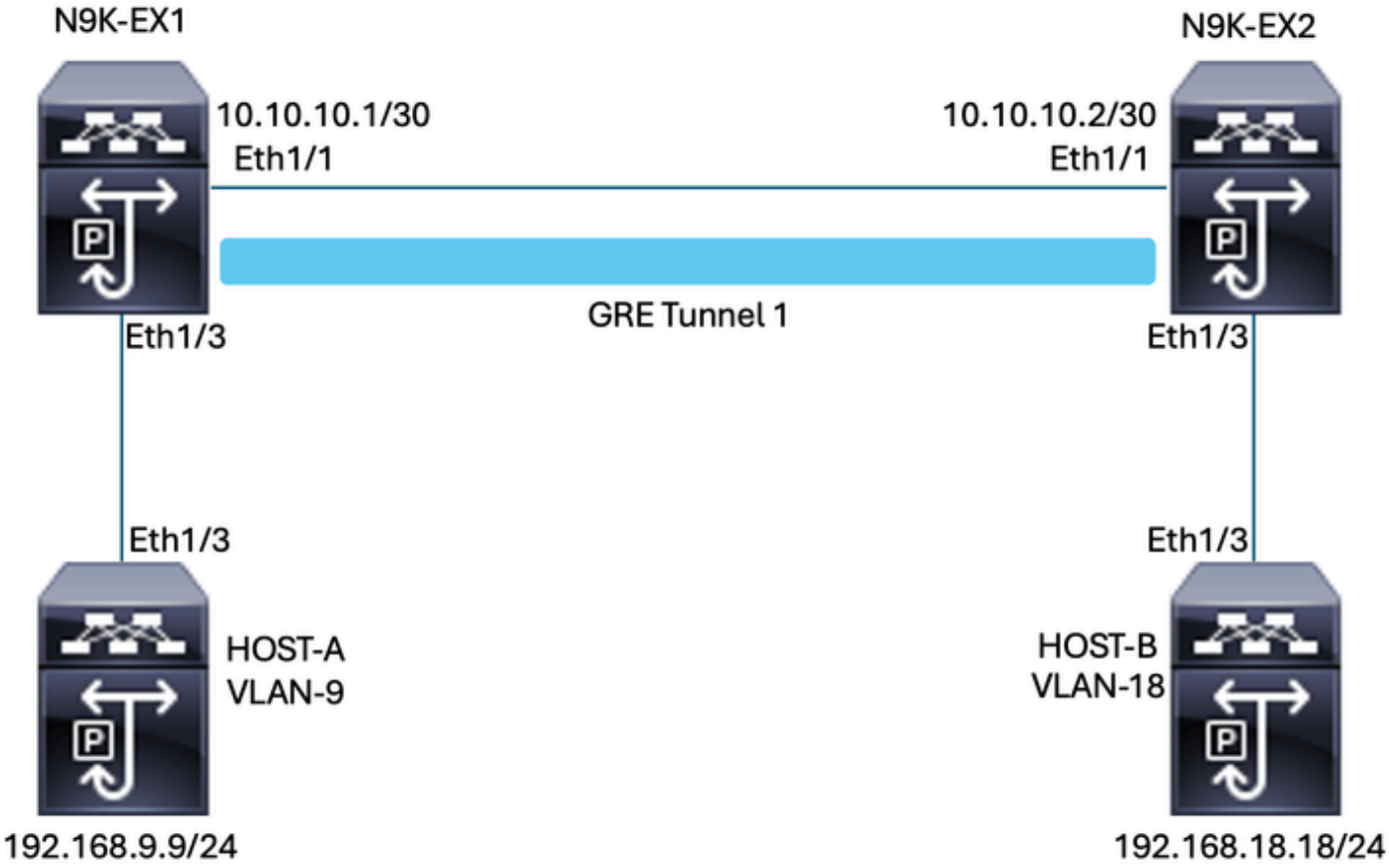
Pour configurer les fonctions QoS, procédez comme suit :

1. Des classes sont créées pour classer les paquets entrants vers le réseau qui correspondent à des critères tels que l'adresse IP ou les champs QoS.
2. Crée des politiques qui spécifient les actions à entreprendre sur les classes de trafic, telles que surveiller, marquer ou rejeter des paquets.
3. Appliquez des politiques à un port, un canal de port, un VLAN ou une sous-interface.

Valeurs DSCP couramment utilisées

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2

Diagramme du réseau



Configurer

L'objectif de la configuration de la QoS sur le tunnel GRE est de définir un DSCP pour le trafic d'un certain VLAN à traverser le tunnel GRE entre N9K-EX1 et N9K-EX2.

Le Nexus encapsule le trafic et l'envoie sur le tunnel GRE sans perte de marquage QoS comme vous l'avez fait précédemment dans le VLAN pour la valeur DSCP, dans ce cas la valeur de DSCP AF-11 est utilisée pour le VLAN 9.

Hôte-A

```
interface Ethernet1/3
  switchport
  switchport access vlan 9
  no shutdown

interface Vlan9
  no shutdown
  ip address 192.168.9.9/24
```

Hôte-B

```
interface Ethernet1/3
```

```
switchport
switchport access vlan 18
no shutdown

interface Vlan18
no shutdown
ip address 192.168.18.18/24
```

Configuration des interfaces N9K-EX1

```
interface Ethernet1/1
ip address 10.10.10.1/30
no shutdown

interface Ethernet1/3
switchport
switchport access vlan 9
no shutdown

interface Tunnel1
ip address 172.16.1.1/30
tunnel source Ethernet1/1
tunnel destination 10.10.10.2
no shutdown

interface Vlan9
no shutdown
ip address 192.168.9.1/24
```

Configuration du routage N9K-EX1

```
ip route 0.0.0.0/0 Tunnel
```

Configuration QoS N9K-EX1

Comme la QoS n'est pas prise en charge sur l'interface de tunnel GRE dans NXOS, il est nécessaire de configurer et d'appliquer la stratégie de service dans la configuration VLAN. Comme vous pouvez le voir, créez d'abord la liste de contrôle d'accès pour qu'elle corresponde à la source et à la destination, puis définissez la configuration QoS avec le DSCP souhaité et enfin utilisez la stratégie de service pour la configuration VLAN.

```
ip access-list TAC-QoS-GRE
10 permit ip any 192.168.18.0/24
class-map type qos match-all CM-TAC-QoS-GRE
match access-group name TAC-QoS-GRE
policy-map type qos PM-TAC-QoS-GRE
class CM-TAC-QoS-GRE
```

```
set dscp 10

vlan configuration 9
service-policy type qos input PM-TAC-QoS-GRE
```

Configuration des interfaces N9K-EX2

```
interface Ethernet1/1
ip address 10.10.10.2/30
no shutdown

interface Ethernet1/3
switchport
switchport access vlan 18
no shutdown

interface Tunnel1
ip address 172.16.1.2/30
tunnel source Ethernet1/1
tunnel destination 10.10.10.1
no shutdown

interface Vlan18
no shutdown
ip address 192.168.18.1/24
```

Configuration du routage N9K-EX2

```
ip route 0.0.0.0/0 Tunnel
```

Dépannage

Vérification du tunnel

Les deux commandes :

- Show ip interface brief (afficher un aperçu de l'interface IP)
- show interface tunnel 1 brief

S'affiche si le tunnel est actif.

```
N9K-EX1# show ip interface brief

IP Interface Status for VRF "default"(1)
```

```
Interface IP Address Interface Status
Vlan9 192.168.9.1 protocol-up/link-up/admin-up
Tunnel1 172.16.1.1 protocol-up/link-up/admin-up
Eth1/1 10.10.10.1 protocol-up/link-up/admin-up


N9K-EX1# show interface tunnel 1 brief

--------------------------------------------------------------------------------
---------------------------
Interface Status IP Address
Encap type MTU
--------------------------------------------------------------------------------
---------------------------
Tunnel1 up 172.16.1.1/30
GRE/IP 1476
```

Les deux commandes

- show interface tunnel 1
- show interface tunnel 1 counters

Affiche des informations similaires telles que les paquets reçus et transmis.

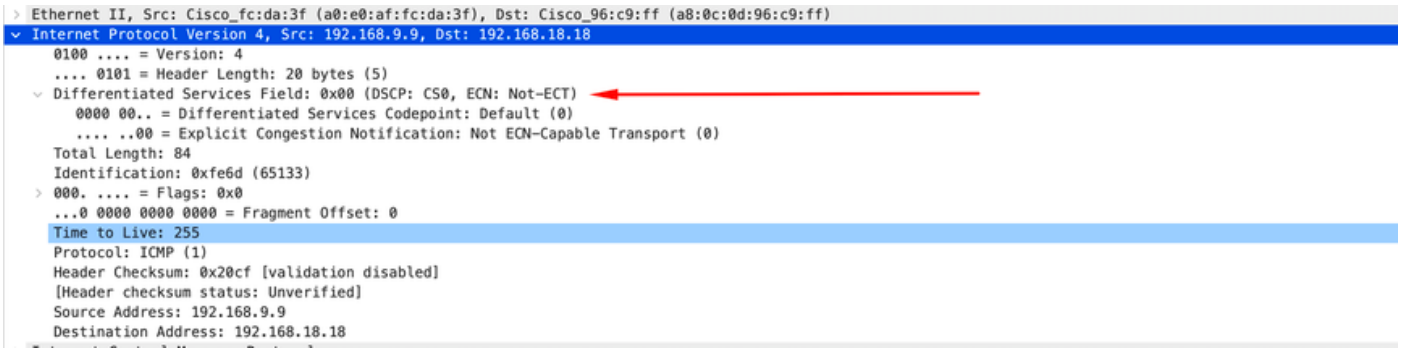
```
N9K-EX1# show interface tunnel 1
Tunnel1 is up
Admin State: up
Internet address is 172.16.1.1/30
MTU 1476 bytes, BW 9 Kbit
Tunnel protocol/transport GRE/IP
Tunnel source 10.10.10.1 (Ethernet1/1), destination 10.10.10.2
Transport protocol is in VRF "default"
Tunnel interface is in VRF "default"
Last clearing of "show interface" counters never
Tx
3647 packets output, 459522 bytes
Rx
3647 packets input, 459522 bytes

N9K-EX1# show interface tunnel 1 counters

--------------------------------------------------------------------------------
--
Port InOctets InUcastPk
ts
--------------------------------------------------------------------------------
--
Tunnel1 459522 36
47

--------------------------------------------------------------------------------
--
Port InMcastPkts InBcastPk
ts
--------------------------------------------------------------------------------
--
```

```
Tunnel1 --
--

--------------------------------------------------------------------------------
--
Port OutOctets OutUcastPk
ts
--------------------------------------------------------------------------------
--
Tunnel1 459522 36
47

--------------------------------------------------------------------------------
--
Port OutMcastPkts OutBcastPk
ts
--------------------------------------------------------------------------------
--
Tunnel1 --
--
N9K-EX1#
```

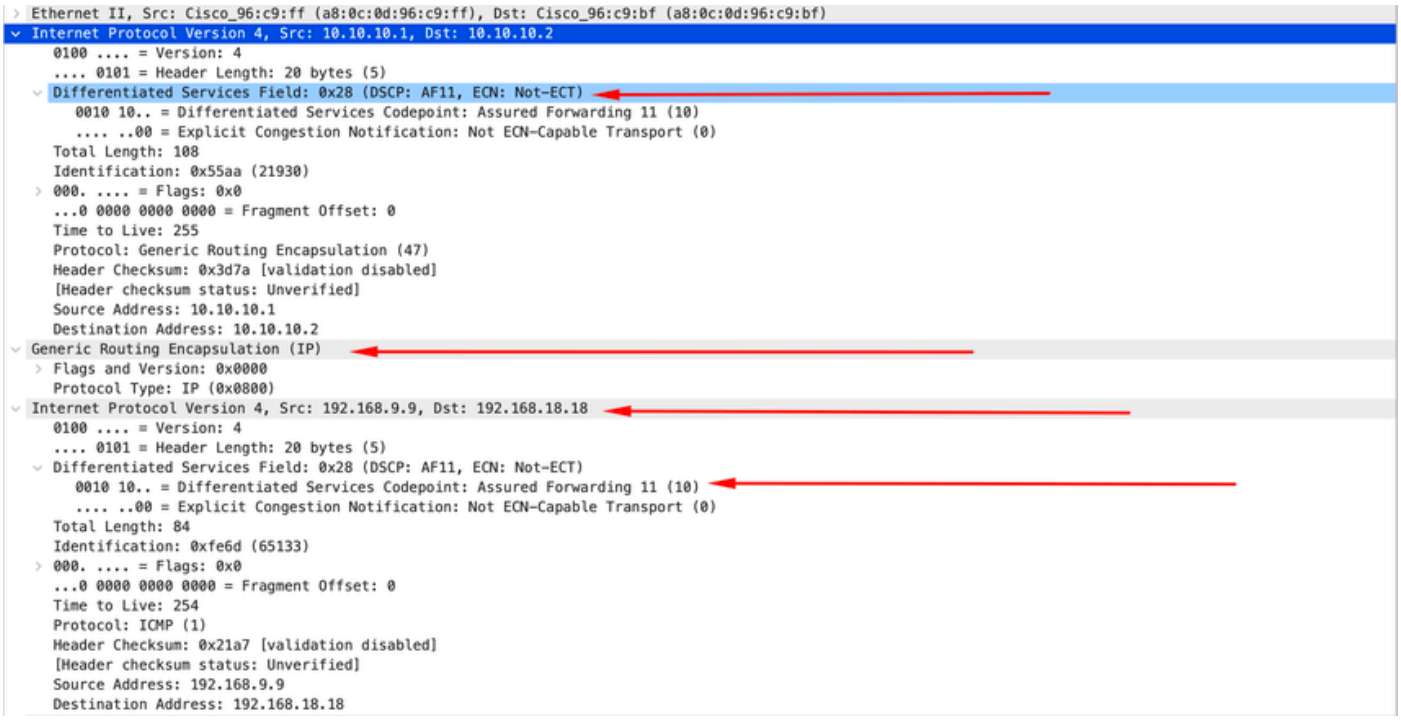
Captures de trafic

Captures SPAN

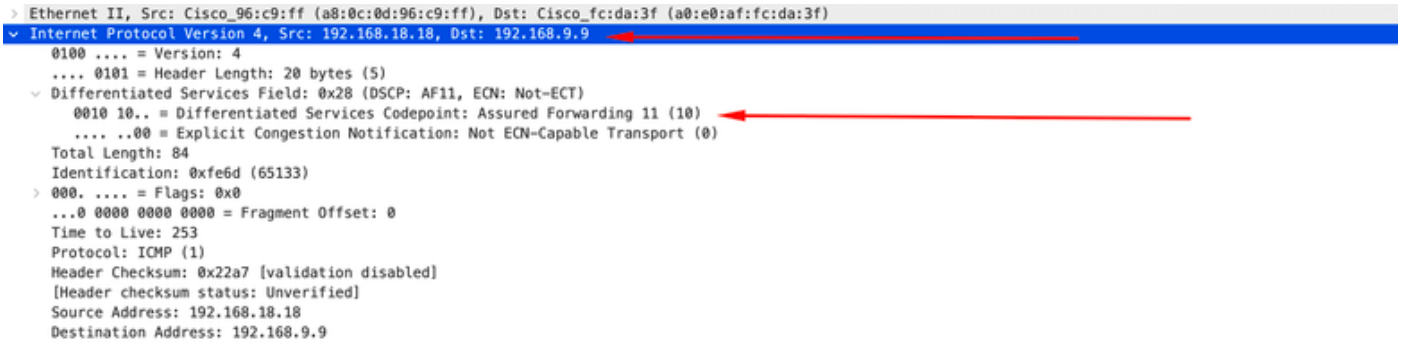
Cette image montre la capture de la requête ARP à l'entrée de l'interface Ethernet 1/3 sur le commutateur N9K-EX1. Vous pouvez voir que le trafic n'est pas encore marqué avec le DSCP (AF11) que vous voulez utiliser puisque la capture est à l'entrée du commutateur.



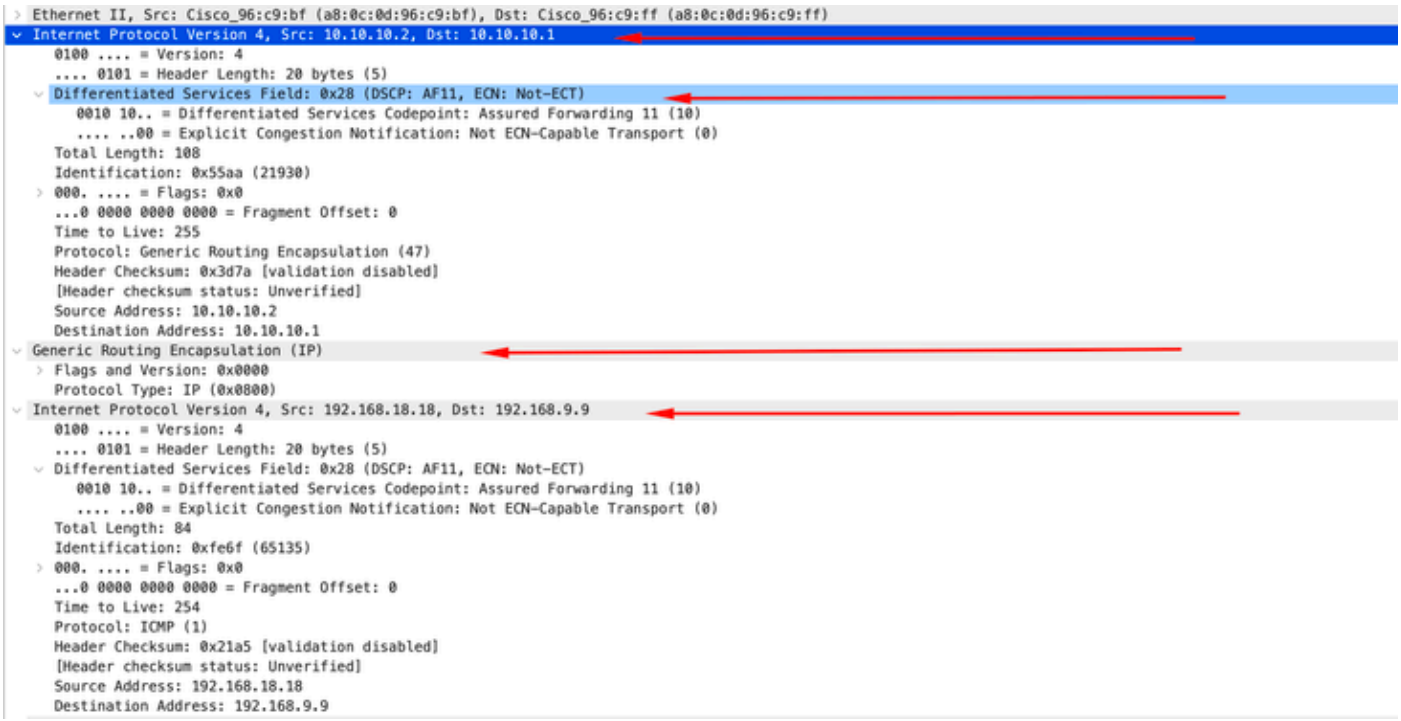
L'image montre la capture de la requête ARP à l'entrée de l'interface Ethernet 1/1 sur le commutateur N9K-EX2. Vous pouvez voir que le trafic a déjà la valeur DSCP AF11 que vous devez utiliser. Vous remarquerez également que le paquet est encapsulé par le tunnel qui est configuré entre les deux Nexus.



L'image montre la capture de la réponse ARP à la sortie de l'interface Ethernet 1/3 sur le commutateur N9K-EX1. Vous pouvez voir que le trafic a toujours la valeur DSCP AF11 que vous devez utiliser. Vous remarquerez également que le paquet n'est pas encapsulé par le tunnel qui est configuré entre les deux Nexus.



Cette image montre la capture de la réponse ARP à la sortie de l'interface Ethernet 1/1 sur le commutateur N9K-EX2. Vous pouvez voir que le trafic a toujours la valeur DSCP AF11 que vous devez utiliser. Vous remarquerez également que le paquet est encapsulé par le tunnel qui est configuré entre les deux Nexus.



Il est important de noter que les captures de paquets n'indiquent pas l'IP du tunnel pour l'encapsulation puisque le Nexus utilise les physiques. Il s'agit du comportement naturel du Nexus lors de l'utilisation de la tunnellisation GRE puisqu'ils utilisent les IP physiques pour acheminer les paquets.

Capture ELAM

Utilisez la capture ELAM sur N9KEX-2 avec la sélection interne 9 pour afficher l'en-tête l3 externe et l'en-tête l3 interne. Vous devez filtrer par l'adresse IP source et cible.

```
debug platform internal tah elam
trigger init in-select 9
reset
set inner ipv4 src_ip 192.168.9.9 dst_ip 192.168.18.18
start
report
```

Vous pouvez vérifier que le Nexus reçoit le paquet via l'interface 1/1. En outre, vous voyez que l'en-tête L3 externe est l'adresse IP physique des interfaces qui sont directement connectées et que l'en-tête L3 interne a les adresses IP de l'hôte A et de l'hôte B.

```
SUGARBOWL ELAM REPORT SUMMARY
slot - 3, asic - 1, slice - 0
==============================

Incoming Interface: Eth1/1
Src Idx : 0x41, Src BD : 4433
Outgoing Interface Info: dmod 2, dpid 10
```

```
Dst Idx : 0x3, Dst BD : 18

Packet Type: IPv4

Outer Dst IPv4 address: 10.10.10.2
Outer Src IPv4 address: 10.10.10.1
Ver = 4, DSCP = 10, Don't Fragment = 0
Proto = 47, TTL = 255, More Fragments = 0
Hdr len = 20, Pkt len = 108, Checksum = 0x3d7a

Inner Payload
Type: IPv4

Inner Dst IPv4 address: 192.168.18.18
Inner Src IPv4 address: 192.168.9.9

L4 Protocol : 47
L4 info not available

Drop Info:
----------

LUA:
LUB:
LUC:
LUD:
Final Drops:
```

Dépannage de QoS

Vous pouvez vérifier la configuration QoS comme indiqué .

```
N9K-EX1# show running-config ipqos

!Command: show running-config ipqos
!Running configuration last done at: Thu Apr 4 11:45:37 2024
!Time: Fri Apr 5 11:50:54 2024

version 9.3(8) Bios:version 08.39
class-map type qos match-all CM-TAC-QoS-GRE
match access-group name TAC-QoS-GRE
policy-map type qos PM-TAC-QoS-GRE
class CM-TAC-QoS-GRE
set dscp 10

vlan configuration 9
service-policy type qos input PM-TAC-QoS-GRE
```

Vous pouvez afficher les stratégies QoS configurées sur le VLAN spécifié, ainsi que les paquets qui correspondent à la liste de contrôle d'accès associée au policy-map.

```
N9K-EX1# show policy-map vlan 9


Global statistics status : enabled

Vlan 9

Service-policy (qos) input: PM-TAC-QoS-GRE
SNMP Policy Index: 285219173

Class-map (qos): CM-TAC-QoS-GRE (match-all)

Slot 1
5 packets
Aggregate forwarded :
5 packets
Match: access-group TAC-QoS-GRE
set dscp 10
```

Vous pouvez également effacer les statistiques QoS à l'aide de la commande indiquée ici.

```
N9K-EX1# clear qos statistics
```

Vérifier la liste de contrôle d’accès programmée dans le logiciel

```
N9K-EX1# show system internal access-list vlan 9 input entries detail

slot 1
=======


Flags: F - Fragment entry E - Port Expansion
D - DSCP Expansion M - ACL Expansion
T - Cross Feature Merge Expansion
N - NS Transit B - BCM Expansion C - COPP


INSTANCE 0x2
---------------

Tcam 1 resource usage:
----------------------
LBL B = 0x1
Bank 2
------
IPv4 Class
Policies: QoS
Netflow profile: 0
Netflow deny profile: 0
Entries:
```

```
[Index] Entry [Stats]
---------------------
[0x0000:0x0000:0x0700] permit ip 0.0.0.0/0 192.168.18.0/24 [5]
```

Vérifier la liste de contrôle d'accès programmée dans le matériel

```
N9K-EX1# show hardware access-list vlan 9 input entries detail

slot 1
=======


Flags: F - Fragment entry E - Port Expansion
D - DSCP Expansion M - ACL Expansion
T - Cross Feature Merge Expansion
N - NS Transit B - BCM Expansion C - COPP


INSTANCE 0x2
---------------

Tcam 1 resource usage:
----------------------
LBL B = 0x1
Bank 2
------
IPv4 Class
Policies: QoS
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0x0000:0x0000:0x0700] permit ip 0.0.0.0/0 192.168.18.0/24 [5]
```

Avec la commande présentée ici, vous pouvez vérifier les ports qui utilisent le VLAN. Dans cet exemple, il s'agit de l'ID de VLAN 9 et vous pouvez également noter la stratégie QoS utilisée.

```
N9K-EX1# show system internal ipqos vlan-tbl 9

Vlan range asked: 9 - 9

==================================================

Vlan: 9, pointer: 0x132e3eb4, Node Type:  VLAN

IfIndex array:

    alloc count:    5, valid count:    1, array ptr : 0x13517aac          0: IfI

ndex: 0x1a000400 (Ethernet1/3)     Policy Lists (1): Flags: 01

        Type: INP QOS, Name: PM-TAC-QoS-GRE, Ghost Id: 0x45001c7, Real Id: 0x450
```

```
01c8

                        Defnode Id: 0x45001c9



================================================

N9K-EX1#
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.