Konfigurieren von QoS über Tunnel-GRE

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von QoS über Tunnel-GRE im Nexus 9300-Modell (EX-FX-GX).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- QoS
- Tunnel-GRE
- Nexus 9000

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

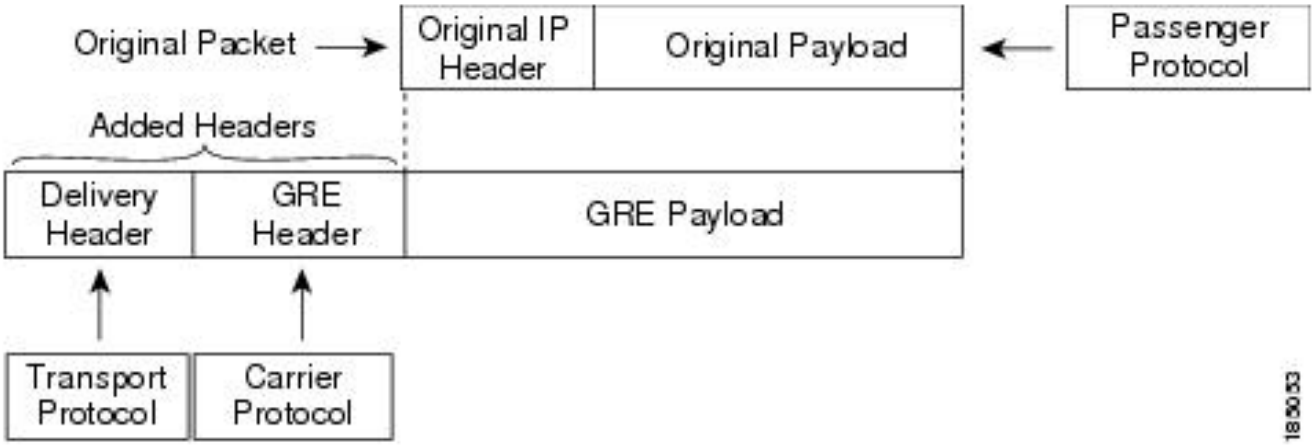
dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Sie können Generic Routing Encapsulation (GRE) als Trägerprotokoll für eine Reihe von Passagierprotokollen verwenden.

Im Bild sehen Sie, dass die IP-Tunnelkomponenten für einen GRE-Tunnel. Das ursprüngliche Passagierprotokollpaket wird zur GRE-Nutzlast, und das Gerät fügt dem Paket einen GRE-Header hinzu.

Das Gerät fügt dann dem Paket den Transportprotokoll-Header hinzu und sendet ihn.



Die Verarbeitung des Datenverkehrs basiert auf der Klassifizierung sowie auf den Richtlinien, die Sie erstellen und auf Datenverkehrsklassen anwenden.

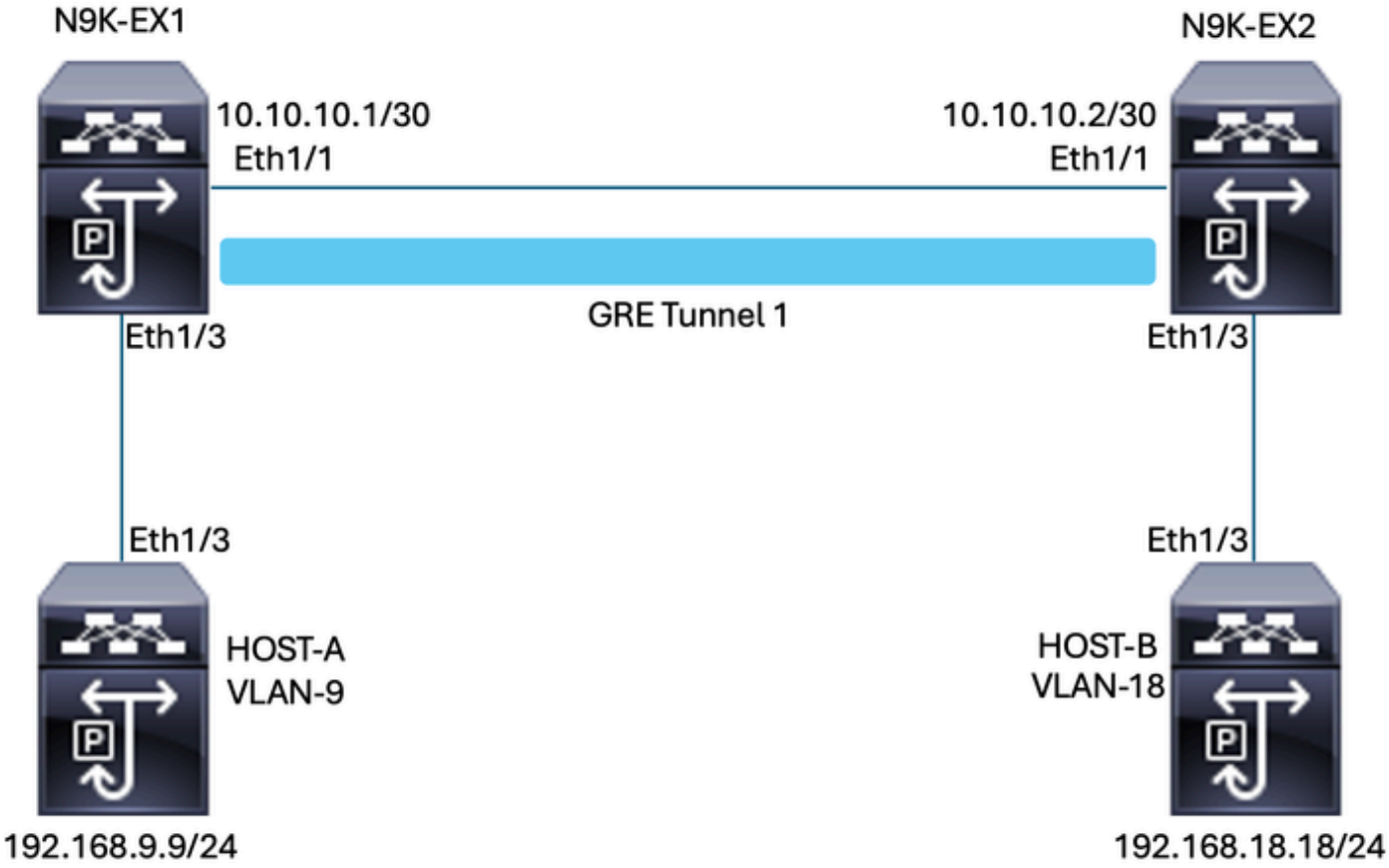
Gehen Sie wie folgt vor, um QoS-Funktionen zu konfigurieren:

1. Es werden Klassen erstellt, die eingehende Pakete an den Nexus klassifizieren, die Kriterien wie IP-Adresse oder QoS-Feldern entsprechen.
2. Erstellt Richtlinien, die die Aktionen für Datenverkehrsklassen festlegen, z. B. Pakete überwachen, markieren oder verwerfen.
3. Wenden Sie Richtlinien auf einen Port, Port-Channel, ein VLAN oder eine Subschnittstelle an.

Häufig verwendete DSCP-Werte

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

Netzwerkdiagramm



Konfigurieren

Ziel der Konfiguration von QoS über Tunnel-GRE ist es, einen DSCP für den Datenverkehr eines bestimmten VLAN festzulegen, der zwischen N9K-EX1 und N9K-EX2 durch den GRE-Tunnel verläuft.

Der Nexus kapselt den Datenverkehr und sendet ihn an die Tunnel-GRE, ohne dass die QoS-Markierung verloren geht, wie zuvor im VLAN für den DSCP-Wert. In diesem Fall wird der Wert von DSCP AF-11 für VLAN 9 verwendet.

Host A

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

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

Host B

```
interface Ethernet1/3
switchport
switchport access vlan 18
no shutdown

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

N9K-EX1-Schnittstellenkonfiguration

```
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
```

N9K-EX1 Routing-Konfiguration

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

N9K-EX1 QoS-Konfiguration

Da QoS auf der GRE-Tunnelschnittstelle in NX-OS nicht unterstützt wird, muss die Dienstrichtlinie in der VLAN-Konfiguration konfiguriert und angewendet werden. Wie Sie sehen, erstellen Sie zuerst die ACL, um die Quelle und das Ziel abzugleichen, und legen dann die QoS-Konfiguration mit dem gewünschten DSCP fest. Verwenden Sie dann schließlich die Service-Richtlinie für die VLAN-Konfiguration.

```
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
```

N9K-EX2 Schnittstellenkonfiguration

```
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
```

N9K-EX2 Routing-Konfiguration

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

Fehlerbehebung

Tunnelüberprüfung

Beide Befehle:

- show ip interface brief
- show interface tunnel 1 brief

Zeigt an, ob der Tunnel aktiv ist.

```
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
```

Beide Befehle

- Schnittstellentunnel 1 anzeigen
- Schnittstellentunnel 1-Zähler anzeigen

Zeigt ähnliche Informationen an, wie z. B. empfangene und übertragene Pakete.

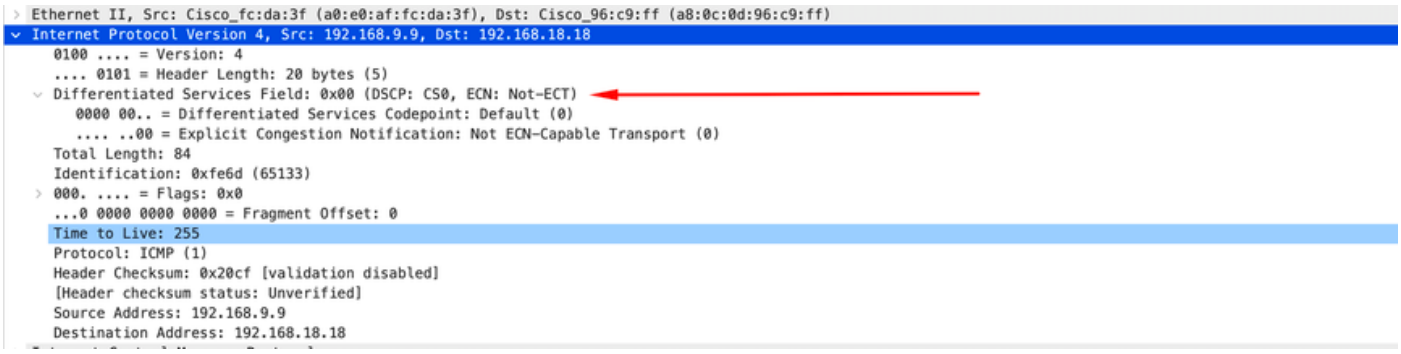
```
N9K-EX1# show interface tunnel 1
Tunnel1 is up
Admin State: up
Internet address is 172.16.1.1/30
MTU 1476 bytes, BW 9 Kbit
Tunnel protocol/transport GRE/IP
Tunnel source 10.10.10.1 (Ethernet1/1), destination 10.10.10.2
Transport protocol is in VRF "default"
Tunnel interface is in VRF "default"
Last 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#
```

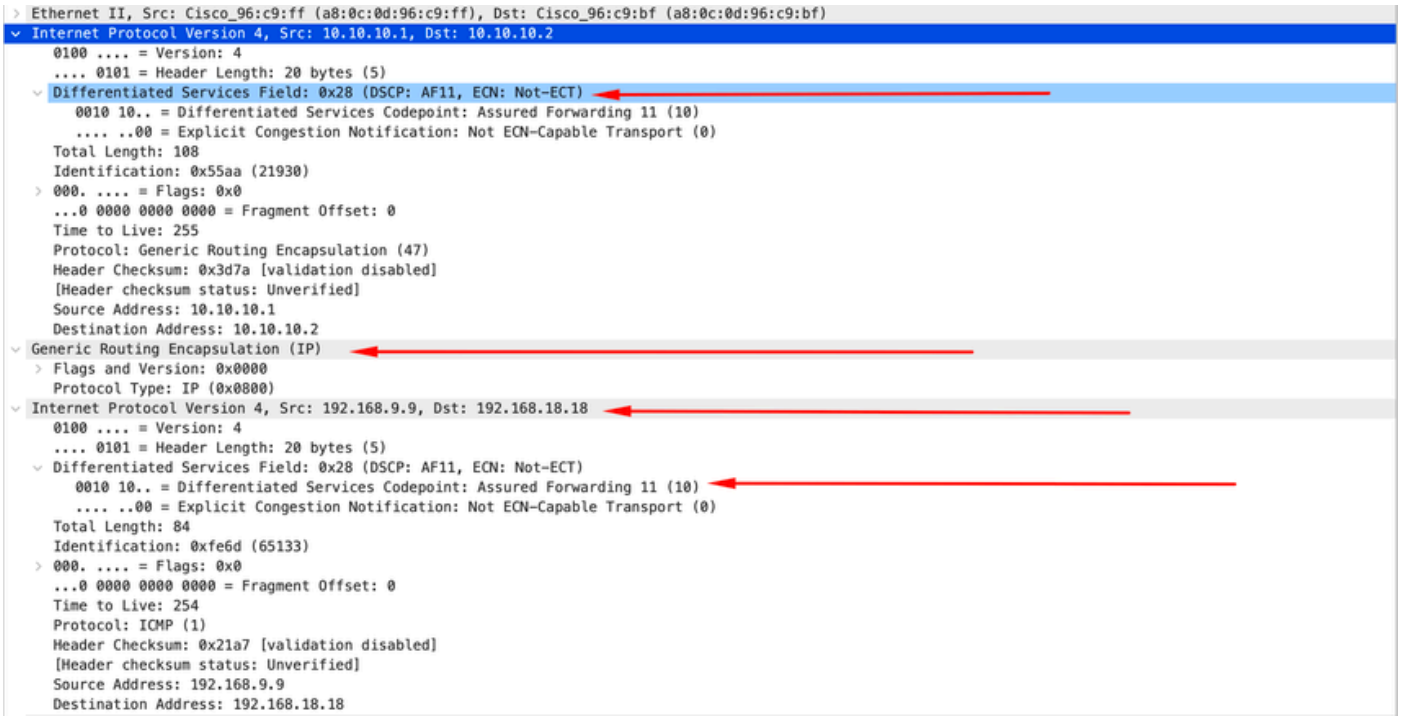
Datenerfassung

SPAN-Erfassung

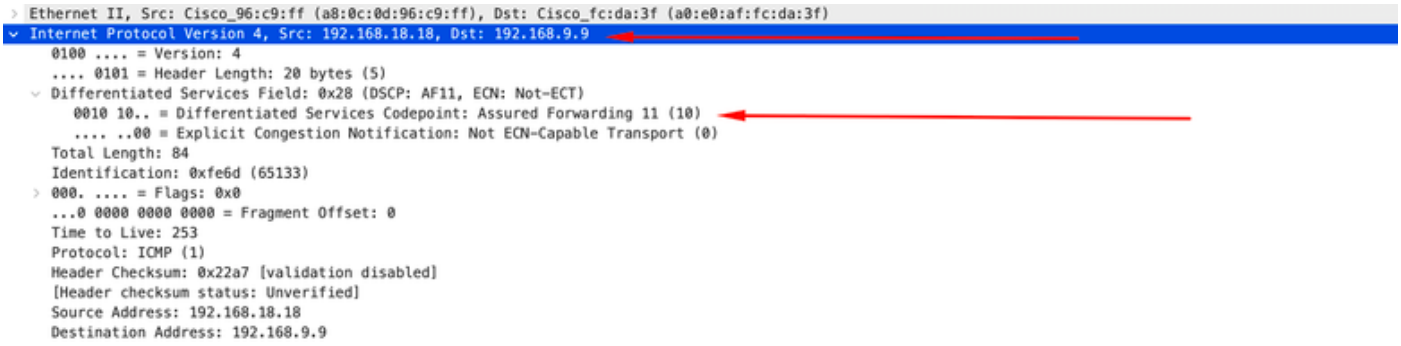
Dieses Bild zeigt die Erfassung der ARP-Anforderung am Eingang der Schnittstelle Ethernet 1/3 auf dem N9K-EX1-Switch. Sie können sehen, dass der Datenverkehr noch nicht mit dem DSCP (AF11) markiert ist, den Sie verwenden möchten, da die Erfassung am Eingang des Switches erfolgt.



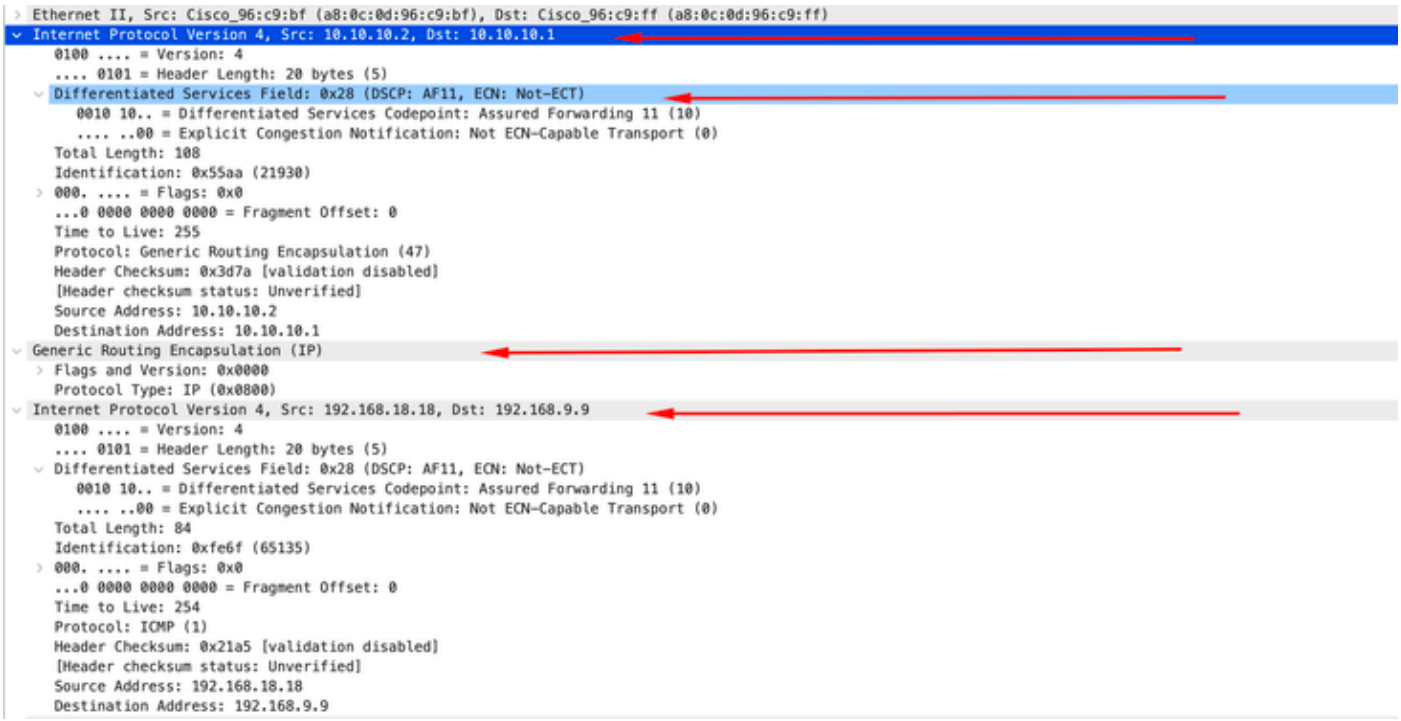
Das Bild zeigt die Erfassung der ARP-Anforderung am Eingang der Schnittstelle Ethernet 1/1 auf dem N9K-EX2-Switch. Wie Sie sehen, hat der Datenverkehr bereits den benötigten DSCP AF11-Wert. Sie stellen außerdem fest, dass das Paket von dem Tunnel gekapselt wird, der zwischen den beiden Nexus-Switches konfiguriert ist.



Das Bild zeigt die Erfassung der ARP-Antwort am Ausgang der Schnittstelle Ethernet 1/3 auf dem N9K-EX1-Switch. Wie Sie sehen, weist der Datenverkehr weiterhin den zu verwendenden DSCP AF11-Wert auf. Sie stellen außerdem fest, dass das Paket nicht von dem Tunnel gekapselt wird, der zwischen den beiden Nexus-Switches konfiguriert ist.



Dieses Bild zeigt die Erfassung der ARP-Antwort am Ausgang der Schnittstelle Ethernet 1/1 auf dem N9K-EX2-Switch. Wie Sie sehen, weist der Datenverkehr weiterhin den zu verwendenden DSCP AF11-Wert auf. Sie stellen außerdem fest, dass das Paket von dem Tunnel gekapselt wird, der zwischen den beiden Nexus-Switches konfiguriert ist.



Es ist wichtig zu beachten, dass die Paketerfassung nicht die Tunnel-IP für die Kapselung anzeigt, da der Nexus die physischen verwendet. Dies ist das natürliche Verhalten des Nexus bei der Verwendung von GRE-Tunneling, da die Pakete mithilfe der physischen IPs geroutet werden.

ELAM-Erfassung

Sie verwenden die ELAM-Erfassung auf N9KEX-2 mit in-select 9, um den äußeren l3- und inneren l3-Header anzuzeigen. Sie müssen nach der Quell- und Ziel-IP filtern.

```
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
```

Sie können überprüfen, ob der Nexus das Paket über die Schnittstelle 1/1 empfängt. Außerdem sehen Sie, dass der äußere L3-Header die physische IP-Adresse der Schnittstellen ist, die direkt verbunden sind, und der innere L3-Header die IPs von Host A und Host B hat.

```
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:
```

Fehlerbehebung: QoS

Sie können die QoS-Konfiguration wie dargestellt überprüfen.

```
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
```

Sie können die im angegebenen VLAN konfigurierten QoS-Richtlinien und die Pakete anzeigen, die mit der ACL übereinstimmen, die der Richtlinienzuordnung zugeordnet ist.

```
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
```

Sie können die QoS-Statistiken auch mit dem hier gezeigten Befehl löschen.

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

Überprüfen der in der Software programmierten ACL

```
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]
```

Überprüfen der in der Hardware programmierten ACL

```
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]
```

Mit dem hier gezeigten Befehl können Sie die Ports überprüfen, die das VLAN verwenden. In diesem Beispiel wäre dies die VLAN-ID 9, und Sie können sich auch die verwendete QoS-Richtlinie notieren.

```
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#
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.