

Configurazione e risoluzione dei problemi di Q-in-Q selettivo su Nexus 9000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Risoluzione dei problemi](#)

[Verifica coerenza](#)

[Comandi utili per raccogliere e controllare eventuali problemi Q-in-Q](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare e risolvere i problemi relativi a Selective Q-in-Q nel modello Nexus 9300 (EX-FX-GX).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Incapsulamento Q-in-Q
- Switching dot1q
- Nexus 9000

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Hardware: N9K-C9336C-FX2
- Versione: 10.2(3)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Un tunnel VLAN Q-in-Q consente a un provider di servizi di segregare il traffico di diversi utenti nella propria infrastruttura, fornendo al tempo stesso una gamma completa di VLAN per l'uso interno, aggiungendo un secondo tag 802.1Q a un frame già contrassegnato.

Q-in-Q selettivo con VLAN di più provider è una funzione di tunneling che consente di associare un intervallo di VLAN specifico dell'utente su una porta a una VLAN di provider specifica.

Q-in-Q consente di avere più mapping di VLAN utente-provider su una porta.

I pacchetti forniti con un tag VLAN che corrisponde a una delle VLAN utente configurate sulla porta vengono tunneling nell'infrastruttura usando le proprietà della VLAN del provider di servizi. Il pacchetto incapsulato conserva il tag VLAN dell'utente come parte dell'intestazione di layer 2 del pacchetto interno.

Esempio di rete



Configurazione

L'obiettivo della configurazione di Selective Q-in-Q è mappare le VLAN sul traffico ricevuto in N9KFX2 e N9KFX2-1 sulle interfacce eth1/1.

Il Nexus incapsula il traffico e lo invia con l'intestazione DOT1Q VLAN 20 al provider, simulata da Nexus 93180FX.

Host-A

```
interface Ethernet1/1
  switchport
  switchport mode trunk
  no shutdown

interface Vlan10
  no shutdown
  ip address 192.168.1.1/24
```

Host-B

```
interface Ethernet1/1
  switchport
  switchport mode trunk
  no shutdown

interface Vlan10
  no shutdown
  ip address 192.168.1.2/24
```

N9KFX2

```
interface Ethernet1/1
  switchport
  switchport mode trunk
  switchport vlan mapping all dot1q-tunnel 20
  switchport trunk allowed vlan 20
  spanning-tree port type edge trunk
  spanning-tree bpdupfilter enable
  no shutdown

interface Ethernet1/35
  switchport
  switchport mode trunk
  no shutdown
```

N93180FX

```
system dot1q-tunnel transit

interface Ethernet1/17
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet1/18
  switchport
```

```
switchport mode trunk
no shutdown
```

N9KFX2-1

```
interface Ethernet1/1
switchport
switchport mode trunk
switchport vlan mapping all dot1q-tunnel 20
switchport trunk allowed vlan 20
spanning-tree port type edge trunk
spanning-tree bpdupfilter enable
no shutdown
```

```
interface Ethernet1/35
switchport
switchport mode trunk
no shutdown
```

Risoluzione dei problemi

La programmazione Q-in-Q si sposta dal piano di controllo all'hardware attraverso i seguenti componenti:

:



Verifica coerenza

Nelle versioni più recenti dello switch Nexus è disponibile la verifica di coerenza da utilizzare in caso di programmazione errata.

```
N9KFX2# show consistency-checker selective-qinq
```

```
Box level hardware programming checks      : PASS
Fetching ingressVlanXlate entries from slice: 0 HW
Fetching ingressVlanXlate entries from slice: 1 HW
Fetching ingressVlanXlate TCAM entries
Performing port specific checks for intf Eth1/1
Port specific selective QinQ checks for interface Eth1/1 : PASS
Selective QinQ Overall status              : PASS
```

Piano di controllo

Verificare che la VLAN sia attiva sulle porte.

```
N9KFX2#sh vlan
```

VLAN Name	Status	Ports
1 default	active	Eth1/1
20 VLAN0020	active	Eth1/1, Eth1/35

Confermare che il mapping della VLAN sia chiaramente visibile.

```
N9KFX2# sh vlan internal info mapping
```

Per Port Vlan Translation Details

```
=====
Entry No          : 0
-----
ifindex Eth1/1(0x1a000000)
vlan mapping enabled: TRUE
vlan translation mapping information (count=1):
  Original Vlan      Translated Vlan
  -----
  all                20

Entry No          : 1
-----
ifindex Eth1/35(0x1a004400)
vlan mapping enabled: FALSE
vlan translation mapping information (count=0):
  Original Vlan      Translated Vlan
  -----
```

ELTM

Verificare se sono presenti errori che aumentano o che non siano uguali a zero.

```
N9KFX2# show system internal eltm error count
interface config error: 0
dce error: 0
port struct error: 0
port channel error: 0
tunnel error: 0
tlv count error: 0
vpn count error: 0
SI add to DB error: 0
```

Eseguire il comando attach module X. La X è il modulo in cui è allocata l'interfaccia fisica.

```
N9KFX2# attach module 1
module-1# show system internal eltm info vlan 20
IFTMC Detailed info for VLAN = 20
cr_flags = VLAN , bd = 21(0x15) stg-id = 0 type = 1 stp:0
shut_state = 2 , oper_state = 1
vni = 0, ipmc_idx = 0x0 ipmc_remap_idx = 0x0 ipmc_remap_idx2 = 0x0 dvif: 0
ipmc_mrouter_idx = 0x0 ipmc_mrouter_remap_idx = 0x0 ipmc_mrouter_remap_idx2 = 0x0
pbp_idx=0
eid[0] = 0, alt_eid[0] = 0eid[1] = 0, alt_eid[1] = 0eid[2] = 0, alt_eid[2] = 0eid[3] = 0, alt_eid[3] = 0
```

```
Active ports: <<<<< Confirm Active ports are listed for the
Ethernet1/1(0x1a000000) Ethernet1/35(0x1a004400)
```

```
Active Local ports:
Ethernet1/1(0x1a000000) Ethernet1/35(0x1a004400)
```

```
Ports using this VLAN as Provider: <<<<< Displays the interface that is doing
Ethernet1/1(0x1a000000)
```

```
SDB Active ports:
Ethernet1/1
```

```
pbp_idx:0
```

```
VLAN Features:
prim_vlan : 0, prim_intf_vlan : 0, vlan mode : 0(CE)
pt_cam_en : 1, ipv4_igmp_snoop : 1, ipv4_pim_snoop : 0
ipv6_mld_snoop : 0, ipv6_pim_snoop : 0, l2l3_lkup_cfg : 1
v4_table_id : 1 (0x00000001), v4_vpn_id : 1 (0x1)
v6_table_id : 2147483649 (0x80000001), v6_vpn_id : 1 (0x1)
age_tmr_sel : 1, sm_en : 0 fcf : 0 omf : 1, dhcp_snoop_en : 0
proxy_learn : 0, iic_en : 0, use_oxid : 0, age_grp_sel : 0
disable_learn : 0, otv_en : 0, global : FALSE
bc_uc_ftag : 4095 , mcast_ftag_num : 1, arp_sup: 0x0 , icmpv6 nd local proxy: 0x0
isdot1qvlan : 0 , num_dot1q_ports: 0 num_sel_dot1q_qinvni_ports: 0
num_multi_tag_ports: 0, eid: 0, xconnect: 0, mcast_ftag[1] : {4095}
is_transit : 0 mdns_en: 0,
```

```
TAH:VLAN_CONTROL:
```

```
-----
vrf: 0 forwarding_vlan: 0 forwarding mode: 0
Flags: 0x0
up: 0 vni: 0 is_sr_evpn: 0
```

È possibile controllare la programmazione dell'interfaccia. L'output visualizza informazioni sulla programmazione delle porte.

```
N9KFX2# attach module 1
module-1# show system internal eltm info interface e1/1
IFTMC Detailed info for Interface Ethernet1/1(0x1a000000)
CR_flags = INTF LIF (0x3), LTL = 6144 (0x1800), (S 0x0, P 0x0)
IF_INDEX = Ethernet1/1(0x1a000000), LIF = 4100 (0x1004), SDB LIF = 4100 (0x1004)
```


TAH:L2 INFO: 4100

Flags : 0x41

NIV Index: 1 Source Chip: 1 Source Port: 72

slice: 1 slice_port: 0

is_monitor: 0 lif: 4100 phy_intf_id: 1 vnic_if: 0 learn_en: 1 native_vlan 1

trunk_port: 1 src_if_check: 1

FC info: intf_type = 0x0 port_mode = 0x0 port_vsan = 0 port_speed = 0 fcf_mac = 0:0:0:0:0:0

IFTMC

Per l'IFTMC è possibile eseguire i due comandi. Eseguire il comando attach module 1 prima di eseguire i comandi successivi.

```
N9KFX2# attach module 1
```

```
module-1# show system internal iftmc info interface e1/1
```

```
module-1# show system internal iftmc info vlan 20
```

Entrambi i comandi

- show system internal iftmc info interface ethernet1/1
- show system internal iftmc info vlan 20

Visualizza informazioni simili a quelle degli output ELTM, accertatevi di avere gli stessi valori tra i moduli ELTM e IFTMC.

Hardware

Per verificare che le uscite siano programmate correttamente sull'hardware, è possibile eseguire il comando show hardware internal tah interface ethernet 1/1. Nell'output del comando è possibile passare alla parte BdStateTable.

```
N9KFX2-1(config-if)# show hardware internal tah interface ethernet 1/1
```

```
BdStateTable:
```

```
ENTRY: 1
```

```
    info_leaf_flood_dst_ptr : 1                <<<Displays native vlan
    info_leaf_igmp_mld_dst_ptr : 4098
    info_leaf_fid : 1                          <<<Displays native vlan
    info_leaf_vrf : 1
    info_leaf_igmp_snp_en : 1
    info_leaf_l3_bind_check_en : 1
    info_leaf_v4_omf : 1
    info_leaf_unknown_uc_flood : 1
    info_leaf_unknown_mc_flood : 1
    info_leaf_ecn_mark_en : 1
    info_leaf_l2_bind_check_en : 1
    info_leaf_bd_profile_idx : 1
    info_leaf_analytics_en : 1
    info_leaf_flow_collect_en : 1
    info_spine_info0_gipo_idx : 1              <<<Displays native vlan
```



```
info_spine_info0_scope : 64
info_spine_info0_spare : 0x00000000:0x00100044
info_spine_info1_spare : 0x00001000:0x00000000
info_spine_info2_gipo_idx : 512
info_spine_info2_scope : 12416
info_spine_info2_spare : 0x00005000:0x10000000
info_spine_info3_gipo_idx : 384
info_spine_info3_spare : 0x00000000:0x00000000
=====
```

Comandi utili per raccogliere e controllare eventuali problemi Q-in-Q

- show vlan internal info mapping
- show consistency-checker selective-qinq
- show consistency-checker selective-qinq interface <ethX/Y, port-channel X>
- show hardware internal tah interface ethernet x/y
- show hardware internal tah interface all
- mostra errore hardware interno tah sdk event-history
- show system internal iftmc info interface<>

Sulla piattaforma Nexus è possibile raccogliere show tech-support più specifico del generale, che fornisce una serie di comandi:

- mostra dettagli tecnici
- show tech vlan
- show tech usd-all
- show tech eltm
- allegare il modulo 1 ; show tech iftmc



Nota: per verificare che la configurazione non superi le limitazioni hardware o software, consultare le sezioni delle linee guida e delle limitazioni nella guida alla configurazione riportata in Informazioni correlate per la versione in esecuzione nel sistema Nexus.

Informazioni correlate

- [Release 9.3.X](#)
- [Release 10.1.X](#)
- [Release 10.2.X](#)
- [Release 10.3.X](#)
- [Release 10.4.X](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).