

Risoluzione dei problemi di perdita di pacchetti DHCP in VPN sugli switch Catalyst serie 9500X/9600X

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

[Opzione 1: Applicare una soluzione](#)

[Opzione 2: Aggiornare il software](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle perdite di pacchetti DHCP in VPN sugli switch Cisco Catalyst serie 9500X/9600X.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di DHCP e del relativo funzionamento in una rete.
- Conoscenza dei comandi e delle tecniche di risoluzione dei problemi di Cisco IOS.
- Conoscenza dei protocolli di switching e routing LAN.
- Conoscenza degli scenari di configurazione comuni di EVPN.

Componenti usati

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

- Hardware: Cisco Catalyst 9500X-28C8D, 9500X-60L4D o 9600X-SUP-2
- Versione del software: 17.12.x

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.

Problema

Il problema osservato è che i pacchetti DHCP che ritornano dal server DHCP (DHCP offer) vengono scartati dallo switch che agisce come agente di inoltro, quando il client e il server DHCP sono connessi allo stesso VTEP/nodo foglia, ma si trovano in due VRF diverse.

Nell'esempio, il client si trova nella VLAN 10 in VERDE VRF e il server nella VLAN 20 in ROSSO VRF.

- Il problema può essere identificato dai seguenti output del comando:

```
<#root>
```

```
device#
```

```
show run interface vlan 10
```

```
interface Vlan10
  description CLIENT
  mac-address cafe.cafe.cafe
```

```
vrf forwarding GREEN
```

```
ip dhcp relay source-interface Loopback10
ip address 172.30.208.1 255.255.255.128
```

```
ip helper-address vrf RED 192.168.1.10 <-- Leaking from GREEN to RED
```

```
device#
```

```
show run interface vlan 20
```

```
interface Vlan20
  description SERVER
  mac-address abcd.abcd.abcd
```

```
vrf forwarding RED <--- Server is in VRF RED (Same VTEP)
```

```
ip address 192.168.1.1 255.255.255.0
```

```
device#
```

```
show plat soft fed switch active punt asic-cause br
```

```
ASIC Cause Statistics Brief
```

```
+-----+
| Source | Cause | Rx |
+-----+
Drop
| | | cur | delta | cur | delta |
+-----+
```

```

+-----+
LPTS
DHCPv4 S to S
          577087870          9219
30905

7 <-- Drops in this counter
LPTS  DHCPv4 C to S          56467          0          56467          0

```

Soluzione

La soluzione prevede l'aggiornamento della versione del software per risolvere il problema. Le fasi descritte di seguito descrivono il processo:

Opzione 1: Applicare una soluzione

- Spostare il server DHCP su un VTEP diverso senza client DHCP che si basano su tale server
- Distribuire più server DHCP
- Spostare il server all'esterno dell'infrastruttura.

Opzione 2: Aggiornare il software

Aggiornare lo switch a una versione di codice contenente la correzione per l'ID bug Cisco [CSCwm4805](#)

- Versione 17.15.1 e successive.

Il processo di aggiornamento non rientra nell'ambito di questo documento. Per ulteriori informazioni su come aggiornare lo switch, consultare:

- [Guide all'installazione e all'aggiornamento di 9500](#)
- [Guide all'installazione e all'aggiornamento di 9600](#)
- [Guida all'aggiornamento per i dispositivi Catalyst 9000 Switch](#)
- [Versioni consigliate per le piattaforme Catalyst 9200/9300/9400/9500/9600](#)



Nota: Non è prevista alcuna correzione di questo problema nei treni di rilascio precedenti alla 17.15.1

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- ID bug Cisco [CSCwm44805](#)

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).