Risoluzione dei problemi relativi a DHCP lenti o intermittenti sugli agenti di inoltro DHCP Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di allocazione degli indirizzi DHCP (Dynamic Host Configuration Protocol) lenti o di allocazione degli indirizzi DHCP intermittente sugli switch Catalyst serie 9000 come agenti di inoltro DHCP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Agenti di inoltro DHCP e DHCP
- Protocollo ICMP (Internet Control Message Protocol)
- Control Plane Policing (CoPP)

Componenti usati

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

- Switch Catalyst serie 9000
- Cisco IOS XE® versioni 16.x e 17.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.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Switch Catalyst serie 3650/3850 con Cisco IOS XE® 16.x

Premesse

La funzione CoPP (Control Plane Policing) migliora la sicurezza del dispositivo grazie alla protezione della CPU da traffico non necessario e attacchi DoS (Denial of Service). Può inoltre proteggere il traffico di controllo e di gestione da cadute causate da elevati volumi di traffico di altro tipo con priorità inferiore.

Il dispositivo è in genere segmentato in tre piani operativi, ciascuno con il proprio obiettivo:

- Il piano dati, per inoltrare i pacchetti di dati.
- Il piano di controllo, per instradare correttamente i dati.
- Il piano di gestione, per gestire gli elementi di rete.

Èpossibile utilizzare il protocollo CoPP per proteggere la maggior parte del traffico basato sulla CPU e garantire la stabilità del routing, la raggiungibilità e la consegna dei pacchetti. È inoltre possibile utilizzare il protocollo CoPP per proteggere la CPU da attacchi DoS.

Per raggiungere questi obiettivi, CoPP utilizza l'interfaccia della riga di comando (MQC) QoS modulare e le code della CPU. I diversi tipi di traffico del control plane vengono raggruppati in base a determinati criteri e assegnati a una coda della CPU. È possibile gestire queste code della CPU configurando i criteri dedicati nell'hardware. Ad esempio, è possibile modificare la frequenza del policer per determinate code della CPU (tipo di traffico) oppure disabilitarlo per un determinato tipo di traffico.

Sebbene i policer siano configurati nell'hardware, CoPP non influisce sulle prestazioni della CPU o del piano dati. Tuttavia, poiché limita il numero di pacchetti indirizzati alla CPU, il carico della CPU viene controllato. Ciò significa che i servizi che attendono i pacchetti dall'hardware possono vedere una velocità di ingresso dei pacchetti più controllata (la velocità è configurabile dall'utente).

Problema

Quando il comando **ip helper-address** è configurato su un'interfaccia di routing o SVI, gli switch Catalyst 9000 sono configurati come agenti di inoltro DHCP. L'interfaccia in cui è configurato l'indirizzo dell'helper è in genere il gateway predefinito per i client downstream. Affinché lo switch fornisca correttamente i servizi di inoltro DHCP ai propri client, deve essere in grado di elaborare i messaggi di individuazione DHCP in ingresso. A tal fine, è necessario che lo switch riceva il pacchetto DHCP Discover e che lo indirizzi fino alla CPU da elaborare. Dopo aver ricevuto ed elaborato il comando DHCP Discover, l'agente di inoltro crea un nuovo pacchetto unicast inviato dall'interfaccia su cui è stato ricevuto il comando DHCP Discover e destinato all'indirizzo IP definito nella configurazione dell'**indirizzo dell'helper IP**. Una volta creato il pacchetto, il relativo

hardware viene inoltrato e inviato al server DHCP, dove può essere elaborato e infine inviato all'agente di inoltro, in modo che il processo DHCP possa continuare per il client.

Un problema comune che si verifica quando i pacchetti di transazione DHCP nell'agente di inoltro vengono involontariamente influenzati dal traffico inviato alla CPU perché è soggetto a uno scenario ICMP specifico, ad esempio un reindirizzamento ICMP o un messaggio ICMP "destinazione irraggiungibile". Questo comportamento può manifestarsi come i client non sono in grado di ottenere un indirizzo IP da DHCP in tempo utile o addirittura come totale errore di assegnazione DHCP. In alcuni scenari, il comportamento può essere osservato solo in determinati orari del giorno, ad esempio nelle ore di punta quando il carico sulla rete è completamente massimizzato.

Come accennato nella sezione Background, gli switch Catalyst serie 9000 sono forniti con una policy CoPP predefinita configurata e abilitata sul dispositivo. Questo criterio CoPP funziona come criterio QoS (Quality of Service), posizionato nel percorso del traffico ricevuto sulle porte del pannello anteriore e destinato alla CPU del dispositivo. Limita il traffico in base al tipo di traffico e alle soglie predefinite configurate nel criterio. Alcuni esempi di traffico classificato e con velocità limitata per impostazione predefinita sono i pacchetti di controllo di routing (in genere contrassegnati con DSCP CS6), i pacchetti di controllo della topologia (BPDU STP) e i pacchetti a bassa latenza (BFD). È necessario assegnare la priorità a questi pacchetti perché la capacità di elaborarli in modo affidabile determina un ambiente di rete stabile.

Visualizzare le statistiche del policer CoPP con il comando **show platform hardware fed switch active qos queue stats internal cpu policer**.

La coda di reindirizzamento ICMP (coda 6) e la coda BROADCAST (coda 12) condividono entrambe lo stesso PlcIdx di 0 (indice Policer). Ciò significa che tutto il traffico di broadcast che deve essere elaborato dalla CPU del dispositivo, ad esempio un rilevamento DHCP, viene condiviso con il traffico destinato anche alla CPU del dispositivo nella coda di reindirizzamento ICMP. Ciò può causare il problema menzionato in precedenza, ovvero il mancato completamento delle transazioni DHCP perché il traffico della coda di reindirizzamento ICMP diminuisce il traffico che deve essere gestito dalla coda BROADCAST, con conseguente eliminazione dei pacchetti di broadcast legittimi.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      0            0  <-- Policer
Index 0
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12   0      BROADCAST                   Yes     600       600      0            0  <-- Policer
Index 0
```

```
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>
```

Il traffico che supera la frequenza predefinita di 600 pacchetti al secondo nei criteri CoPP viene scartato prima di raggiungere la CPU.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
------------------------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      3063106173577 3925209161
<-- Dropped packets in queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
9 19 EWLC Control Yes 13000 13000 0 0
10 16 EWLC Data Yes 2000 2000 0 0
11 13 L2 LVX Data Pack Yes 1000 1000 0 0
12   0      BROADCAST                   Yes     600       600      1082560387 3133323
<-- Dropped packets in queue
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
15 8 Topology Control Yes 13000 16000 0 0
16 12 Proto Snooping Yes 2000 2000 0 0
17 6 DHCP Snooping Yes 500 500 0 0
18 13 Transit Traffic Yes 1000 1000 0 0
19 10 RPF Failed Yes 250 250 0 0
20 15 MCAST END STATION Yes 2000 2000 0 0
<snip>
```

Scenario 1: Reindirizzamenti ICMP

Per il primo scenario, prendere in considerazione la topologia seguente:

La sequenza degli eventi è la seguente:

1. Un utente che accede alla porta 10.10.10.100 avvia una connessione telnet con il dispositivo

10.100.100.100, una rete remota.

2. L'IP di destinazione si trova in una subnet diversa, quindi il pacchetto viene inviato al gateway predefinito dell'utente, 10.10.15.

3. Quando il Catalyst 9300 riceve il pacchetto da indirizzare, lo reindirizza alla CPU per generare un reindirizzamento ICMP.

Il reindirizzamento ICMP è stato generato perché, dal punto di vista dello switch 9300, sarebbe più efficiente per il laptop inviare semplicemente il pacchetto al router alla velocità 10.10.10.1 direttamente, poiché questo è comunque l'hop successivo del Catalyst 9300 e si trova nella stessa VLAN in cui si trova l'utente.

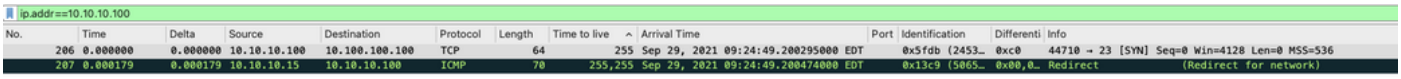
Il problema è che l'intero flusso viene elaborato sulla CPU in quanto soddisfa i criteri di reindirizzamento ICMP. Se altri dispositivi inviano traffico che soddisfa lo scenario di reindirizzamento ICMP, un volume ancora maggiore di traffico inizierà a raggiungere la CPU in questa coda, il che potrebbe influire sulla coda BROADCAST, in quanto condividono lo stesso policer CoPP.

Eseguire il debug di ICMP per visualizzare il syslog di reindirizzamento ICMP.

```
9300-Switch#debug ip icmp       <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | inc ICMP
*Sep 29 12:41:33.217: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.218: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:41:33.219: ICMP: echo reply sent, src 10.10.10.15, dst 10.10.10.100, topology BASE,
dscp 0 topoid 0
*Sep 29 12:43:08.127: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:09.517: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:10.017: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1     <-- ICMP Redirect to use 10.10.10.1 as Gateway
*Sep 29 12:50:14.293: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:19.053: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:23.797: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:28.537: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
*Sep 29 12:50:33.284: ICMP: redirect sent to 10.10.10.100 for dest 10.100.100.100, use gw
10.10.10.1
```

> Attenzione: a causa del livello di dettaglio delle informazioni, si consiglia di disabilitare la registrazione sulla console e il monitoraggio dei terminali prima di abilitare i debug ICMP.

Un'acquisizione pacchetto incorporata sulla CPU Catalyst 9300 mostra la SYN TCP iniziale per la connessione Telnet sulla CPU e il reindirizzamento ICMP generato.



Il pacchetto di reindirizzamento ICMP proviene dall'interfaccia Catalyst 9300 VLAN 10 destinata al client e contiene le intestazioni originali del pacchetto per cui viene inviato il pacchetto di reindirizzamento ICMP.

```
▼ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x13c9 (5065)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x7f75 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.15
    Destination: 10.10.10.100
▼ Internet Control Message Protocol
    Type: 5 (Redirect)
    Code: 0 (Redirect for network)
    Checksum: 0x2bec [correct]
    [Checksum Status: Good]
    Gateway address: 10.10.10.1
  ▼ Internet Protocol Version 4, Src: 10.10.10.100, Dst: 10.100.100.100
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      Total Length: 44
      Identification: 0x5fdb (24539)
    ▶ Flags: 0x0000
      Time to live: 255
      Protocol: TCP (6)
      Header checksum: 0xd7fa [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.10.10.100
      Destination: 10.100.100.100
  ▶ Transmission Control Protocol, Src Port: 44710, Dst Port: 23
```

Soluzione

In questo scenario, è possibile impedire che i pacchetti vengano reindirizzati alla CPU, interrompendo così la generazione del pacchetto di reindirizzamento ICMP.

I moderni sistemi operativi non utilizzano i messaggi di reindirizzamento ICMP, quindi le risorse necessarie per generare, inviare ed elaborare questi pacchetti non rappresentano un uso efficiente delle risorse della CPU sui dispositivi di rete.

In alternativa, selezionare l'utente per utilizzare il gateway predefinito 10.10.10.1, ma questa configurazione può essere implementata per un motivo e non è inclusa nell'ambito del presente documento.

Èsufficiente disabilitare i reindirizzamenti ICMP con la CLI **senza reindirizzamenti ip**.

```
9300-Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip redirects       <-- disable IP redirects
9300-Switch(config-if)#end
```

Verificare che i reindirizzamenti ICMP siano disabilitati su un'interfaccia.

```
9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent       <-- redirects disabled
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>
```

Per ulteriori informazioni sui reindirizzamenti ICMP e sulla data e l'ora di invio, visitare questo sito Web: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

Scenario 2: ICMP non raggiungibili

Si consideri la stessa topologia in cui l'utente alla posizione 10.10.10.100 avvia una connessione Telnet alla posizione 10.100.100.100. Questa volta è stato configurato un elenco degli accessi in entrata sulla VLAN 10 SVI che blocca le connessioni telnet.


```
9300-Switch#show running-config interface vlan 10
Building Configuration..
```

```
Current Configuration : 491 bytes
!
interface Vlan10
ip address 10.10.10.15 255.255.255.0
no ip proxy-arp
ip access-group BLOCK-TELNET in              <-- inbound ACL
end
9300-Switch#
9300-Switch#show ip access-list BLOCK-TELNET
Extended IP access list BLOCK-TELNET
10 deny tcp any any eq telnet            <-- block telnet
20 permit ip any any
9300-Switch#
```

La sequenza degli eventi è la seguente:

1. L'utente alla posizione 10.10.10.100 avvia una connessione telnet con il dispositivo 10.100.100.100.

2. L'IP di destinazione si trova in una subnet diversa, quindi il pacchetto viene inviato al gateway predefinito dell'utente.

3. Quando Catalyst 9300 riceve questo pacchetto, il pacchetto viene valutato rispetto all'ACL in entrata e viene bloccato.

4. Poiché il pacchetto è bloccato e i pacchetti IP non raggiungibili sono abilitati sull'interfaccia, il pacchetto viene indirizzato alla CPU in modo che il dispositivo possa generare un pacchetto ICMP destinazione non raggiungibile.

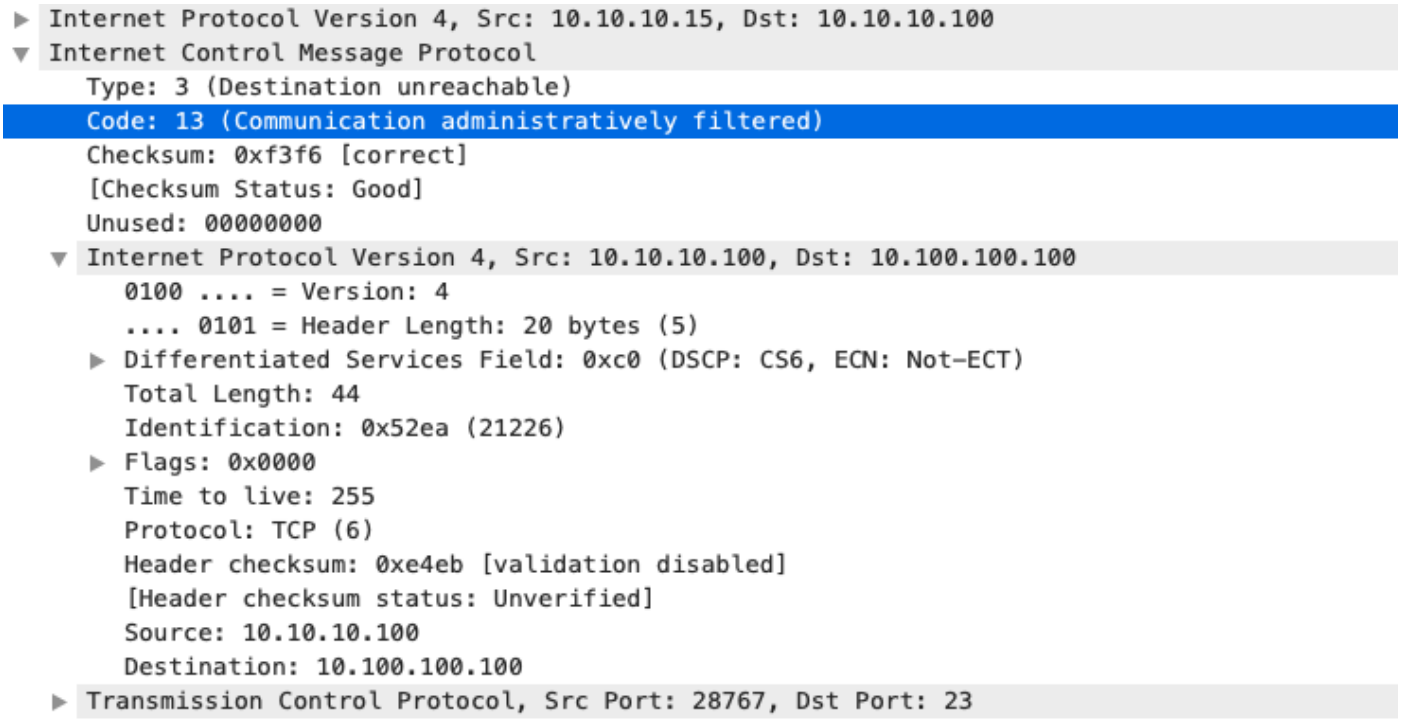
Eseguire il debug di ICMP per visualizzare il syslog di destinazione ICMP non raggiungibile.

```
9300-Switch#debug ip icmp              <-- enables ICMP debugs
ICMP packet debugging is on
9300-Switch#show logging | include ICMP
<snip>
*Sep 29 14:01:29.041: ICMP: dst (10.100.100.100) administratively prohibited unreachable sent to
10.10.10.100    <-- packet blocked and ICMP message sent to client
```

> **Attenzione**: a causa del livello di dettaglio delle informazioni, si consiglia di disabilitare la registrazione sulla console e il monitoraggio dei terminali prima di abilitare i debug ICMP.

Un'operazione Embedded Packet Capture sulla CPU Catalyst 9300 mostra la SYN TCP iniziale per la connessione Telnet sulla CPU e la destinazione ICMP "destinazione irraggiungibile" inviata.

Il pacchetto ICMP "Destination Unreachable" (Destinazione non raggiungibile) proviene dall'interfaccia Catalyst 9300 VLAN 10 destinata al client e contiene le intestazioni dei pacchetti originali per cui il pacchetto ICMP viene inviato.



Soluzione

In questo scenario, disattivare il comportamento in cui i pacchetti con puntamento bloccati da un ACL generano il messaggio ICMP "Destination Unreachable" (Destinazione irraggiungibile).

La funzionalità IP Unreachable è abilitata per impostazione predefinita sulle interfacce di routing sugli switch Catalyst serie 9000.

```
9300-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip unreachables      <-- disable IP unreachables
```

Verificare che siano disabilitati per l'interfaccia.

```
9300-Switch#show ip interface vlan 10
Vlan10 is up, line protocol is up
Internet address is 10.10.10.15/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.102
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is BLOCK-TELNET
Proxy ARP is disabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachables are never sent     <-- IP unreachables disabled
ICMP mask replies are never sent
```

```
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
<snip>
```

Scenario 3: valore TTL ICMP superato

Si consideri la topologia utilizzata in precedenza per i due scenari precedenti. Questa volta l'utente alla 10.10.10.100 cerca di raggiungere una risorsa in una rete che da allora è stata smantellata. Per questo motivo, la SVI e la VLAN che erano usate per ospitare questa rete non esistono più sul Catalyst 9300. Tuttavia, il router ha ancora un percorso statico che punta all'interfaccia Catalyst 9300 VLAN 10 come hop successivo per questa rete.

Poiché Catalyst 9300 non dispone più di questa rete configurata, non viene visualizzata come connessa direttamente e lo switch 9300 instrada tutti i pacchetti per i quali non dispone di un percorso specifico verso il proprio percorso statico predefinito che punta al router in modalità 10.10.10.1.

Questo comportamento introduce un loop di routing nella rete quando l'utente tenta di connettersi a una risorsa nello spazio di indirizzi 192.168.10.0/24. Il pacchetto viene inoltrato tra il router 9300 e il router fino alla scadenza del valore TTL.

1. L'utente tenta di connettersi a una risorsa nella rete 192.168.10/24

2. Il pacchetto viene ricevuto da Catalyst 9300 e inviato al percorso predefinito con l'hop successivo 10.10.10.1. Il valore TTL viene diminuito di 1.

3. Il router riceve questo pacchetto e controlla la tabella di routing per trovare un percorso per questa rete con l'hop successivo 10.10.10.15. Diminuisce il valore TTL di 1 e indirizza il pacchetto indietro al 9300.

4. Catalyst 9300 riceve il pacchetto e, ancora una volta, lo instrada indietro fino a 10.10.10.1 e diminuisce il valore TTL di 1.

Questo processo si ripete finché il valore TTL IP non raggiunge zero.

Quando il Catalyst riceve il pacchetto con IP TTL = 1, reindirizza il pacchetto alla CPU e genera un messaggio ICMP TTL-Exceeded.

Il tipo di pacchetto ICMP è 11 con codice 0 (TTL scaduto durante la trasmissione). Impossibile disabilitare questo tipo di pacchetto tramite i comandi CLI

In questo scenario viene attivato il problema del traffico DHCP perché i pacchetti con loop sono soggetti al reindirizzamento ICMP perché non includono la stessa interfaccia su cui sono stati ricevuti.

Anche i pacchetti inviati dall'utente sono soggetti al reindirizzamento ICMP. In questo scenario, il traffico DHCP può facilmente essere ridotto alla fame dalla coda BROADCAST. Su scala ridotta, questo scenario sarebbe ancora peggiore a causa del numero di pacchetti puntati nella coda di reindirizzamento.

Le cadute del CoPP vengono mostrate sulla rete 192.168.10.0/24 tramite 1000 ping, con un timeout di 0 secondi tra ciascun ping. Le statistiche CoPP sullo switch 9300 vengono cancellate e il valore è zero byte scartati prima dell'invio dei ping.

```
9300-Switch#clear platform hardware fed switch active qos statistics internal cpu policer
<-- clear CoPP stats

9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer | i
Redirect|Drop   <-- verify 0 drops
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
6 0 ICMP Redirect Yes 600 600 0               0                       <-- bytes dropped 0
<snip>
```

L'utente invia il traffico alla rete remota.

```
User#ping 192.168.10.10 timeout 0 rep 1000   <-- User sends 1000 pings
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.10, timeout is 0 seconds:
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
...................
Success rate is 0 percent (0/1000)
```

I debug ICMP mostrano i syslog di reindirizzamento e TTL-superato causati dal loop di routing.

```
9300-Switch#debug ip icmp
ICMP packet deubgging is on
*Sep 29 16:33:22.676: ICMP: redirect sent to 10.10.10.100 for dest 192.168.10.10, use gw
10.10.10.1    <-- redirect sent
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0    <-- TTL exceeded observed
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
*Sep 29 16:33:22.678: ICMP: time exceeded (time to live) sent to 10.10.10.100 (dest was
192.168.10.10), topology BASE, dscp 0 topoid 0
<snip>
```

> **Attenzione**: a causa del livello di dettaglio delle informazioni, si consiglia di disabilitare la registrazione sulla console e il monitoraggio dei terminali prima di abilitare i debug ICMP.

Le cadute CoPP sono dovute alla quantità di traffico puntato alla CPU per il reindirizzamento. Si

noti che questa operazione è valida solo per un singolo client.

```
9300-Switch#show platform hardware fed switch active qos queue stats internal cpu policer

CPU Queue Statistics
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
0 11 DOT1X Auth Yes 1000 1000 0 0
1 1 L2 Control Yes 2000 2000 0 0
2 14 Forus traffic Yes 4000 4000 0 0
3 0 ICMP GEN Yes 600 600 0 0
4 2 Routing Control Yes 5400 5400 0 0
5 14 Forus Address resolution Yes 4000 4000 0 0
6    0      ICMP Redirect               Yes     600       600      15407990     126295    <--
drops in redirect queue
7 16 Inter FED Traffic Yes 2000 2000 0 0
8 4 L2 LVX Cont Pack Yes 1000 1000 0 0
<snip>
```

Soluzione

La soluzione di questo scenario è disabilitare i reindirizzamenti ICMP, come nello scenario 1. Anche il ciclo di routing è un problema, ma l'intensità viene incrementata in quanto i pacchetti vengono anche reindirizzati.

Anche i pacchetti ICMP TTL-Exceeded vengono reindirizzati quando TTL è 1, ma questi pacchetti usano un indice del Policer CoPP diverso e non condividono una coda con BROADCAST, quindi il traffico DHCP non viene influenzato.

Èsufficiente disabilitare i reindirizzamenti ICMP con la CLI senza reindirizzamenti IP.

```
9300-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
9300-Switch(config)#interface vlan 10
9300-Switch(config-if)#no ip redirects        <-- disable IP redirects
9300-Switch(config-if)#end
```

Informazioni correlate

- Configurazione di Embedded Packet Capture
- Informazioni sui reindirizzamenti ICMP
- Documentazione e supporto tecnico – Cisco Systems

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).