Resolución de problemas de DHCP lento o intermitente en los agentes de retransmisión DHCP de Catalyst 9000

Contenido

Introducción

Este documento describe cómo resolver problemas de asignación de direcciones de protocolo de configuración dinámica de host (DHCP) lento o fallas intermitentes de asignación de direcciones DHCP en switches Catalyst de la serie 9000 como agentes de retransmisión DHCP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Agentes de retransmisión DHCP y DHCP
- Internet Control Message Protocol (ICMP)
- Control Plane Policing (CoPP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9000 Series Switches
- Cisco IOS XE® versiones 16.x y 17.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Catalyst 3650/3850 Series Switches con Cisco IOS XE® 16.x

Antecedentes

La función Control Plane Policing (CoPP) mejora la seguridad del dispositivo mediante la protección de la CPU frente a tráfico innecesario y ataques de denegación de servicio (DoS). También puede proteger el tráfico de control y el tráfico de gestión de caídas de tráfico causadas por grandes volúmenes de otro tráfico de menor prioridad.

El dispositivo suele estar segmentado en tres planos de funcionamiento, cada uno con su propio objetivo:

- El plano de datos, para reenviar paquetes de datos.
- El plano de control, para enrutar los datos correctamente.
- El plano de gestión, para gestionar elementos de red.

Puede utilizar CoPP para proteger la mayor parte del tráfico destinado a la CPU y garantizar la estabilidad de routing, la disponibilidad y la entrega de paquetes. Lo más importante es que puede utilizar CoPP para proteger la CPU de un ataque DoS.

CoPP utiliza la interfaz de línea de comandos (MQC) de QoS modular y las colas de CPU para lograr estos objetivos. Los diferentes tipos de tráfico del plano de control se agrupan en función de determinados criterios y se asignan a una cola de CPU. Puede administrar estas colas de CPU mediante la configuración de controladores de políticas dedicados en el hardware. Por ejemplo, puede modificar la velocidad del regulador para ciertas colas de CPU (tipo de tráfico) o puede inhabilitar el regulador para un tipo de tráfico determinado.

Aunque los reguladores de tráfico están configurados en hardware, la CoPP no afecta el rendimiento de la CPU ni el rendimiento del plano de datos. Sin embargo, dado que limita el número de paquetes dirigidos a la CPU, la carga de la CPU está controlada. Esto significa que los servicios que esperan paquetes del hardware pueden ver una velocidad de ingreso de paquetes más controlada (la velocidad es configurable por el usuario).

Problema

Un switch Catalyst 9000 se configura como un agente relay DHCP cuando el comando **ip helper-address** se configura en una interfaz ruteada o SVI. La interfaz en la que se configura la dirección del ayudante suele ser el gateway predeterminado para los clientes de flujo descendente. Para que el switch proporcione servicios de retransmisión DHCP exitosos a sus clientes, debe ser capaz de procesar los mensajes de detección DHCP entrantes. Esto requiere que el switch reciba la detección de DHCP y envíe este paquete a su CPU para su procesamiento. Una vez que se recibe y se procesa la detección de DHCP, el agente de retransmisión crea un nuevo paquete de

unidifusión originado en la interfaz donde se recibió la detección de DHCP y destinado a la dirección IP como se define en la configuración **ip helper-address**. Una vez creado el paquete, se reenvía por hardware y se envía al servidor DHCP, donde se puede procesar y, finalmente, se devuelve al agente de retransmisión para que el proceso DHCP pueda continuar para el cliente.

Un problema común que se experimenta es cuando los paquetes de transacción DHCP en el agente de retransmisión se ven afectados inadvertidamente por el tráfico que se envía a la CPU porque está sujeto a un escenario ICMP específico, como un mensaje ICMP Redirect o ICMP Destination Unreachable . Este comportamiento puede manifestarse como clientes que no pueden obtener una dirección IP de DHCP a tiempo, o incluso como falla total de asignación DHCP. En algunos escenarios, el comportamiento solo se puede observar en ciertas horas del día, como las horas punta de trabajo cuando la carga en la red está completamente maximizada.

Como se mencionó en la sección de fondo, los switches Catalyst serie 9000 vienen con una política CoPP predeterminada configurada y habilitada en el dispositivo. Esta política de CoPP actúa como una política de calidad de servicio (QoS) que se sitúa en la ruta del tráfico recibido en los puertos del panel frontal y destinado a la CPU del dispositivo. Su velocidad limita el tráfico según el tipo de tráfico y los umbrales predefinidos que se configuran en la política. Algunos ejemplos de tráfico clasificado y con velocidad limitada de forma predeterminada son los paquetes de control de routing (normalmente marcados con DSCP CS6), los paquetes de control de topología (BPDU de STP) y los paquetes de baja latencia (BFD). Se debe dar prioridad a estos paquetes, ya que la capacidad de procesarlos de forma fiable da como resultado un entorno de red estable.

Vea las estadísticas del regulador de CoPP con el comando **show platform hardware fed switch active qos queue stats internal cpu policer**.

Tanto la cola de redirección ICMP (cola 6) como la cola de DIFUSIÓN (cola 12) comparten el mismo PlcIdx de 0 (índice del regulador). Esto significa que cualquier tráfico de difusión que deba ser procesado por la CPU del dispositivo, como una detección de DHCP, se comparte con el tráfico que también está destinado a la CPU del dispositivo en la cola de redirección ICMP. Esto puede resultar en el problema mencionado anteriormente, donde las transacciones DHCP fallan porque el tráfico de cola de redirección ICMP priva el tráfico que necesita ser atendido por la cola BROADCAST, lo que resulta en paquetes de difusión legítimos perdidos.

```
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>
```

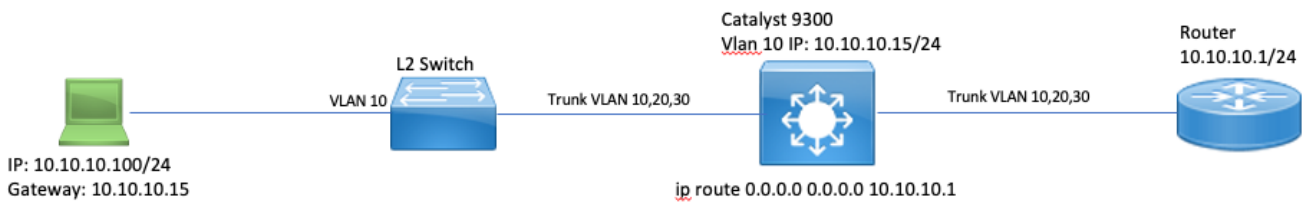
El tráfico que excede la velocidad predeterminada de 600 paquetes por segundo en la política CoPP se descarta antes de que llegue a la CPU.

```
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>
```

Situación 1: redirecciones ICMP

Considere esta topología para el primer escenario:



La secuencia de eventos es la siguiente:

1. Un usuario en 10.10.10.100 inicia una conexión telnet al dispositivo 10.100.100.100, una red remota.

2. La IP de destino está en una subred diferente, por lo que el paquete se envía a la gateway predeterminada de los usuarios, 10.10.10.15.

3. Cuando el Catalyst 9300 recibe este paquete para rutear, lo envía a su CPU para generar un Redireccionamiento ICMP.

La redirección ICMP se genera porque, desde la perspectiva del switch 9300, sería más eficiente para el portátil simplemente enviar este paquete al router en 10.10.10.1 directamente, ya que es el siguiente salto de Catalyst 9300 de todos modos, y está en la misma VLAN en la que está el usuario.

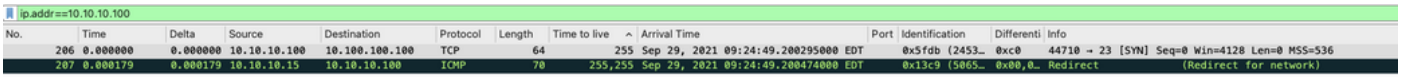
El problema es que todo el flujo se procesa en la CPU, ya que cumple con los criterios de Redirección ICMP. Si otros dispositivos envían tráfico que cumple con el escenario de redirección ICMP, aún más tráfico comienza a ser impulsado a la CPU en esta cola, lo que podría afectar a la cola BROADCAST ya que comparten el mismo regulador CoPP.

Debug ICMP para ver el syslog de redirección 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
```

> Precaución: debido a la verbosidad a escala, se recomienda inhabilitar el registro de la consola y el monitoreo de terminal antes de habilitar los debugs ICMP.

Una captura de paquetes incorporada en la CPU de Catalyst 9300 muestra el TCP SYN inicial para la conexión Telnet en la CPU, así como el ICMP Redirect que se genera.



El paquete de redirección ICMP se origina en la interfaz Catalyst 9300 VLAN 10 destinada al cliente y contiene los encabezados de paquete originales para los cuales se envía el paquete de redirección 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
```

Solución

En esta situación, los paquetes que se dirigen a la CPU pueden evitarse, lo que también detiene la generación del paquete de redirección ICMP.

Los sistemas operativos modernos no emplean el uso de mensajes de redirección ICMP, por lo que los recursos necesarios para generar, enviar y procesar estos paquetes no son un uso eficiente de los recursos de la CPU en los dispositivos de red.

Alternativamente, indique al usuario que utilice la gateway predeterminada de 10.10.10.1, pero dicha configuración puede estar en su lugar por una razón y está fuera del alcance de este documento.

Simplemente inhabilite las redirecciones ICMP con la CLI **no ip redirects**.

```
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
```

Verifique que las redirecciones ICMP estén inhabilitadas en una interfaz.

```
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>
```

Puede encontrar más información sobre las redirecciones ICMP y cuándo se envían en este enlace: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

Situación 2: ICMP inalcanzables

Considere la misma topología donde el usuario en 10.10.10.100 inicia una conexión Telnet a 10.100.100.100. Esta vez se ha configurado una lista de acceso entrante en la VLAN 10 SVI que bloquea las conexiones 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 secuencia de eventos es la siguiente:

1. El usuario en 10.10.10.100 inicia una conexión telnet al dispositivo 10.100.100.100.

2. La IP de destino está en una subred diferente, por lo que el paquete se envía a la gateway predeterminada de los usuarios.

3. Cuando el Catalyst 9300 recibe este paquete, se evalúa frente a la ACL entrante y se bloquea.

4. Dado que el paquete está bloqueado y las IP inalcanzables están habilitadas en la interfaz, el paquete se envía a la CPU para que el dispositivo pueda generar un paquete de destino ICMP inalcanzable.

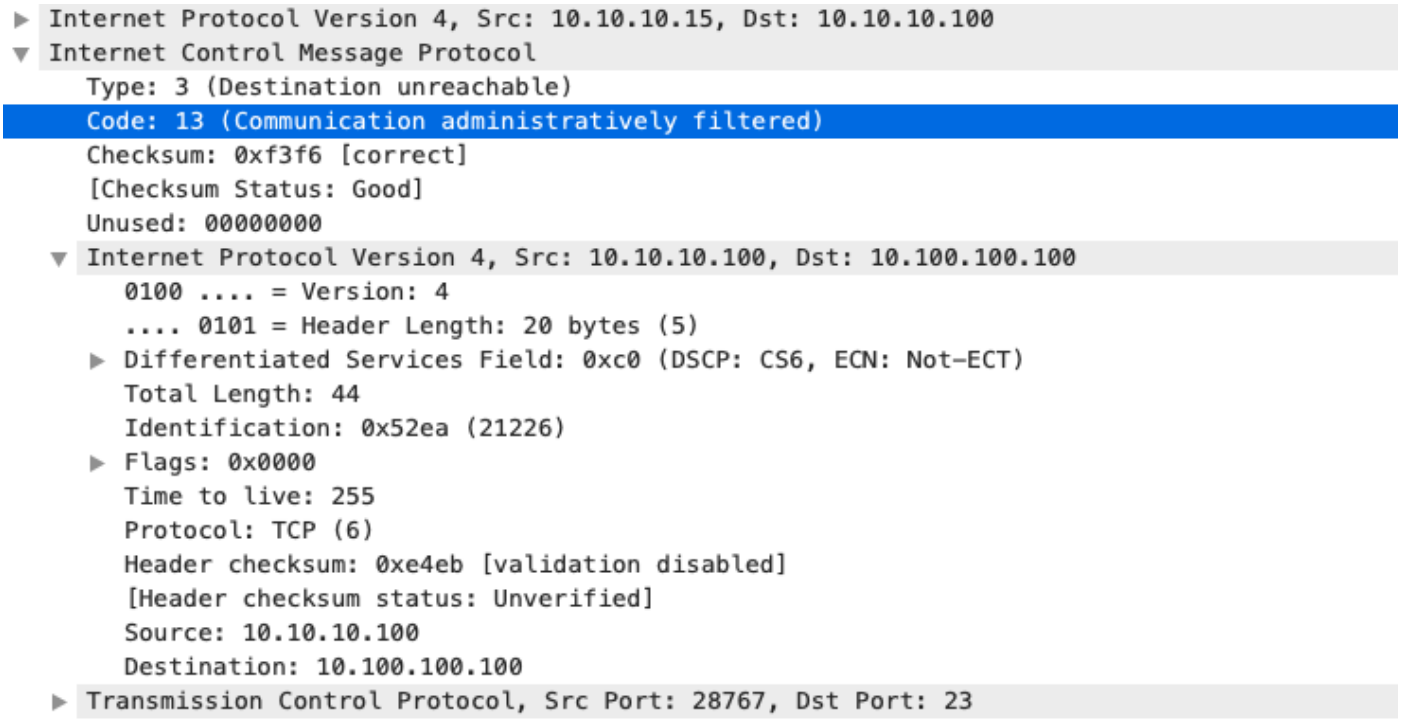
Debug ICMP para ver el syslog de destino ICMP inalcanzable.

```
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
```

> Precaución: debido a la verbosidad a escala, se recomienda inhabilitar el registro de la consola y el monitoreo de terminal antes de habilitar los debugs ICMP.

Una captura de paquetes incorporada en la CPU de Catalyst 9300 muestra el TCP SYN inicial para la conexión Telnet en la CPU, así como el destino ICMP inalcanzable que se envía.

El paquete ICMP de destino inalcanzable se origina en la interfaz Catalyst 9300 VLAN 10 destinada al cliente y contiene los encabezados de paquete originales para los cuales se envía el paquete ICMP.



Solución

En este escenario, inhabilite el comportamiento donde los paquetes punteados que son bloqueados por una ACL para generar el mensaje ICMP Destination Unreachable.

La funcionalidad IP Unreachable se habilita de forma predeterminada en las interfaces enrutadas en los switches Catalyst de la 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
```

Verifique que estén inhabilitados para la interfaz.

```
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>
```

Situación 3: TTL ICMP superado

Considere la topología anterior utilizada para los 2 escenarios anteriores. Esta vez, el usuario de 10.10.10.100 intenta acceder a un recurso de una red que se ha retirado desde entonces. Debido a esto, la SVI y la VLAN que solían alojar esta red ya no existen en el Catalyst 9300. Sin embargo, el router todavía tiene una ruta estática que apunta a la interfaz de VLAN 10 de Catalyst 9300 como el salto siguiente para esta red.

Dado que el Catalyst 9300 ya no tiene esta red configurada, no se muestra como conectado directamente y el 9300 enruta todos los paquetes para los cuales no tiene una ruta específica a su ruta estática predeterminada que apunta al router en 10.10.10.1.

Este comportamiento introduce un loop de ruteo en la red cuando el usuario intenta conectarse a un recurso en el espacio de direcciones 192.168.10.0/24. El paquete se pone en loop entre el 9300 y el router hasta que caduca el TTL.

1. El usuario intenta conectarse a un recurso de la red 192.168.10/24

2. El paquete es recibido por el Catalyst 9300 y se rutea a su ruta predeterminada con el salto siguiente 10.10.10.1 y disminuye el TTL en 1.

3. El router recibe este paquete y verifica la tabla de ruteo para encontrar que hay una ruta para esta red con el salto siguiente 10.10.10.15. Reduce el TTL en 1 y enruta el paquete de vuelta al 9300.

4. El Catalyst 9300 recibe el paquete y una vez más lo rutea de nuevo a 10.10.10.1 y reduce el TTL en 1.

Este proceso se repite hasta que el TTL IP llega a cero.

Cuando el Catalyst recibe el paquete con IP TTL = 1, dirige el paquete a la CPU y genera un mensaje ICMP TTL-Exceeded .

El tipo de paquete ICMP es 11 con el código 0 (TTL caducado en tránsito). Este tipo de paquete no se puede inhabilitar mediante comandos CLI

El problema con el tráfico DHCP entra en juego en este escenario porque los paquetes que se looped están sujetos a la redirección ICMP ya que dejan fuera la misma interfaz en la que se recibieron.

Los paquetes enviados desde el usuario también están sujetos a la redirección ICMP. El tráfico DHCP se puede eliminar fácilmente de la cola BROADCAST en este escenario. A escala, este escenario sería aún peor debido al número de paquetes impulsados en la cola de redirección.

Aquí las caídas de CoPP se demuestran a través de 1000 pings a la red 192.168.10.0/24 con un tiempo de espera de 0 segundos entre cada ping. Las estadísticas de CoPP en el 9300 se borran y se descartan a cero bytes antes de que se envíen los pings.

```
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>
```

El usuario envía tráfico a la red 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)
```

Los debugs ICMP muestran los syslogs Redirect y TTL-Exceeded debido al loop de ruteo.

```
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>
```

> Precaución: debido a la verbosidad a escala, se recomienda inhabilitar el registro de la consola y el monitoreo de terminal antes de habilitar los debugs ICMP.

Se observan caídas de CoPP debido a la cantidad de tráfico dirigido a la CPU para su redirección. Tenga en cuenta que esto es solo para un único cliente.

```
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>
```

Solución

La solución en este escenario es inhabilitar las redirecciones ICMP, al igual que en el escenario 1. El loop de ruteo también es un problema, pero la intensidad se agrava porque los paquetes también se puntean para la redirección.

Los paquetes ICMP TTL-Exceeded también son impulsados cuando TTL es 1 pero estos paquetes utilizan un índice CoPP Policer diferente y no comparten una cola con BROADCAST para que el tráfico DHCP no se vea afectado.

Simplemente inhabilite las redirecciones ICMP con la CLI no ip redirects.

```
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
```

Información Relacionada

- Configuración de Captura de Paquetes Integrada
- Comprensión de ICMP Redirects
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).