Probleemoplossing voor langzame of intermitterende DHCP op Catalyst 9000 DHCP Relay-agents

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij de toewijzing van langzame Dynamic Host Configuration Protocol (DHCP)-adressen of bij incidentele DHCP-adrestoewijzing op Catalyst 9000 Series switches als DHCP-relay agents.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- DHCP- en DHCP Relay-agents
- Internet Control Message Protocol (ICMP)
- Toezicht op besturingsplane (CoPP)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9000 Series switches
- Cisco IOS XE® versies 16.x en 17.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- Catalyst 3650/3850 Series switches met Cisco IOS XE® 16.x

Achtergrondinformatie

De Control Plane Policing (CoPP)-functie verbetert de beveiliging van uw apparaat door de CPU te beschermen tegen onnodig verkeer en DoS-aanvallen (Denial of Service). Het kan ook controleverkeer en beheersverkeer beschermen tegen verkeersdalingen die worden veroorzaakt door grote hoeveelheden ander verkeer met een lagere prioriteit.

Uw apparaat is gewoonlijk opgedeeld in drie operationele vlakken, elk met een eigen doel:

- Het gegevensvlak, om gegevenspakketten door:sturen.
- Het controlevlak, om gegevens correct te leiden.
- Het beheersplatform, om netwerkelementen te beheren.

U kunt CoPP gebruiken om het grootste deel van het CPU-gebonden verkeer te beveiligen en om routerstabiliteit, bereikbaarheid en pakketlevering te garanderen. Het belangrijkste is dat u CoPP kunt gebruiken om de CPU te beschermen tegen een DoS-aanval.

CoPP gebruikt de modulaire QoS-opdrachtregelinterface (MQC) en CPU-wachtrijen om deze doelstellingen te bereiken. Verschillende typen verkeer van besturingsplane worden gegroepeerd op basis van bepaalde criteria en toegewezen aan een CPU-wachtrij. U kunt deze CPU-wachtrijen beheren door specifieke policers in hardware te configureren. U kunt bijvoorbeeld de policersnelheid wijzigen voor bepaalde CPU-wachtrijen (traffic-type) of u kunt de policer uitschakelen voor een bepaald type verkeer.

Hoewel de policers in hardware zijn geconfigureerd, heeft CoPP geen invloed op de CPU-prestaties of de prestaties van het gegevensvlak. Maar omdat de CPU het aantal pakketten beperkt dat naar de CPU gaat, wordt de lading van de CPU bepaald. Dit betekent dat diensten die wachten op pakketten van hardware een meer gecontroleerde snelheid van ingangspakketten kunnen zien (het tarief is gebruiker-configureerbaar).

Probleem

Een Catalyst 9000 switch wordt geconfigureerd als DHCP-relay-agent wanneer de **ip helper-address** opdracht is geconfigureerd op een routeringsinterface voor SVI. De interface waar het helperadres wordt gevormd is typisch de standaardgateway voor stroomafwaartse cliënten. Voor de switch om de succesvolle DHCP Relay-services aan zijn clients te kunnen leveren, moet het inkomende DHCP Discover-berichten kunnen verwerken. Dit vereist dat de switch de DHCP Discover ontvangt en dit pakket naar zijn CPU stopt om te verwerken. Zodra de DHCP Discover is ontvangen en verwerkt, maakt de relay-agent een nieuw unicastpakket dat afkomstig is van de interface waar de DHCP Discover is ontvangen en bestemd is voor het IP-adres zoals gedefinieerd in de configuratie van het **IP-helperadres**. Nadat het pakket is gemaakt, wordt de

hardware doorgestuurd en verzonden naar de DHCP-server waar het kan worden verwerkt en uiteindelijk teruggestuurd naar de relay agent zodat het DHCP-proces kan worden voortgezet voor de client.

Een gemeenschappelijk probleem dat wordt ervaren is wanneer de transactiepakketten van DHCP bij de relay agent per ongeluk door verkeer worden beïnvloed dat naar CPU wordt verzonden omdat het aan een specifiek scenario ICMP, zoals een ICMP Redirect of een Onbereikbaar bericht van de Bestemming ICMP onderworpen is. Dit gedrag kan zich manifesteren als cliënten niet bekwaam om een IP adres van DHCP, of zelfs totale de taakmislukking van DHCP tijdig te krijgen. In sommige scenario's zou het gedrag slechts op bepaalde tijden van de dag, zoals piekuren kunnen worden waargenomen wanneer de lading op het netwerk volledig wordt gemaximaliseerd.

Zoals vermeld in de sectie Achtergrond, Catalyst 9000 Series Switches worden geleverd met een standaard CoPP-beleid dat op het apparaat is geconfigureerd en ingeschakeld. Dit CoPP-beleid fungeert als een QoS-beleid (Quality of Service) dat zich in het pad van verkeer bevindt dat wordt ontvangen op poorten op het voorpaneel en is bestemd voor de CPU van het apparaat. Het tarief beperkt verkeer op basis van het verkeerstype en de vooraf gedefinieerde drempels die in het beleid zijn geconfigureerd. Sommige voorbeelden van verkeer dat is geclassificeerd en tarief dat door gebrek wordt beperkt zijn Routing Control-pakketten (die doorgaans worden gemarkeerd met DSCP CS6), Topology Control-pakketten (STP BPDU's) en Low Latency-pakketten (BFD). Aan deze pakketten moet prioriteit worden gegeven omdat de mogelijkheid om deze op betrouwbare wijze te verwerken resulteert in een stabiele netwerkomgeving.

Bekijk de CoPP politiestatistieken met de **show platform hardware gevoede switch actieve qos wachtrij stats internal cpu politiecommando**.

De ICMP Redirect-wachtrij (wachtrij 6) en de BROADCAST-wachtrij (wachtrij 12) delen beide dezelfde PlcIndex van 0 (Policer Index). Dit betekent dat om het even welk uitzendingsverkeer dat door het apparaat cpu moet worden verwerkt, zoals een Ontdekking van DHCP, met verkeer wordt gedeeld dat ook bestemd is voor het apparaat cpu in de rij van ICMP Redirect. Dit kan resulteren in het eerder genoemde probleem waar DHCP-transacties mislukken omdat het ICMP-omleiden wachtrijverkeer verkeer uitdooft dat moet worden onderhouden door de BROADCAST-wachtrij, wat resulteert in het vervallen van legitieme uitzendingspakketten.

```
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>
```

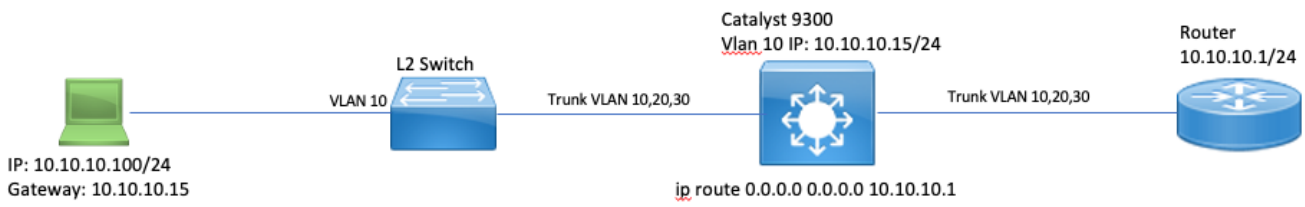
Verkeer dat het standaard 600-pakket per seconde in het CoPP-beleid overschrijdt, wordt gedropt voordat het de CPU bereikt.

```
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: ICMP-omleidingen

Overweeg deze topologie voor het eerste scenario:



De volgorde van de gebeurtenissen is als volgt:

1. Een gebruiker op 10.10.10.100 start een Telnet-verbinding met apparaat 10.100.100.100, een extern netwerk.

2. Het bestemmingsIP-adres bevindt zich in een andere subnetverbinding, zodat het pakket naar de standaardgateway van de gebruikers wordt verzonden, 10.10.10.15.

3. Wanneer Catalyst 9300 dit pakket naar route ontvangt, wordt het pakket doorgeprikt naar de CPU om een ICMP-omleiding te genereren.

ICMP Redirect wordt gegenereerd omdat vanuit het perspectief van de 9300 switch, het efficiënter voor de laptop zou zijn om dit pakket eenvoudig naar de router te verzenden op 10.10.10.1 direct, aangezien dat Catalyst 9300's volgende hop hoe dan ook is, en het in hetzelfde VLAN is waarin de gebruiker is.

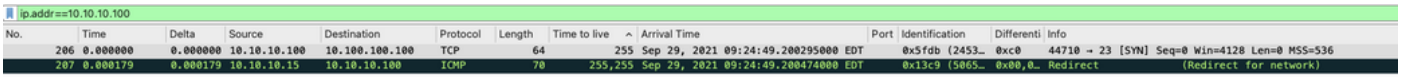
Het probleem is dat de gehele stroom bij de CPU wordt verwerkt omdat deze voldoet aan de ICMP-omleidingscriteria. Als andere apparaten worden verzonden verkeer dat voldoet aan de ICMP omleiden scenario nog meer verkeer begint te worden gestraft naar de CPU in deze wachtrij die de BROADCAST-wachtrij zou kunnen beïnvloeden omdat ze dezelfde CoPP-policer delen.

Debug ICMP om de ICMP Redirect-syslog te bekijken.

```
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
```

> Waarschuwing: vanwege de breedsprakigheid op schaal is het aan te raden om de logboekregistratie van de console en de controle van de terminal uit te schakelen voordat u ICMP-debugs inschakelt.

Een ingesloten pakketvastlegging op de Catalyst 9300 CPU toont de initiële TCP-SYN voor de Telnet-verbinding op de CPU, alsook de gegenereerde ICMP-omleiding.



Het ICMP Redirect-pakket is afkomstig van de Catalyst 9300 VLAN 10-interface die is bestemd voor de client en bevat de oorspronkelijke pakketkopregels waarvoor het ICMP Redirect-pakket is verzonden.

```
▼ 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
```

Oplossing

In dit scenario kunnen de pakketten die tot op de CPU zijn doorgeprikt worden voorkomen, wat ook een einde maakt aan de generatie van het ICMP-pakket voor omleiding.

Moderne besturingssystemen maken geen gebruik van ICMP Redirect-berichten, zodat de bronnen die nodig zijn om deze pakketten te genereren, verzenden en verwerken geen efficiënt gebruik van CPU-bronnen op netwerkapparaten zijn.

U kunt ook de gebruiker aanwijzen om de standaardgateway van 10.10.10.1 te gebruiken, maar een dergelijke configuratie kan met reden zijn geïnstalleerd en valt buiten het bereik van dit document.

Schakel ICMP-omleidingen eenvoudigweg uit met de CLI **zonder IP-omleidingen**.

```
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
```

Controleer of ICMP-omleidingen op een interface zijn uitgeschakeld.

```
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>
```

Meer informatie over ICMP-omleidingen en wanneer deze worden verzonden, kunt u vinden op deze link: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html

Scenario 2: ICMP-onbereikbaar

Overweeg dezelfde topologie waar de gebruiker op 10.10.10.100 een Telnet-verbinding met 10.100.100.100 initieert. Ditmaal is een toegangslijst inbound geconfigureerd op VLAN 10 SVI dat telnet-verbindingen blokkeert.


```
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#
```

De volgorde van de gebeurtenissen is als volgt:

1. Gebruiker op 10.10.10.100 start een Telnet-verbinding met apparaat 10.100.100.100.

2. De bestemming IP bevindt zich in een andere subnetverbinding, zodat het pakket naar de standaardgateway van de gebruikers wordt verzonden.

3. Wanneer Catalyst 9300 dit pakket ontvangt, wordt het beoordeeld op basis van de inkomende ACL en wordt het geblokkeerd.

4. Aangezien het pakket wordt geblokkeerd en IP-onbereikbaar wordt ingeschakeld op de interface, wordt het pakket naar de CPU geprikt, zodat het apparaat een ICMP-bestemmingspakket kan genereren dat onbereikbaar is.

Debug ICMP om de ICMP bestemming onbereikbare syslog te bekijken.

```
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
```

> **Waarschuwing**: vanwege de breedsprakigheid op schaal is het aan te raden om de logboekregistratie van de console en de controle van de terminal uit te schakelen voordat u ICMP-debugs inschakelt.

Een ingesloten pakketvastlegging op Catalyst 9300 CPU toont de eerste TCP-SYN voor de Telnet-verbinding op de CPU en de onbereikbare ICMP-bestemming die wordt verzonden.

Het onbereikbare pakket voor ICMP-bestemming is afkomstig van de Catalyst 9300 VLAN 10-interface die is bestemd voor de client en bevat de oorspronkelijke pakketheader waarvoor het ICMP-pakket wordt verzonden.

```
▶ Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.100
▼ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 13 (Communication administratively filtered)
    Checksum: 0xf3f6 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▼ 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: 0x52ea (21226)
    ▶ Flags: 0x0000
      Time to live: 255
      Protocol: TCP (6)
      Header checksum: 0xe4eb [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.10.10.100
      Destination: 10.100.100.100
  ▶ Transmission Control Protocol, Src Port: 28767, Dst Port: 23
```

Oplossing

In dit scenario, maak het gedrag onbruikbaar waar punted pakketten die door ACL worden geblokkeerd om het Onbereikbare bericht van de Bestemming te produceren ICMP.

IP Onbereikbare functionaliteit is standaard ingeschakeld op routed interfaces op Catalyst 9000 Series switches.

```
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
```

Controleer of ze uitgeschakeld zijn voor de interface.

```
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: ICMP TTL-overtroffen

Overweeg de vroegere topologie die voor de vorige 2 scenario's wordt gebruikt. Ditmaal probeert de gebruiker op 10.10.10.10 een hulpbron te bereiken in een netwerk dat sindsdien uit bedrijf is genomen. Hierdoor bestaan de SVI en VLAN die gebruikt werden om dit netwerk te hosten niet meer op Catalyst 9300. De router heeft echter nog steeds een statische route die naar de Catalyst 9300 VLAN 10-interface wijst als de volgende hop voor dit netwerk.

Aangezien Catalyst 9300 dit netwerk niet meer geconfigureerd heeft, wordt het niet weergegeven zoals direct verbonden en de 9300 routert pakketten waarvoor het geen specifieke route voor zijn statische standaardroute heeft die naar de router op 10.10.10.1 wijst.

Dit gedrag introduceert een routinglus in het netwerk wanneer de gebruiker probeert verbinding te maken met een resource in de adresruimte van 192.168.10.0/24. Het pakket wordt van een lus voorzien tussen de 9300 en de router tot het TTL verloopt.

1. Gebruiker probeert verbinding te maken met een resource in 192.168.10/24

2. Packet wordt ontvangen door Catalyst 9300 en wordt met volgende hop 10.10.10.1 en decreten op de TTL met 1 gerouteerd naar de standaardroute.

3. De router ontvangt dit pakket en controleert de routeringstabel om er achter te komen dat er een route is voor dit netwerk met volgende hop 10.10.10.15. Het decreteert de TTL met 1 en leidt het pakket terug naar 9300.

4. Catalyst 9300 ontvangt het pakket en routeert het opnieuw naar 10.10.10.1 en legt het TTL vast op 1.

Dit proces herhaalt zich tot de IP TTL nul bereikt.

Wanneer de Catalyst het pakket met IP TTL = 1 ontvangt, wordt het pakket doorboord naar de CPU en wordt een ICMP-bericht met TTL-overschrijding gegenereerd.

Het ICMP-pakkettype is 11 met code 0 (TTL is verlopen tijdens het transport). Dit pakkettype kan niet worden uitgeschakeld met CLI-opdrachten

Het probleem met DHCP-verkeer speelt zich af in dit scenario omdat de pakketten die in een lusje worden weergegeven onderworpen zijn aan ICMP-omleiding omdat ze dezelfde interface uitsluiten als ze op werden ontvangen.

De pakketten die van de Gebruiker worden verzonden zijn ook onderworpen aan omleiding ICMP. DHCP-verkeer kan in dit scenario eenvoudig worden overbodig uit de BROADCAST-wachtrij. Op schaal, zou dit scenario nog slechter zijn toe te schrijven aan het aantal pakketten die in de redirect rij worden gestraft.

Hier worden CoPP druppels gedemonstreerd via 1000 pings aan het 192.168.10.0/24 netwerk met onderbreking van 0 seconden tussen elk pingelen. De CoPP-statistieken op de 9300 worden gewist en op nul bytes gedropt voordat de pings worden verzonden.

```
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>
```

Gebruiker verzendt verkeer naar extern netwerk.

```
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)
```

ICMP-debugs tonen de systemen met omleiding en TTL-overschrijding die het gevolg zijn van een routinglus.

```
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>
```

> **Waarschuwing**: vanwege de breedsprakigheid op schaal is het aan te raden om de logboekregistratie van de console en de controle van de terminal uit te schakelen voordat u ICMP-debugs inschakelt.

CoPP-dalingen worden gezien door de hoeveelheid verkeer die naar CPU wordt gestraft voor omleiding. Let op dat dit slechts voor één client is.

```
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>
```

Oplossing

De oplossing in dit scenario is ICMP-omleidingen uit te schakelen, hetzelfde als in scenario 1. De routing loop is ook een probleem, maar de intensiteit wordt samengeperst omdat de pakketten ook voor omleiding worden gestraft.

ICMP TTL-Exceeded pakketten worden ook gestraft wanneer TTL 1 is maar deze pakketten gebruiken een verschillende CoPP Policer index en delen geen wachtrij met BROADCAST zodat wordt het DHCP-verkeer niet beïnvloed.

Schakel ICMP-omleidingen simpelweg uit met de no-ip-omleidingen CLI.

```
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
```

Gerelateerde informatie

- Ingesloten pakketvastlegging configureren
- ICMP-omleidingen begrijpen
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.