# Identificar e Solucionar Problemas de DHCP Lento ou Intermitente em Agentes de Retransmissão DHCP do Catalyst 9000

## Contents



## Introduction

Este documento descreve como solucionar problemas de alocação de endereço lenta do Dynamic Host Configuration Protocol (DHCP) ou falhas intermitentes de alocação de endereço DHCP nos switches da série Catalyst 9000 como agentes de retransmissão DHCP.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Agentes de DHCP e de retransmissão de DHCP
- ICMP (Internet Control Message Protocol)
- Política de plano de controle (CoPP)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9000 Series Switches
- Cisco IOS XE® versões 16.x e 17.x

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

### Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

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

## Informações de Apoio

O recurso de Políticas de Plano de Controle (CoPP - Control Plane Policing) melhora a segurança do dispositivo através da proteção da CPU contra tráfego desnecessário e ataques de negação de serviço (DoS - Denial of Service). Ele também pode proteger o tráfego de controle e o tráfego de gerenciamento contra quedas de tráfego causadas por grandes volumes de outros tráfegos de prioridade mais baixa.

Seu dispositivo é normalmente segmentado em três planos de operação, cada um com seu próprio objetivo:

- O plano de dados, para encaminhar pacotes de dados.
- O plano de controle, para rotear dados corretamente.
- O plano de gerenciamento, para gerenciar elementos de rede.

Você pode usar o CoPP para proteger a maior parte do tráfego vinculado à CPU e garantir a estabilidade do roteamento, o alcance e a entrega de pacotes. O mais importante é que você pode usar CoPP para proteger a CPU de um ataque de DoS.

O CoPP usa a interface de linha de comando QoS modular (MQC) e as filas de CPU para atingir esses objetivos. Diferentes tipos de tráfego de plano de controle são agrupados com base em determinados critérios e atribuídos a uma fila de CPU. Você pode gerenciar essas filas de CPU pela configuração de vigilantes dedicados no hardware. Por exemplo, você pode modificar a taxa do vigilante para determinadas filas da CPU (tipo de tráfego) ou pode desativar o vigilante para um determinado tipo de tráfego.

Embora os vigilantes sejam configurados no hardware, o CoPP não afeta o desempenho da CPU nem o desempenho do plano de dados. Mas como ele limita o número de pacotes enviados para a CPU, a carga da CPU é controlada. Isso significa que os serviços que aguardam pacotes do hardware podem ver uma taxa mais controlada de pacotes de entrada (a taxa é configurável pelo usuário).

## Problema

Um switch Catalyst 9000 é configurado como um agente de retransmissão DHCP quando o comando **ip helper-address** é configurado em uma interface roteada ou SVI. A interface em que o endereço do auxiliar é configurado normalmente é o gateway padrão para clientes downstream. Para que o switch forneça serviços de retransmissão DHCP bem-sucedidos a seus clientes, ele deve ser capaz de processar mensagens de descoberta de DHCP de entrada. Isso exige que o switch receba o DHCP Discover e coloque esse pacote na CPU para processá-lo. Depois que a descoberta de DHCP é recebida e processada, o agente de retransmissão cria um novo pacote unicast originado da interface em que a descoberta de DHCP foi recebida e destinado ao

endereço IP, conforme definido na configuração **ip helper-address**. Depois que o pacote é criado, ele é encaminhado por hardware e enviado ao servidor DHCP, onde pode ser processado e finalmente enviado de volta ao agente de retransmissão para que o processo DHCP possa continuar para o cliente.

Um problema comum observado ocorre quando os pacotes de transação DHCP no agente de retransmissão são inadvertidamente afetados pelo tráfego enviado à CPU porque está sujeito a um cenário ICMP específico, como um Redirecionamento ICMP ou uma mensagem de Destino Inalcançável ICMP. Esse comportamento pode se manifestar como clientes que não conseguem obter um endereço IP do DHCP em tempo hábil ou até mesmo uma falha total na atribuição de DHCP. Em alguns cenários, o comportamento só pode ser observado em determinadas horas do dia, como horário comercial de pico, quando a carga na rede é totalmente maximizada.

Como mencionado na seção Plano de fundo, os switches Catalyst 9000 Series vêm com uma política de CoPP padrão configurada e ativada no dispositivo. Essa política de CoPP atua como uma política de Qualidade de Serviço (QoS) que reside no caminho do tráfego que é recebido nas portas do painel frontal e é destinado à CPU do dispositivo. A taxa limita o tráfego com base no tipo de tráfego e nos limites predefinidos configurados na política. Alguns exemplos de tráfego que é classificado e cuja taxa é limitada por padrão são pacotes de controle de roteamento (normalmente marcados com DSCP CS6), pacotes de controle de topologia (STP BPDUs), pacotes de baixa latência (BFD). Esses pacotes devem ser priorizados porque a capacidade de processá-los de forma confiável resulta em um ambiente de rede estável.

Exiba as estatísticas do vigilante de CoPP com o comando **show platform hardware fed switch ative qos queue stats internal cpu policer**.

A fila de redirecionamento ICMP (Fila 6) e a fila de BROADCAST (Fila 12) compartilham o mesmo PlcIdx de 0 (Índice do vigilante). Isso significa que qualquer tráfego de broadcast que precise ser processado pela CPU do dispositivo, como uma Descoberta de DHCP, é compartilhado com o tráfego que também é destinado à CPU do dispositivo na fila de Redirecionamento de ICMP. Isso pode resultar no problema mencionado anteriormente, onde as transações DHCP falham, porque o tráfego da fila de redirecionamento de ICMP elimina o tráfego que precisa ser atendido pela fila de BROADCAST, o que resulta na eliminação de pacotes de broadcast legítimos.

```
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>
```

O tráfego que excede a taxa padrão de 600 pacotes por segundo na política de CoPP é descartado antes de alcançar a 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>
```

## Cenário 1: Redirecionamentos de ICMP

Considere esta topologia para o primeiro cenário:


A sequência de eventos é a seguinte:

1. Um usuário em 10.10.10.100 inicia uma conexão telnet com o dispositivo 10.100.100.100, uma

rede remota.

2. O IP destino está em uma sub-rede diferente, de modo que o pacote é enviado ao gateway padrão do usuário, 10.10.10.15.

3. Quando o Catalyst 9300 recebe esse pacote para rotear, ele direciona o pacote para sua CPU para gerar um Redirecionamento ICMP.

O Redirecionamento ICMP é gerado porque, da perspectiva do switch 9300, seria mais eficiente para o laptop simplesmente enviar esse pacote para o Roteador diretamente em 10.10.10.1, já que esse é o próximo salto do Catalyst 9300 de qualquer maneira, e está na mesma VLAN em que o usuário está.

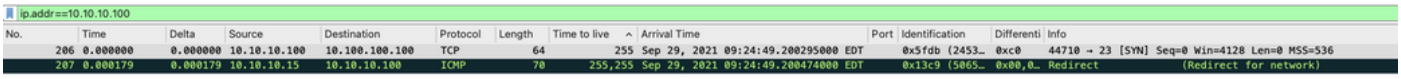
O problema é que todo o fluxo é processado na CPU, já que ele atende aos critérios de redirecionamento ICMP. Se outros dispositivos enviarem tráfego que atenda ao cenário de redirecionamento de ICMP, ainda mais tráfego começará a ser direcionado para a CPU nessa fila, o que poderia afetar a fila de BROADCAST, já que eles compartilham o mesmo vigilante de CoPP.

Depurar o ICMP para exibir o syslog de redirecionamento do 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
```

> Cuidado: devido à verbosidade em escala, é recomendável desativar o registro de console e o monitoramento de terminal antes de habilitar as depurações ICMP.

Uma Captura de Pacote Incorporada na CPU do Catalyst 9300 mostra o TCP SYN inicial para a conexão Telnet na CPU, bem como o Redirecionamento ICMP gerado.




O pacote de redirecionamento ICMP é originado da interface Catalyst 9300 VLAN 10 destinada ao cliente e contém os cabeçalhos originais dos pacotes para os quais o pacote de redirecionamento ICMP é enviado.

```
▼ 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
```

## Solução

Neste cenário, os pacotes que são lançados para a CPU podem ser impedidos, o que também interrompe a geração do pacote de redirecionamento ICMP.

Os sistemas operacionais modernos não empregam o uso de mensagens de redirecionamento ICMP, de modo que os recursos necessários para gerar, enviar e processar esses pacotes não são um uso eficiente dos recursos da CPU em dispositivos de rede.

Como alternativa, aponte o usuário para usar o gateway padrão de 10.10.10.1, mas essa configuração pode estar em vigor por um motivo e está fora do escopo deste documento.

Simplesmente desative os redirecionamentos de ICMP com a 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
```

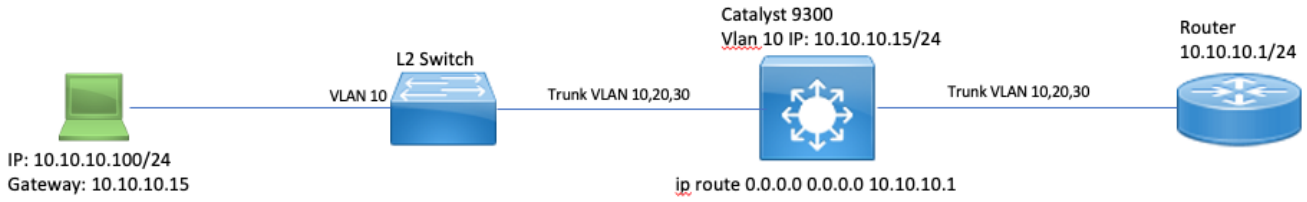
Verifique se os redirecionamentos ICMP estão desativados em uma interface.

```
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       <-- 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>
```

Mais informações sobre redirecionamentos de ICMP e quando eles são enviados podem ser encontradas neste link: [https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html](https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13714-43.html)

## Cenário 2: ICMP Inalcançável

Considere a mesma topologia em que o usuário em 10.10.10.100 inicia uma conexão Telnet para 10.100.100.100. Desta vez, uma lista de acesso foi configurada na entrada da SVI da VLAN 10 que bloqueia as conexões 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#
```

A sequência de eventos é a seguinte:

1. O usuário em 10.10.10.100 inicia uma conexão telnet com o dispositivo 10.100.100.100.

2. O IP de destino está em uma sub-rede diferente, de modo que o pacote é enviado ao gateway padrão do usuário.

3. Quando o Catalyst 9300 recebe esse pacote, ele é avaliado em relação à ACL de entrada e bloqueado.

4. Como o pacote está bloqueado e IP inalcançável está ativado na interface, o pacote é apontado para a CPU de modo que o dispositivo possa gerar um pacote ICMP de destino inalcançável.

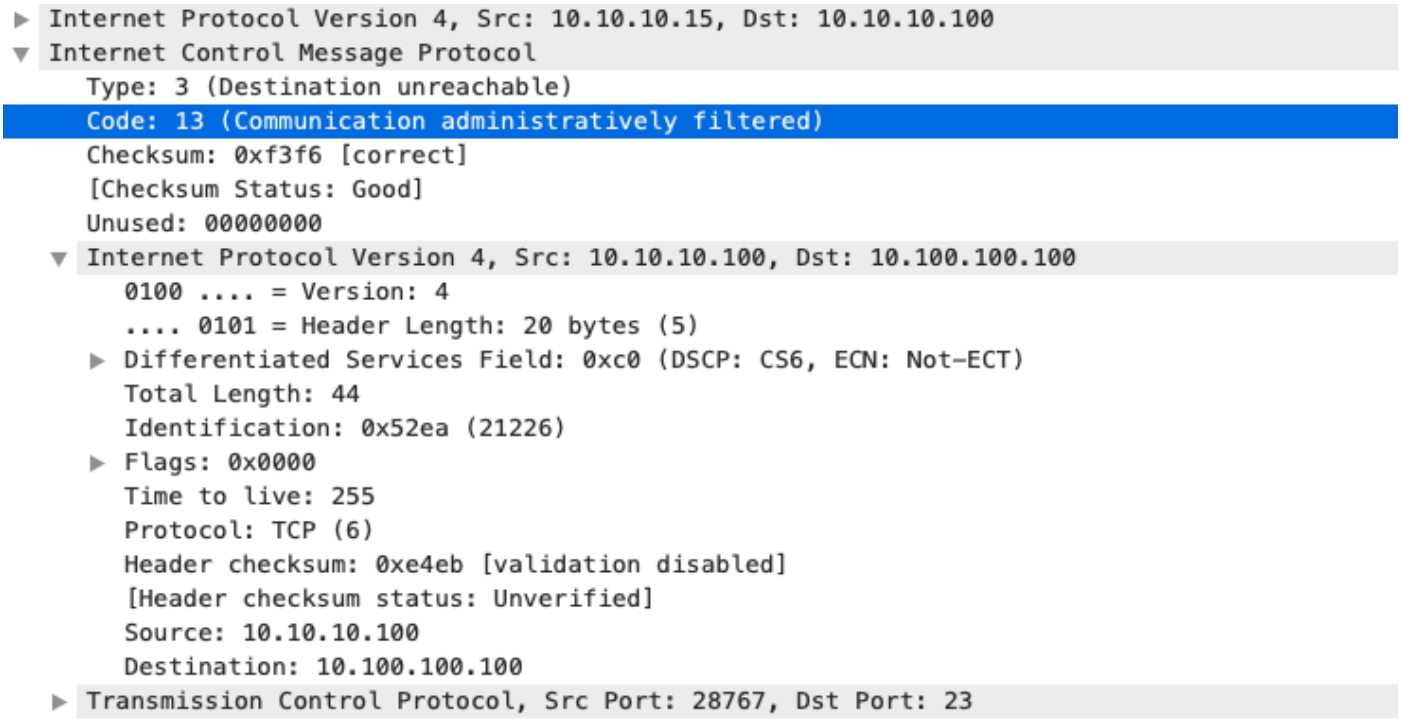
Depurar o ICMP para exibir o syslog de destino inalcançável do ICMP.

```
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
```

> **Cuidado**: devido à verbosidade em escala, é recomendável desativar o registro de console e o monitoramento de terminal antes de habilitar as depurações ICMP.

Uma Captura de Pacote Incorporada na CPU do Catalyst 9300 mostra o TCP SYN inicial para a conexão Telnet na CPU, bem como o Destino Inalcançável ICMP que é enviado.


O pacote ICMP de destino inalcançável é originado da interface Catalyst 9300 VLAN 10 destinada ao cliente e contém os cabeçalhos originais dos pacotes para os quais o pacote ICMP é enviado.




## Solução

Neste cenário, desabilite o comportamento onde pacotes puntados são bloqueados por uma ACL para gerar a mensagem ICMP de destino inalcançável.

A funcionalidade IP Inalcançável é habilitada por padrão em interfaces roteadas nos switches da série Catalyst 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 se eles estão desabilitados para a 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>
```

## Cenário 3: TTL ICMP excedido

Considere a topologia anterior usada para os dois cenários anteriores. Desta vez, o usuário em 10.10.10.100 tenta acessar um recurso em uma rede que foi descomissionada desde então. Devido a isso, o SVI e a VLAN que eram usados para hospedar essa rede não existem mais no Catalyst 9300. No entanto, o Roteador ainda tem uma rota estática que aponta para a interface da VLAN 10 do Catalyst 9300 como o próximo salto dessa rede.

Como o Catalyst 9300 não tem mais essa rede configurada, ele não mostra como conectado diretamente e o 9300 roteia todos os pacotes para os quais não tem uma rota específica para a sua rota padrão estática que aponta para o Roteador em 10.10.10.1.

Esse comportamento introduz um loop de roteamento na rede quando o usuário tenta se conectar a um recurso no espaço de endereço 192.168.10.0/24. O pacote fica em loop entre o 9300 e o Roteador até que o TTL expire.


1. O usuário tenta se conectar a um recurso na rede 192.168.10/24

2. O pacote é recebido pelo Catalyst 9300 e é roteado para sua rota padrão com o próximo salto 10.10.10.1 e diminui o TTL em 1.

3. O roteador recebe esse pacote e verifica a tabela de roteamento para descobrir se há uma rota para essa rede com o próximo salto 10.10.10.15. Ele diminui o TTL em 1 e roteia o pacote de volta para o 9300.

4. O Catalyst 9300 recebe o pacote e mais uma vez o roteia de volta para 10.10.10.1 e diminui o TTL em 1.

Esse processo se repete até que o TTL IP chegue a zero.

Quando o Catalyst recebe o pacote com IP TTL = 1, ele envia o pacote para a CPU e gera uma mensagem ICMP TTL-Exceeded.

O tipo de pacote ICMP é 11 com o Código 0 (TTL expirado em trânsito). Este tipo de pacote não pode ser desativado através de comandos CLI

O problema com o tráfego DHCP entra em cena nesse cenário porque os pacotes que estão em loop estão sujeitos ao redirecionamento ICMP, pois deixam de fora a mesma interface em que foram recebidos.

Os pacotes enviados do usuário também estão sujeitos ao redirecionamento ICMP. Nesse cenário, o tráfego DHCP pode facilmente ficar privado da fila de BROADCAST. Em escala, esse cenário seria ainda pior devido ao número de pacotes lançados na fila de redirecionamento.

Aqui, as quedas de CoPP são demonstradas através de 1000 pings para a rede 192.168.10.0/24 com intervalo de 0 segundos entre cada ping. As estatísticas de CoPP no 9300 são limpas e em zero bytes são descartados antes que os pings sejam enviados.

```
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>
```

O usuário envia tráfego para a rede 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)
```

As depurações do ICMP mostram os syslogs de Redirecionamento e TTL excedido devido ao loop de roteamento.

```
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>
```

> Cuidado: devido à verbosidade em escala, é recomendável desativar o registro de console e o monitoramento de terminal antes de habilitar as depurações ICMP.

As quedas de CoPP são vistas devido à quantidade de tráfego apontado para a CPU para

redirecionamento. Observe que isso é apenas para um 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>
```

### Solução

A solução nesse cenário é desativar os redirecionamentos ICMP, o mesmo que no Cenário 1. O loop de roteamento também é um problema, mas a intensidade é aumentada porque os pacotes também são apontados para redirecionamento.

Os pacotes ICMP TTL-Exceeded também são lançados quando o TTL é 1, mas esses pacotes usam um índice CoPP Policer diferente e não compartilham uma fila com BROADCAST para que o tráfego DHCP não seja afetado.

Simplesmente desative os redirecionamentos de ICMP com a 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
```

## Informações Relacionadas

- Configurando a Captura de Pacotes Incorporados
- Entendendo os redirecionamentos de ICMP
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.