# Troubleshooting de Latência de Rede e Quedas de Pacotes nos Catalyst 9000 Switches

## Introdução

Este documento descreve uma metodologia detalhada para solucionar problemas de latência de rede e perda de pacotes nos switches Cisco Catalyst 9000 Series.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha uma compreensão fundamental dos conceitos de rede, incluindo TCP/IP, VLANs e Protocolos Spanning Tree (STPs). O conhecimento dos switches Cisco Catalyst 9000 Series e da CLI do Cisco IOS® XE é essencial. Também é necessário estar familiarizado com as ferramentas de monitoramento de rede e privilégios de acesso para configuração e diagnóstico.

### Componentes Utilizados

As informações neste documento são baseadas nos Cisco Catalyst 9000 Switches com todas as versões. Este documento não está restrito a nenhuma versão específica de software ou hardware.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Este documento foi elaborado para administradores e engenheiros de rede, fornecendo orientação para identificar, isolar e resolver esses problemas com eficiência em ambientes de rede corporativos. A latência de rede e a queda de pacotes podem afetar adversamente o

desempenho e a confiabilidade em ambientes corporativos. Esses problemas geralmente resultam de congestionamento de rede, configuração incorreta ou fatores ambientais. Os switches Cisco Catalyst 9000 Series são projetados para alto desempenho e resiliência. Este documento fornece etapas de Troubleshooting focadas para ajudar os profissionais de rede a identificar e resolver problemas de latência e queda de pacotes usando esses switches.

# Entendendo a latência de rede e quedas de pacotes

## Latência de rede

A latência de rede é a medição do atraso observado à medida que os dados atravessam uma rede da origem para o destino. Mais comumente, a latência é expressa como Round Trip Time (RTT) — o tempo que leva para um pacote trafegar da origem para o destino e de volta.

A latência é geralmente medida em milissegundos (ms).

Impacto: A alta latência pode degradar o desempenho do aplicativo, especialmente para protocolos como o TCP, que confiam em confirmações oportunas para enviar dados com eficiência.

## Quedas de pacotes

As quedas de pacotes ocorrem quando os dispositivos de rede não conseguem encaminhar pacotes para o destino pretendido, geralmente devido a congestionamento, estouros de buffer, configurações incorretas ou hardware com defeito. As quedas de pacotes são normalmente medidas como uma porcentagem de pacotes perdidos durante um intervalo específico.

Impacto: as quedas de pacotes reduzem o throughput, causam retransmissões e podem afetar a confiabilidade do aplicativo.

## Referências de latência esperadas

| Tipo de rede | RTT típico |
|---|---|
| Mesma VLAN (camada de acesso) | < 1 ms |
| Campus Core Traversal | 1 a 5 ms |

| | |
|---|---|
| WAN metro | 5 a 30 ms |
| Internet/WAN | 30 a 150 ms |

Note: A distância geográfica entre os saltos da rede pode aumentar o RTT e contribuir para uma maior latência.

## Meça a latência da rede

Comece compreendendo completamente sua rede e sua topologia. Quando sua rede é projetada com variáveis determinísticas e imprevisibilidade mínima, o processo de identificação e resolução de problemas de latência e queda de pacotes torna-se significativamente mais simples.

Duas ferramentas principais são normalmente usadas para medir a latência de rede.

### Ping

Retorna como saída se um destino é alcançável juntamente com estatísticas sobre perda de pacotes e RTT. Assim que identificar os saltos problemáticos, você pode tentar fazer ping entre eles diretamente e verificar os dispositivos para encontrar o problema.

<#root>

**Switch#ping 8.8.8.8**

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!.!!.
```

**Success rate is 60 percent (3/5),**

```
 round-trip min/avg/max = 12/
```

**15**

```
/22 ms
```

**<===== 2 dropped out of 5 packets, Average RTT 15 ms**

### Traceroute

O traceroute mostra todos os saltos no caminho de roteamento da origem para o destino, juntamente com os resultados de RTT para cada salto. Por exemplo, um traceroute pode mostrar onde na rede (que salta no caminho de roteamento) o atraso existe ou começa. Esse exemplo é mostrado na próxima saída do traceroute.

<#root>

```
Switch#traceroute 8.8.8.8



Type escape sequence to abort.
Tracing the route to 8.8.8.8

1 2 ms 2 ms 2 ms   [10.10.10.10]
2 2 ms 1 ms 1 ms   [20.20.20.20]

3 7 ms 45 ms 40 ms [30.30.30.30]



<===== High latency at this hop


4 7 ms 3 ms 1 ms   [40.40.40.40]

Note: The IP addresses shown for each hop are provided for demonstration purposes only.
```

Essa saída indica um atraso provável no salto 3, como evidenciado por um aumento significativo no RTT entre o salto 2 e o salto 3. A diferença de tempo relativamente pequena entre o salto 3 e o salto 4 sugere que o problema está localizado no segmento entre 20.20.20.20 e 30.30.30.30.

## Causas comuns de latência e quedas de pacotes

### Problemas da camada 1 (camada física)

As questões da camada 1 são uma fonte comum de latência de rede e quedas de pacotes. É importante verificar estes aspectos na camada física:

- Verifique se as configurações de duplex e velocidade estão definidas corretamente em todas as interfaces.
- Verifique se há erros de entrada e CRC nas interfaces, o que pode indicar problemas na camada física.
- Cabos de rede, conexões de fibra, módulos SFP ou portas de switch defeituosos também podem causar atrasos e quedas de pacotes.

<#root>

**Switch#show interface gi1/0/1**

```
GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```

**Full-duplex, 1000Mb/s,**

```
 media type is 10/100/1000BaseTX
  ...
  5 minute input rate 2000 bits/sec, 5 packets/sec
  5 minute output rate 3000 bits/sec, 8 packets/sec
     250000 packets input, 22000000 bytes, 0 no buffer
     Received 300 broadcasts (200 multicasts)
     0 runts, 0 giants, 0 throttles
```

**85 input errors, 85 CRC,**

```
 0 frame, 0 overrun, 0 ignored
```

**<===== Input errors and CRC**

```
     0 watchdog, 0 multicast, 0 pause input
  ...
     260000 packets output, 23000000 bytes, 0 underruns
     5 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
```

**Switch# show interfaces counters errors**

| Port | Align-Err | FCS-Err | Xmit-Err | Rcv-Err | UnderSize | OutDiscards |
|---|---|---|---|---|---|---|
| **Gi1/0/1** | **0** | **0** | **0** | **0** | **0** | **0** |

```
Gi1/0/2     0           0           0         0         0           0
...
```

## Quedas de saída

As quedas de saída ocorrem quando uma fila de transmissão de uma interface de switch está cheia e não pode encaminhar pacotes adicionais. Isso pode levar a um aumento da latência à medida que os pacotes aguardam na fila e também pode resultar em quedas de pacotes se a fila estourar, afetando o desempenho do aplicativo e a confiabilidade da rede.



```
Switch#show interface gi1/0/1


GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
...
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d00h
  Input queue: 0/2000/0/0 (size/max/drops/flushes)

; Total output drops: 4216760900


  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 389946000 bits/sec, 84175 packets/sec
  5 minute output rate 694899000 bits/sec, 106507 packets/sec
     7885666654 packets input, 4677291827948 bytes, 0 no buffer
...
```

O contador de descartes de saída total mostra um grande número de pacotes descartados, indicando congestionamento ou excesso de fila nessa interface. Isso pode aumentar a latência e a perda de pacotes, afetando o desempenho da rede e dos aplicativos.

## Estabilidade de STP

A instabilidade do STP pode contribuir significativamente para a latência da rede e quedas de pacotes. Em uma rede estável, as alterações de topologia devem ser mínimas. Mudanças

frequentes de topologia podem indicar problemas subjacentes e podem interromper as operações normais de encaminhamento.

Principais considerações para minimizar a latência relacionada ao STP:

Alterações de Topologia (TCNs): Mudanças excessivas na topologia do STP podem resultar na descarga frequente do endereço MAC da tabela do switch (CAM), causando aumento no tráfego de broadcast e na latência à medida que os switches inundam pacotes unicast desconhecidos até que a tabela seja preenchida novamente.

Configuração da porta de borda: Verifique se todas as portas de borda estão configuradas com PortFast. A habilitação do PortFast impede que as TCNs (Topology Change Notifications) do STP sejam geradas quando clientes ou servidores se conectam ou desconectam, o que reduz o envelhecimento desnecessário da tabela CAM e melhora a estabilidade.

Planejamento de Bridge Raiz: Planeje e atribua manualmente a bridge raiz e as prioridades do STP para manter uma topologia de rede previsível e minimizar alterações desnecessárias na topologia.

Quando ocorre uma alteração de topologia (como estados de transição de porta), o switch envia um TCN BPDU em direção à bridge raiz. A bridge raiz propaga BPDUs de TCN para todos os switches, solicitando que eles reduzam o tempo de envelhecimento do endereço MAC do padrão (300 segundos) para o valor de retardo de encaminhamento (geralmente 15 segundos). Isso faz com que as entradas ociosas recentemente sejam liberadas, resultando em mais unicasts desconhecidos e maior inundação na rede.

<#root>

**Switch#show spanning-tree detail | include ieee|from|occur|is exec**

VLAN0705 is executing the ieee compatible Spanning Tree protocol

**Number of topology changes 6233**

last change occurred 00:00:03 ago

**<===== Topology Changes**

**from GigabitEthernet1/0/25 <===== From Gi1/0/25**

## Flapping de MAC/Loops de Camada 2

A oscilação de MAC/loops de Camada 2 causam latência de rede e quedas de pacotes, atualizando continuamente a tabela de endereços MAC com o mesmo MAC de origem em portas diferentes. Essa alteração constante interrompe o encaminhamento de tráfego, levando a interrupções e perda de pacotes. Os loops de Camada 2 pioram o problema, fazendo com que os pacotes de broadcast circulem sem parar, disparando mais oscilações de MAC e degradando ainda mais o desempenho da rede. A implementação de protocolos de prevenção de loop, como o STP, é essencial para manter a operação estável da rede e evitar esses problemas.

Para configurar a notificação de movimentação de MAC, use o comando mac address-table notification mac-move no modo de configuração global.

<#root>

**Mac Flapping logs:**

```
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po1 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host b0f1.ec27.69ea in vlan 154 is flapping between port Po9 and port Po
```

## controle de fluxo

Quando o controle de fluxo está ativado e um buffer de recepção de uma porta de switch se aproxima da capacidade, o switch envia quadros de pausa para interromper temporariamente o tráfego de entrada. Esse processo pode aumentar a latência à medida que a transmissão de dados é interrompida intermitentemente. Por outro lado, se o controle de fluxo não estiver habilitado ou os dispositivos upstream não honrarem os quadros de pausa, o tráfego de entrada pode exceder a capacidade do buffer, resultando em saturação do buffer e descartes de pacotes.

O controle de fluxo deve ser configurado com cuidado, considerando os recursos de todos os dispositivos no caminho do tráfego. O uso incorreto ou a configuração incorreta pode levar a um aumento da latência e quedas de pacotes, afetando negativamente o desempenho do aplicativo.

<#root>

**Switch#show interfaces gigabitEthernet 1/0/1**

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
□
input flow-control is on,
 output flow-control is unsupported
<===== Input Flow Control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 6530
5 minute input rate 8000 bits/sec, 8 packets/sec□
5 minute output rate 0 bits/sec, 0 packets/s
0 watchdog, 5014620 multicast,
1989 pause input
<===== Pause Input

0 unknown protocol drops□0 babbles, 0 late collision,
0 deferred□0 lost carrier, 0 no carrier, 0 pause output

Switch#show controllers ethernet-controller gigabitEthernet 1/0/1

Transmit        GigabitEthernet1/0/1     Receive
0 MacUnderrun frames                0 MacOverrun frames
0 Pause frames
1878 Pause frames              <===== Pause frames in RX
```

## Utilização da CPU

A alta utilização da CPU pode levar ao aumento da latência da rede e quedas de pacotes. Quando a CPU está sobrecarregada, o switch não pode processar o tráfego do plano de controle, as atualizações de roteamento ou as funções de gerenciamento de forma eficiente. Isso pode atrasar o encaminhamento de pacotes, causar timeouts para protocolos como ARP ou Spanning Tree e resultar em pacotes descartados, especialmente para o tráfego que requer intervenção da CPU.



```
Switch#show processes cpu sorted

CPU utilization for five seconds:
95%/8%;
 one minute: 92%; five minutes: 90%
```

**<===== CPU utilization 93%**

```
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
```

**439     3560284      554004       6426 54.81% 55.37% 48.39%   0 SISF Main Thread**

**438     2325444      675817       3440 22.67% 28.17% 27.15%   0**

**SISF Switcher Th**

```
 104      548861       84846       6468 10.76%  8.17%  7.51%   0 Crimson flush tr
 119      104155      671081        155  1.21%  1.27%  1.26%   0 IOSXE-RP Punt Se
```

## Utilização de memória

O alto uso de memória pode causar latência e quedas de pacotes sobrecarregando a CPU e os processos do plano de controle. Essa sobrecarga atrasa o tratamento de atualizações de roteamento, políticas de QoS e gerenciamento de buffer, levando a um congestionamento no pipeline de processamento de pacotes. Consequentemente, os pacotes podem ser descartados ou atrasados. Assim, a alta utilização de memória afeta o desempenho da rede, reduzindo a eficiência do switch no gerenciamento do tráfego.

<#root>

**Switch#show platform resources**

```
Resource                  Usage                    Max             Warning         Critical
-------------------------------------------------------------------------------------------
Control Processor       25.00%                     100%            90%             95%
  DRAM
```

**3656MB(94%)**

```
           866MB           90%             95%             W
```

**High memory logs:**

```
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
```

```
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
```

## Redirecionamentos de ICMP e mensagens inalcançáveis

Quando um pacote chega a uma interface de Camada 3 e é roteado para fora da mesma interface, o switch gera uma mensagem de redirecionamento ICMP para informar a origem de um próximo salto mais eficiente na mesma sub-rede. Isso faz com que o pacote original passe pela vLAN duas vezes, aumentando o uso da largura de banda. Além disso, o próprio pacote de redirecionamento ICMP consome largura de banda e exige processamento da CPU, o que pode levar a interrupções da CPU e aumento da latência. Se muitos desses redirecionamentos ocorrerem, especialmente durante o tráfego intenso, a carga da CPU poderá aumentar significativamente, causando potencialmente quedas de pacotes.

A geração e o processamento frequentes de mensagens ICMP inalcançáveis também podem aumentar a utilização da CPU, afetando o desempenho da rede. Grandes volumes de tráfego inalcançável ICMP consomem recursos da CPU, o que pode levar à latência e quedas de pacotes.

Para atenuar esses efeitos, a Cisco recomenda desativar as mensagens ICMP inalcançáveis e os redirecionamentos ICMP nas interfaces de Switch Virtual (SVIs) e Camada 3 usando os comandos no ip unreachables e no ip redirects . Essa prática recomendada reduz a carga da CPU e melhora a estabilidade da rede.

<#root>

**Switch#show ip traffic | in unreachable**

```
...
  Rcvd: 194943 format errors, 369707 checksum errors,
```

**3130 redirects,**

**734412 unreachable**

```
  Sent: 29265 redirects, 14015958 unreachable, 196823 echo, 786959149 echo reply
...
```

**Switch#show platform hardware fed 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     3296567      2336
3    0      ICMP GEN                    Yes     750       750      0            0
4    2      Routing Control             Yes     5500      5500     1085196      12919
5    14     Forus Address resolution    Yes     4000      4000     51723336     760639


6    0      ICMP Redirect               Yes     750       750      8444220485535  6978564145


...
```

## Tempestades de tráfego

Uma tempestade de tráfego ocorre quando pacotes excessivos de broadcast, multicast ou unicast inundam uma LAN, sobrecarregando os recursos do switch e degradando o desempenho da rede.

O controle de storm nos switches monitora o tráfego de broadcast, multicast e unicast nas interfaces físicas e o compara aos limites configurados. Quando o tráfego excede esses limites, o switch bloqueia temporariamente o tráfego excessivo para evitar a degradação da rede. Isso protege os recursos do switch e mantém a estabilidade e o desempenho gerais da rede.

<#root>

**Switch#show interfaces counters**

```
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts

Gi1/0/1        125487955     550123004     250123555     105234788


Gi1/0/2           500123        100123          5123          1024
Gi1/0/3           250123         50123          1024           512
```

**Switch#show platform hardware fed switch active qos queue stats internal cpu policer**

CPU Queue Statistics

| QId | PlcIdx | Queue Name | Enabled | (default) Rate | (set) Rate | Queue Drop(Bytes) | Queue Drop(Frames) |
|---|---|---|---|---|---|---|---|
| 11 | 13 | L2 LVX Data Pack | Yes | 1000 | 1000 | 0 | 0 |
| **12** | **0** | **BROADCAST** | **Yes** | **750** | **750** | **32529067** | **186363** |
| 13 | 10 | Openflow | Yes | 250 | 250 | 0 | 0 |
| **14** | **13** | **Sw forwarding** | **Yes** | **1000** | **1000** | **48317658492** | **245507344** |
| 15 | 8 | Topology Control | Yes | 13000 | 16000 | 0 | 0 |

## Tempo de envelhecimento CAM vs ARP

O tempo de envelhecimento da CAM (Tabela de Endereços MAC) versus o tempo de envelhecimento do Protocolo de Resolução de Endereços (ARP) também pode causar latência de rede e quedas de pacotes. Isso acontece porque a tabela CAM, que armazena o endereço MAC para os mapeamentos de porta, geralmente expira as entradas mais rapidamente (padrão em torno de cinco minutos) do que a tabela ARP, que armazena os mapeamentos de endereço IP para MAC (padrão em torno de quatro horas). Quando um endereço MAC expira fora da tabela CAM, mas ainda existe na tabela ARP, o switch não conhece mais a porta específica para encaminhar o tráfego unicast para esse endereço MAC. Como resultado, o switch inunda o tráfego unicast para todas as portas na VLAN, causando congestionamento na rede e possível perda de pacotes.

## Como o tempo de envelhecimento CAM versus ARP causa latência e quedas de pacotes

- Quando a entrada da tabela CAM expira antes da entrada ARP, o switch inunda pacotes unicast porque não possui o mapeamento de MAC para porta.
- Essa inundação aumenta a carga da CPU e consome a largura de banda desnecessariamente, levando à latência da rede e quedas de pacotes.
- A incompatibilidade também pode causar encaminhamento ineficiente e maior processamento do plano de controle.

**Switch#show mac address-table aging-time**

Global Aging Time:

**300 <===== MAC aging**

Vlan Aging Time
---- ----------

**Switch#show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.95.1

**124**

Incomplete ARPA

**<===== Arp age**

...

**Switch#show interface vlan1**

Vlan1 is up, line protocol is up , Autostate Enabled
Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
ARP type: ARPA,

**ARP Timeout 04:00:00**

Last input never, output never, output hang never

**Configuring MAC Aging and ARP Timeout:**

Switch#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.

**Switch(config)#mac-address-table aging-time ?**

```
  <0-0>         Enter 0 to disable aging
  <10-1000000>  Aging time in seconds
```

**Switch(config)#mac-address-table aging-time 14400 ?**

```
  routed-mac  Set RM Aging interval
  vlan        VLAN Keyword
```

**Switch(config)#interface vlan 1**

```
Switch(config-if)#arp timeout 300

Switch(config-if)#do show interface vlan 1

Vlan1 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA,
```

**ARP Timeout 00:05:00**

```
  Last input never, output never, output hang never
```

## sessão de monitor

Quando as sessões de monitor ativo (SPAN) são configuradas em um switch com várias portas de origem e destino, elas podem contribuir para a latência da rede e quedas de pacotes.

<#root>

**Example:**

**Session 1**

---

Type : Local Session

**Source Ports :**

**Both : Po101,Po105,Po109,Po125,Po161,Po170 <===== Multiple source ports**

**Destination Ports : Te9/8**

Egress SPAN Replication State:
Operational mode : Centralized
Configured mode : Centralized (default)

**Session 2**

---

Type : Local Session

**Source Ports :**

**Both : Po161,Po170**

**Destination Ports : Te9/1**

Egress SPAN Replication State:
Operational mode : Centralized

```
Configured mode        : Centralized (default)
```

Como funciona o SPAN

O SPAN (Switched Port Analyzer) é um recurso assistido por hardware que espelha o tráfego das portas de origem para as portas de destino sem envolver pesquisas de CPU. O ASIC de replicação no módulo supervisor lida com o espelhamento de pacotes, enquanto o mecanismo de encaminhamento redireciona os pacotes espelhados para as portas de destino. Os pacotes espelhados são comutados com a mesma temporização do tráfego regular.

Impacto de várias portas de origem e destino:

No exemplo anterior, o switch deve replicar o tráfego de todas as interfaces de origem para as interfaces de destino. Por exemplo, o tráfego da interface Po170 é espelhado e encaminhado duas vezes para dois destinos diferentes. Essa replicação aumenta a carga no mecanismo de encaminhamento e pode causar congestionamento no painel traseiro do switch.

- Se um canal de porta transportar três GBPS de tráfego, a replicação desse tráfego para vários destinos pode resultar em mais de 15 GBPS de tráfego espelhado.
- A carga no ASIC de replicação aumenta proporcionalmente à taxa de tráfego nas interfaces de origem.
- Com taxas de tráfego mais baixas, o impacto da latência pode ser mínimo, mas à medida que o tráfego aumenta, a latência e o congestionamento podem se tornar significativos.

## Exceções de nível ASIC

Use esse comando para verificar a interface para mapeamentos ASIC, que mostra a instância ASIC onde a interface reside.

<#root>

```
Switch#show platform software fed switch active ifm mappings

Interface                IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type Active

GigabitEthernet2/0/12    0x13

 1     0    1

     11     0      20    17   12   108  NIF   Y
```

```
<===== ASIC Instance 1 (Asic 0/Core 1)
```

Depois que a instância ASIC for identificada, execute o próximo comando para exibir as exceções de queda de ASIC de encaminhamento para esse ASIC.

<#root>

```
Switch#show platform hardware fed switch active fwd-asic drops exceptions asic
```

Example output snippet for ASIC instance 1:

```
****EXCEPTION STATS ASIC INSTANCE 1 (asic/core 0/1)****
==========================================================================================
 Asic/core |                NAME                    |   prev       |  current  |  delta

==========================================================================================
0       1  NO_EXCEPTION                             2027072618   2028843223    1770605
0       1  ROUTED_AND_IP_OPTIONS_EXCEPTION          735          735           0
0       1  PKT_DROP_COUNT                           14556203    14556203        0
0       1  BLOCK_FORWARD                           14556171    14556171        0
0       1  IGR_EXCEPTION_L5_ERROR                   1            1             0
...
```

## Bugs de software

Às vezes, bugs de software podem causar comportamentos não intencionais e inesperados. Esses bugs podem resultar em problemas como latência de rede, quedas de pacotes ou outras degradações de desempenho. Para resolver esses problemas, um primeiro passo comum é recarregar o switch, que pode eliminar falhas transitórias e restaurar a operação normal. Além disso, é essencial manter seus dispositivos atualizados aplicando regularmente as atualizações de firmware e software mais recentes. Essas atualizações frequentemente incluem correções para bugs conhecidos e melhorias que melhoram a estabilidade e o desempenho do dispositivo, ajudando a evitar problemas relacionados a defeitos de software.

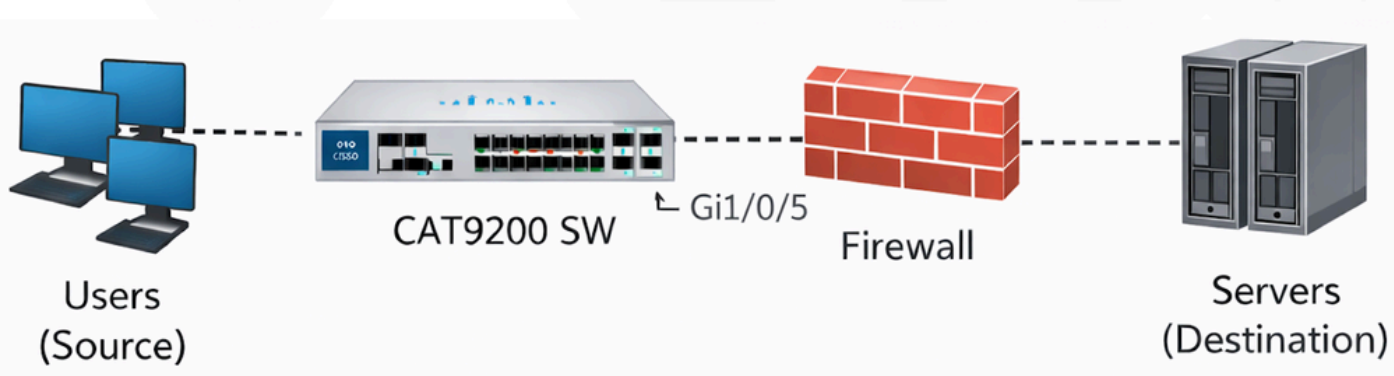
Ferramenta Cisco Bug Search

# Casos Práticos

## Detalhes do problema

Os usuários estão experimentando perda intermitente de conectividade de rede durante tentativas para transferir grandes volumes de dados através de vLANs, como durante transferências de arquivos de alta capacidade. Essas interrupções se manifestam como falhas esporádicas na transmissão de dados, apesar de várias tentativas bem-sucedidas, afetando significativamente a confiabilidade da rede e o desempenho do aplicativo. O problema é temporariamente resolvido ao recarregar o switch.

Topologia




Sintomas observados

- As transferências de arquivos entre a origem e o destino falham intermitentemente após várias tentativas bem-sucedidas.
- O switch perde a conectividade com o firewall durante os períodos de falha.
- A autenticação 802.1X permanece operacional durante os incidentes.
- O switch permanece responsivo através do console durante os incidentes.
- A porta conectada do firewall exibe apenas o tráfego de broadcast durante os períodos de falha.
- Os testes de diagnóstico (DiagGoldPktTest) falham regularmente na interface Gi1/0/5, indicando um problema no caminho dos dados.

Troubleshooting Executado

- Os contadores de interface e as estatísticas de buffer no nível da plataforma são revisados.
- A interface Gi1/0/5 do switch mostra um volume muito alto de quadros de pausa 802.3x recebidos do firewall.
- Os descartes de saída e as estatísticas de quadros de pausa são monitorados de perto.
- As estatísticas de fila do mecanismo de encaminhamento de software da plataforma são

examinadas para identificar o comportamento do buffer.
- As configurações de controle de fluxo na interface do switch são verificadas.

Estatísticas de interface relevantes

<#root>

**Switch#show interfaces GigabitEthernet 1/0/5**

GigabitEthernet1/0/5 is up, line protocol is up (connected)
□

**input flow-control is on,**

output flow-control is unsupported

**<===== Input Flow-control is ON**

Input queue: 0/2000/0/0 (size/max/drops/flushes);

**Total output drops: 78444**

5 minute input rate 8000 bits/sec, 8 packets/sec□

**5 minute output rate 0 bits/sec, 0 packets/s <===== Output rate**

0 watchdog, 5014620 multicast,

**1989 pause input**

0 unknown protocol drops□0 babbles, 0 late collision,
...

**Switch#show controllers ethernet-controller GigabitEthernet 1/0/5**

Transmit GigabitEthernet1/0/5. Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

**1878 Pause frames**

**<===== Pause Frames In RX**

...

**Switch#diagnostic start switch 1 test DiagGoldPktTest port 5**

**Switch#show diagnostic result switch 1 test DiagGoldPktTest detail**

□Test results: (. = Pass, F = Fail, U = Untested)
_____
1) DiagGoldPktTest:
 Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24□
      U U U U

**F**

 U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U.

**<===== DiagGoldPktTest Failed For Port 5**

Port 25 26 27 28□----------------□U U U U

Switch#show flowcontrol interface GigabitEthernet 1/0/

| Port | Send FlowControl admin | Send FlowControl oper | Receive FlowControl admin | Receive FlowControl Oper | RxPause | TxPause |
|---|---|---|---|---|---|---|
| Gi1/0/5 | Unsupp. | Unsupp. | on | on. | | |

**13256**

0

**<===== Pause Frames In RX**

**Switch#show platform hardware fed switch active qos queue stats interface GigabitEthernet 1/0/5**

Asic:0 Core:0 DATA Port:8 Hardware Drop Counters□

```
-------------------------------------------------------------
Q   Drop-TH0      Drop-TH1      Drop-TH2      SBufDrop          QebDrop
□    (Bytes)        (Bytes)       (Bytes)       (Bytes)             (Bytes)□
-------------------------------------------------------------
0     0               0
```

**18106020**

```
           0               0
```

Causa raiz identificada

A causa raiz foi identificada como bloqueio de buffer devido ao excesso de quadros de pausa 802.3x enviados pelo Firewall para a interface do switch. Os quadros de pausa Ethernet instruem o switch a parar a transmissão para permitir que o dispositivo receptor se recupere do congestionamento. No entanto, quando os quadros de pausa são enviados repetidamente ou por durações estendidas:

- A fila de saída do buffer do switch para a interface fica totalmente saturada.
- O switch continua a aceitar pacotes de entrada destinados à interface pausada, que se acumulam na fila de saída.
- A saturação da fila leva a quedas de saída e blackholing de tráfego.
- Nesse caso, os buffers ficaram bloqueados e o encaminhamento não foi retomado mesmo depois que a taxa de quadros de pausa diminuiu.
- Uma recarga do switch foi necessária para limpar o estado de buffer bloqueado.

Esse comportamento é documentado no bug Cisco CSCwm14612, que descreve como os quadros de pausa sobrecarregados fazem com que a interface armazene incorretamente os buffers, resultando em quedas de saída.

## Resolução

O controle de fluxo de entrada foi desabilitado na interface do switch afetado usando o comando:

<#root>

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 1/0/5
Switch(config-if)#
```

**flowcontrol receive off**

### Conclusão

As falhas intermitentes de conectividade de rede e quedas de pacotes entre o switch Cisco C9200L e o Firewall foram causadas por um travamento de fila de software disparado por um volume excessivo de quadros de pausa 802.3x. Desativar o controle de fluxo de entrada na interface do switch resolveu o problema, evitando que a fila ficasse saturada e bloqueada.

## Informações Relacionadas

- Solucionar problemas de descartes de saída nos switches Catalyst 9000
- Solucionar problemas de STP em switches Catalyst
- Identificar e Solucionar Problemas de Flaps/Loop MAC em Switches Cisco Catalyst
- Suporte técnico e downloads da Cisco

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.