Catalyst 9000 스위치의 네트워크 레이턴시 및 패킷 삭제 문제 해결

목차

소개

이 문서에서는 Cisco Catalyst 9000 Series 스위치의 네트워크 지연 및 패킷 손실 문제를 해결하기 위한 자세한 방법론에 대해 설명합니다.

사전 요구 사항

요구 사항

TCP/IP, VLAN 및 STP(Spanning Tree Protocol)를 비롯한 네트워킹 개념을 기본적으로 이해하는 것이 좋습니다. Cisco Catalyst 9000 Series 스위치 및 Cisco IOS® XE CLI에 대한 지식은 필수적입니다. 네트워크 모니터링 툴과 구성 및 진단을 위한 액세스 권한에 대해서도 숙지해야 합니다.

사용되는 구성 요소

이 문서의 정보는 모든 버전의 Cisco Catalyst 9000 스위치를 기반으로 합니다. 이 문서는 특정 소프트웨어 또는 하드웨어 버전으로 제한되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서는 네트워크 관리자 및 엔지니어를 위해 작성되었으며 엔터프라이즈 네트워크 환경 내에서 이러한 문제를 효율적으로 식별, 격리 및 해결하기 위한 지침을 제공합니다. 네트워크 지연 및 패킷 삭제는 엔터프라이즈 환경의 성능과 신뢰성에 악영향을 미칠 수 있습니다. 이러한 문제는 네트워크 혼잡, 잘못된 컨피그레이션 또는 환경 요인으로 인해 발생하는 경우가 많습니다. Cisco Catalyst 9000 Series 스위치는 높은 성능과 복원력을 제공하도록 설계되었습니다. 이 문서에서는 네트워크 전문가들이 이러한 스위치를 사용하여 지연 시간 및 패킷 삭제 문제를 식별하고 해결할 수 있도록 지원하는 주요 문제 해결 단계를 제공합니다.

네트워크 레이턴시 및 패킷 삭제 이해

네트워크 레이턴시

네트워크 레이턴시는 데이터가 소스에서 대상으로 네트워크를 이동할 때 발생하는 지연을 측정하는 것입니다. 가장 일반적으로 레이턴시는 RTT(Round Trip Time)로 표현됩니다. RTT는 패킷이 출발지에서 목적지로, 그리고 목적지로 이동하는 데 걸리는 시간입니다.

레이턴시는 일반적으로 밀리초(ms)로 측정됩니다.

영향: 레이턴시가 높으면 애플리케이션 성능이 저하될 수 있습니다. 특히 TCP와 같은 프로토콜의

경우 데이터를 효율적으로 보내기 위해 적시에 승인을 받아야 합니다.

패킷 삭제

패킷 삭제는 네트워크 디바이스가 패킷을 원하는 목적지로 전달할 수 없는 경우(대개 정체, 버퍼 오버플로, 잘못된 컨피그레이션 또는 하드웨어 오류) 발생합니다. 패킷 삭제는 일반적으로 특정 간격 동안 손실된 패킷의 백분율로 측정됩니다.

영향: 패킷 삭제로 인해 처리량이 감소하고 재전송이 발생하며 애플리케이션 신뢰성이 저하될 수 있습니다.

예상 레이턴시 벤치마크

네트워크 유형	일반적인 RTT
동일한 VLAN(액세스 레이어)	1ms 미만
캠퍼스 코어 접근	1~5ms
메트로 WAN	5~30ms
인터넷/WAN	30~150밀리초

참고: 네트워크 홉 간의 지리적 거리는 RTT를 증가시키고 더 높은 레이턴시를 가져올 수 있습니다.

네트워크 레이턴시 측정

먼저 네트워크와 해당 토폴로지를 철저히 파악합니다. 결정론적 변수와 예측 불가능을 최소화하여 네트워크를 설계하면 지연 및 패킷 삭제 문제를 식별하고 해결하는 프로세스가 훨씬 더 간단해집니다.

네트워크 레이턴시를 측정하기 위해 일반적으로 두 가지 기본 툴이 사용됩니다.

핑

대상이 패킷 손실 및 RTT에 대한 통계와 함께 도달할 수 있는지 여부를 출력으로 반환합니다. 문제가 있는 홉을 식별한 후 바로 해당 홉 간에 ping을 시도하고 디바이스를 체크인하여 문제를 찾을 수 있습니다.

<#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

트레이스라우트

Traceroute는 각 홉에 대한 RTT 결과와 함께 소스에서 대상으로의 라우팅 경로의 모든 홉을 표시합니다. 예를 들어, traceroute는 네트워크에서 지연이 있거나 시작되는 위치를 표시할 수 있습니다. 이러한 예가 다음 traceroute 출력에 표시됩니다.

<#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.
```

이 출력은 hop 2와 hop 3 사이의 RTT가 크게 증가했음을 보여주는 것처럼 hop 3에서의 가능한 지연을 나타냅니다. hop 3과 hop 4 사이의 비교적 작은 시간 차이는 문제가 20.20.20.20과 30.30.30.30 사이의 세그먼트로 현지화되었음을 나타냅니다.

레이턴시 및 패킷 삭제의 일반적인 원인

레이어 1(물리적 레이어) 문제

레이어 1 문제는 네트워크 레이턴시 및 패킷 삭제의 일반적인 소스입니다. 물리적 레이어에서 이러한 측면을 검증하는 것이 중요합니다.

- 듀플렉스 및 속도 설정이 모든 인터페이스에 올바르게 구성되었는지 확인합니다.
- 인터페이스에서 물리적 레이어 문제를 나타낼 수 있는 CRC, 입력 오류를 확인합니다.
- 네트워크 케이블, 파이버 연결, SFP 모듈 또는 스위치 포트에 장애가 발생할 경우 패킷 지연 및 삭제도 발생할 수 있습니다.


```
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
...
```

출력 삭제

스위치 인터페이스의 전송 큐가 꽉 차서 추가 패킷을 전달할 수 없을 때 출력이 삭제됩니다. 이로 인해 패킷이 대기열에서 대기할 때 레이턴시가 증가할 수 있으며, 대기열이 오버플로우될 경우 패킷이 삭제되어 애플리케이션 성능과 네트워크 신뢰성에 영향을 미칠 수 있습니다.


```
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
...
```

Total output drops 카운터는 많은 수의 삭제된 패킷을 보여주는데, 이는 이 인터페이스의 혼잡 또는 큐 오버플로를 나타냅니다. 이로 인해 레이턴시가 증가하고 패킷이 손실되어 네트워크 및 애플리케이션 성능에 영향을 미칠 수 있습니다.

STP 안정성

STP가 불안정하면 네트워크 지연 및 패킷 삭제에 크게 기여할 수 있습니다. 안정적인 네트워크에서는 토폴로지 변경이 최소화되어야 합니다. 토폴로지 변경이 빈번하면 기본 문제를 나타낼 수 있으며 정상적인 포워딩 작업이 중단될 수 있습니다.

STP 관련 레이턴시를 최소화하기 위한 주요 고려 사항:

토폴로지 변경(TCN): 과도한 STP 토폴로지 변경으로 인해 CAM(Switch) 테이블의 MAC 주소가 자주 플러시될 수 있으며, 테이블이 다시 채워질 때까지 스위치가 알 수 없는 유니캐스트 패킷을 플러딩하므로 브로드캐스트 트래픽과 레이턴시가 증가할 수 있습니다.

에지 포트 구성: 모든 에지 포트가 PortFast로 구성되었는지 확인합니다. PortFast를 활성화하면 클라이언트나 서버가 연결되거나 연결이 끊어질 때 STP TCN(Topology Change Notifications)이 생성되지 않으므로 불필요한 CAM 테이블 에이징이 줄어들고 안정성이 향상됩니다.

루트 브리지 계획: 예측 가능한 네트워크 토폴로지를 유지하고 불필요한 토폴로지 변경을 최소화하기 위해 STP 루트 브리지 및 우선 순위를 수동으로 계획하고 할당합니다.

토폴로지 변경(예: 포트 전환 상태)이 발생하면 스위치는 루트 브리지로 TCN BPDU를 전송합니다. 그런 다음 루트 브리지는 TCN BPDU를 모든 스위치에 전파하여 MAC 주소 에이징 시간을 기본값(300초)에서 전달 지연 값(일반적으로 15초)으로 단축하라는 메시지를 표시합니다. 이로 인해 최근에 유휴 상태인 엔트리가 플러시되어 알 수 없는 유니캐스트가 증가하고 네트워크 전체에서 플러딩이 증가합니다.

<#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

MAC 플래핑/레이어 2 루프

MAC 플래핑/레이어 2 루프는 서로 다른 포트에서 동일한 소스 MAC으로 MAC 주소 테이블을 지속적으로 업데이트하여 네트워크 지연 및 패킷 삭제를 유발합니다. 이러한 지속적인 변화로 인해 트래픽 포워딩이 중단되고 패킷 손실이 발생합니다. 레이어 2 루프는 끊임없이 순환하기 위해 브로드캐스트 패킷을 유발하여 문제를 악화시키고, MAC 플래핑을 더 발생시키며, 네트워크 성능을 더욱 떨어뜨립니다. 안정적인 네트워크 운영을 유지하고 이러한 문제를 방지하려면 STP와 같은 루프 방지 프로토콜을 구현하는 것이 필수적입니다.

MAC 이동 알림을 구성하려면 글로벌 컨피그레이션 모드에서 mac address-table notification mac-move 명령을 사용합니다.

<#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
```

Flow Control

플로우 제어가 활성화되고 스위치 포트의 수신 버퍼가 용량에 가까워지면 스위치는 일시 중지 프레임을 전송하여 수신 트래픽을 일시적으로 중지합니다. 이 프로세스는 데이터 전송이 간헐적으로 일시 중지되므로 레이턴시를 늘릴 수 있습니다. 반대로, 흐름 제어가 활성화되지 않거나 업스트림 디바이스가 일시 중지 프레임을 수신하지 않는 경우, 수신 트래픽이 버퍼 용량을 초과하여 버퍼 오버런 및 패킷 삭제를 초래할 수 있습니다.

트래픽 경로에 있는 모든 디바이스의 기능을 고려하여 흐름 제어를 신중하게 구성해야 합니다. 잘못 사용하거나 잘못 구성하면 레이턴시가 증가하고 패킷이 삭제되어 애플리케이션 성능이 저하될 수 있습니다.

<#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

CPU 사용률

CPU 사용률이 높으면 네트워크 레이턴시가 증가하고 패킷이 드롭될 수 있습니다. CPU가 과부하 상태인 경우 스위치에서 컨트롤 플레인 트래픽, 라우팅 업데이트 또는 관리 기능을 효율적으로 처리할 수 없습니다. 이로 인해 패킷 전달이 지연되고, ARP 또는 스패닝 트리와 같은 프로토콜이 시간 초과될 수 있으며, 특히 CPU 개입이 필요한 트래픽의 경우 패킷이 삭제될 수 있습니다.

<#root>

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

메모리 사용률

메모리 사용량이 많으면 CPU 및 컨트롤 플레인 프로세스를 오버로드하여 지연 및 패킷 삭제를 일으킬 수 있습니다. 이 오버로드는 라우팅 업데이트, QoS 정책 및 버퍼 관리의 처리를 지연시켜 패킷 처리 파이프라인의 혼잡으로 이어집니다. 따라서 패킷이 삭제되거나 지연될 수 있습니다. 따라서 메모리 사용률이 높으면 스위치의 트래픽 관리 효율성을 줄여 네트워크 성능에 영향을 미칩니다.

<#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
```

ICMP 리디렉션 및 연결할 수 없는 메시지

패킷이 레이어 3 인터페이스에 도착하고 동일한 인터페이스에서 라우팅되면 스위치에서 ICMP 리디렉션 메시지를 생성하여 동일한 서브넷에서 더 효율적인 다음 홉을 소스에 알립니다. 그러면 원래 패킷이 vLAN을 두 번 통과하므로 대역폭 사용량이 증가합니다. 또한 ICMP 리디렉션 패킷 자체는 대역폭을 소모하며 CPU 처리가 필요합니다. 그러면 CPU 인터럽트가 발생하고 레이턴시가 늘어날 수 있습니다. 특히 트래픽이 많은 동안 이러한 리디렉션이 많이 발생하는 경우 CPU 로드가 크게 증가하여 패킷 삭제를 유발할 수 있습니다.

ICMP 도달 불가 메시지를 자주 생성하고 처리하면 CPU 사용률도 증가하여 네트워크 성능에 영향을 줄 수 있습니다. 대량의 ICMP 도달 불가 트래픽은 CPU 리소스를 소비하며, 이는 지연 및 패킷 삭제로 이어질 수 있습니다.

이러한 영향을 완화하기 위해 Cisco에서는 no ip unreachable 및 no ip redirects 명령을 사용하여 SVI(Switch Virtual Interface) 및 레이어 3 인터페이스에서 ICMP 연결 불가 메시지와 ICMP 리디렉션을 비활성화할 것을 권장합니다. 이 모범 사례는 CPU 로드를 줄이고 네트워크 안정성을 향상시킵니다.

<#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

...
```

교통 폭풍

과도한 브로드캐스트, 멀티캐스트 또는 유니캐스트 패킷이 LAN을 플러딩하여 스위치 리소스를 과도하게 사용하고 네트워크 성능을 저하시킬 때 트래픽 스톰이 발생합니다.

스위치의 스톰 제어는 물리적 인터페이스의 브로드캐스트, 멀티캐스트 및 유니캐스트 트래픽을 모니터링하고 구성된 임계값과 비교합니다. 트래픽이 이러한 제한을 초과하면 네트워크 성능 저하를 방지하기 위해 스위치에서 과도한 트래픽을 일시적으로 차단합니다. 따라서 스위치 리소스가 보호되고 전반적인 네트워크 안정성과 성능이 유지됩니다.

<#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
============================================================================================
                                                (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                  Enabled   Rate     Rate      Drop(Bytes)  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
```

CAM 대 ARP 에이징 시간

CAM(MAC Address Table) 에이징 시간과 ARP(Address Resolution Protocol) 에이징 시간은 네트워크 지연 및 패킷 삭제를 일으킬 수도 있습니다. 이는 MAC 주소와 포트 간 매핑을 저장하는 CAM 테이블이 IP와 MAC 주소 간 매핑을 저장하는 ARP 테이블보다(기본값은 약 5분) 더 빠르게 항목을 에이징하기 때문입니다(기본값은 4시간). MAC 주소가 CAM 테이블에서 벗어나 오래되었지만 ARP 테이블에 계속 존재하는 경우, 스위치는 해당 MAC 주소에 대한 유니캐스트 트래픽을 전달할 특정 포트를 더 이상 알지 못합니다. 그 결과, 스위치는 유니캐스트 트래픽을 VLAN의 모든 포트에 플러딩하여 네트워크 정체와 잠재적인 패킷 손실을 초래합니다.

CAM 대 ARP 에이징 타임으로 인한 지연 및 패킷 삭제

- ARP 엔트리보다 먼저 CAM 테이블 엔트리가 에이징되면 스위치에서 유니캐스트 패킷을 플러딩합니다. MAC-포트 매핑이 없기 때문입니다.
- 이러한 플러딩은 CPU 로드를 늘리고 대역폭을 불필요하게 소비하여 네트워크 지연 및 패킷 삭제를 초래합니다.
- 불일치는 또한 비효율적인 포워딩 및 증가된 제어 평면 프로세싱의 원인이 될 수 있다.

<#root>

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
```

모니터링 세션

SPAN(Active Monitor) 세션이 여러 소스 및 대상 포트가 있는 스위치에 구성된 경우 네트워크 지연 및 패킷 삭제에 기여할 수 있습니다.

```
<#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)
```

SPAN 작동 방식

SPAN(Switched Port Analyzer)은 CPU 조회를 거치지 않고 소스 포트에서 대상 포트로 트래픽을 미러링하는 하드웨어 지원 기능입니다. 수퍼바이저 모듈의 복제 ASIC는 패킷 미러링을 처리하는 반면, 포워딩 엔진은 미러링된 패킷을 대상 포트로 리디렉션합니다. 미러링된 패킷은 일반 트래픽과 동일한 타이밍으로 스위칭됩니다.

여러 소스 및 대상 포트의 영향:

이전 예에서 스위치는 모든 소스 인터페이스에서 대상 인터페이스로 트래픽을 복제해야 합니다. 예를 들어, 인터페이스 Po170의 트래픽은 미러링되고 두 개의 서로 다른 대상으로 두 번 전달됩니다. 이러한 복제는 포워딩 엔진의 부하를 증가시켜 스위치 백플레인에 혼잡이 발생할 수 있습니다.

- 포트 채널이 3GBPS의 트래픽을 전송하는 경우 이 트래픽을 여러 대상에 복제하면 15GBPS 이상의 미러링 트래픽이 발생할 수 있습니다.
- 복제 ASIC의 로드는 소스 인터페이스의 트래픽 속도에 비례하여 증가합니다.
- 더 낮은 트래픽 속도에서 레이턴시에 미치는 영향은 최소화될 수 있지만, 트래픽이 증가함에 따라 레이턴시와 혼잡이 크게 발생할 수 있습니다.

ASIC 레벨 예외

인터페이스가 상주하는 ASIC 인스턴스를 보여주는 ASIC 매핑에 대한 인터페이스를 확인하려면 이 명령을 사용합니다.

<#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)
```

ASIC 인스턴스가 식별되면 다음 명령을 실행하여 해당 ASIC에 대한 포워딩 ASIC 삭제 예외를 확인합니다.

<#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
...
```

소프트웨어 버그

소프트웨어 버그는 때때로 직접적 또는 간접적으로 의도하지 않은 행동을 유발할 수 있습니다. 이러한 버그로 인해 네트워크 지연, 패킷 삭제 또는 기타 성능 저하와 같은 문제가 발생할 수 있습니다. 이러한 문제를 해결하기 위해 일반적인 첫 번째 단계는 스위치를 다시 로드하는 것이며, 이 경우 일시적인 결함이 제거되고 정상적인 작업이 복원될 수 있습니다. 또한 최신 펌웨어 및 소프트웨어 업데이트를 정기적으로 적용하여 장치를 최신 상태로 유지하는 것이 중요합니다. 이러한 업데이트에는 종종 알려진 버그에 대한 수정 사항과 장치 안정성 및 성능을 개선하여 소프트웨어 결함과 관련된 문제를 방지하는 데 도움이 되는 개선 사항이 포함되어 있습니다.

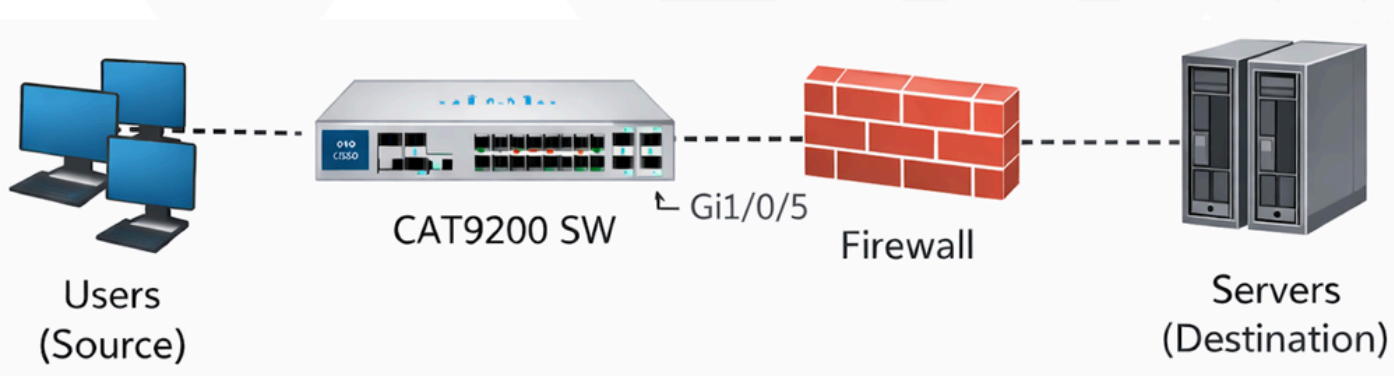
Cisco 버그 검색 툴

사례 연구

문제 세부 정보

대용량 파일 전송과 같이 vLAN을 통해 대량의 데이터를 전송하기 위해 시도하는 동안 사용자의 네트워크 연결이 일시적으로 끊어지는 현상이 나타나고 있습니다. 이러한 중단은 여러 번의 성공적인 시도에도 불구하고 데이터 전송에 산발적인 실패로 나타나며, 네트워크 신뢰성과 애플리케이션 성능에 큰 영향을 미칩니다. 스위치를 다시 로드하면 문제가 일시적으로 해결됩니다.

토폴로지



관찰된 증상

- 몇 번의 시도가 성공한 후 소스와 대상 간의 파일 전송이 간헐적으로 실패합니다.
- 이 스위치는 장애 기간 동안 방화벽과의 연결이 끊어집니다.
- 802.1X 인증은 인시던트 전반에 걸쳐 계속 작동합니다.
- 사고 발생 중에도 스위치는 콘솔을 통해 응답 상태를 유지합니다.
- 방화벽의 연결된 포트는 장애 기간 동안 브로드캐스트 트래픽만 표시합니다.
- Gi1/0/5 인터페이스에서 진단 테스트(DiagGoldPktTest)가 지속적으로 실패하여 데이터 경로 문제가 있음을 나타냅니다.

수행된 트러블슈팅

- 인터페이스 카운터 및 플랫폼 레벨 버퍼 통계를 검토합니다.
- 스위치 인터페이스 Gi1/0/5는 방화벽에서 받은 802.3x 일시 중지 프레임의 매우 큰 볼륨을 보여줍니다.
- 출력 삭제 및 일시 중지 프레임 통계는 자세히 모니터링됩니다.
- 버퍼 동작을 식별하기 위해 플랫폼 소프트웨어 포워딩 엔진 대기열 통계를 검사합니다.
- 스위치 인터페이스의 흐름 제어 설정을 확인합니다.

관련 인터페이스 통계

<#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 Receive FlowControl RxPause TxPause
admin oper admin Oper
---------- -------- -------- -------- -------- ------- -------
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
```

근본 원인 파악

방화벽에서 스위치 인터페이스로 보낸 802.3x 일시 중지 프레임이 너무 많아 근본 원인이 버퍼 잠금으로 식별되었습니다. 이더넷 일시 중지 프레임은 수신 장치가 혼잡으로부터 복구될 수 있도록 스위치에 전송을 중지하도록 지시합니다. 그러나 일시 중지 프레임이 반복해서 전송되거나 기간이 연장된 경우:

- 인터페이스에 대한 스위치 버퍼의 출력 대기열이 완전히 포화됩니다.
- 스위치는 일시 중지된 인터페이스로 향하는 수신 패킷을 계속해서 수락하며, 이는 출력 대기열에 누적됩니다.
- 대기열 채도는 출력 삭제 및 트래픽 블랙홀링으로 이어집니다.
- 이 경우 버퍼가 잠기고 일시 중지 프레임 속도가 감소한 후에도 전달이 재개되지 않았습니다.
- 잠긴 버퍼 상태를 지우려면 스위치를 다시 로드해야 합니다.

이러한 동작은 Cisco 버그 CSCwm14612에 설명되어 있으며, 이 버그는 과도한 일시 중지 프레임으로 인해 인터페이스에서 버퍼를 잘못 보류하여 출력이 삭제되는 방식을 설명합니다.

해결

다음 명령을 사용하여 영향을 받는 스위치 인터페이스에서 입력 흐름 제어가 비활성화되었습니다.

<#root>

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

flowcontrol receive off

결론

Cisco C9200L 스위치와 방화벽 간의 간헐적인 네트워크 연결 실패 및 패킷 삭제는 802.3x 일시 중지 프레임의 과도한 볼륨으로 트리거된 소프트웨어 큐 잠금으로 인해 발생했습니다. 스위치 인터페이스에서 입력 흐름 제어를 비활성화하면 큐가 포화 상태가 되어 잠기는 것을 방지하여 문제가 해결되었습니다.

관련 정보

- Catalyst 9000 스위치의 출력 삭제 문제 해결
- Catalyst 스위치의 STP 문제 해결
- Cisco Catalyst 스위치에서 MAC Flaps/Loop 문제 해결
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.