Null0 및 MSS 클램핑 문제 해결

목차

소개

이 문서에서는 Catalyst 9K에서 MSS(Maximum Segment Size) 조정 및 Null 0을 가리키는 고정 경로가 갖는 의미를 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- TCP 및 MSS 조정에 대한 개념적 지식
- 컨트롤 플레인 포워딩 및 디버그를 위한 Cisco Catalyst 9K 플랫폼 이해

지원되는 플랫폼

이 문서는 Cisco IOS® XE 17.3.x 이상을 실행하는 모든 Catalyst 9K 플랫폼에 적용됩니다.

사용된 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IOS-XE 17.3.4 버전을 실행하는 Catalyst 9300 Series 스위치
- IOS-XE 17.3.4 버전을 실행하는 Catalyst 9400 Series 스위치
- 트래픽 생성을 위한 IXIA

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.

문제 해결 방식

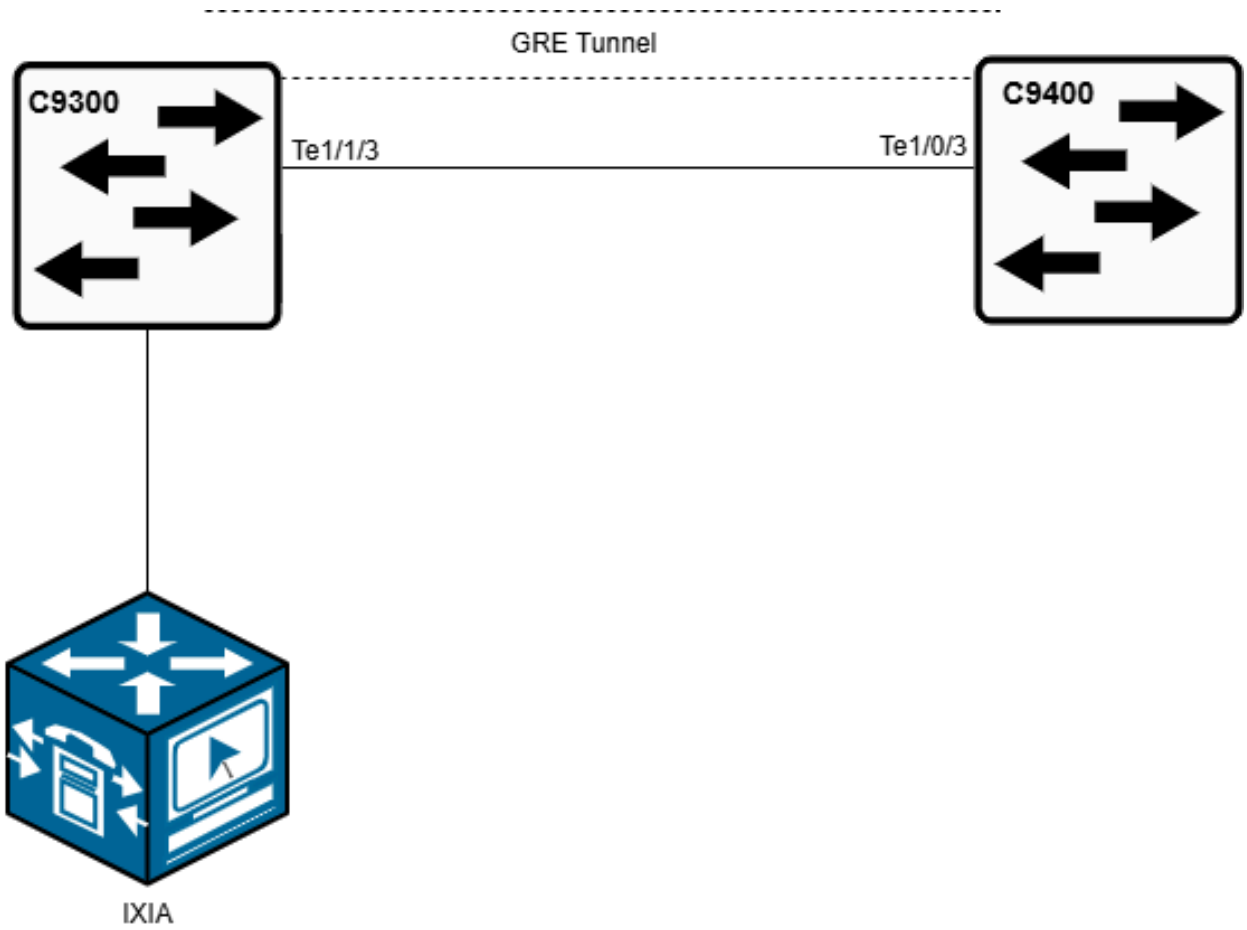
토폴로지

이 설정은 문제를 재현하기 위해 트래픽 생성기가 있는 C9000 스위치로 구성됩니다. 추가 격리를 위한 테스트 포함:

조건 1: 'Null0' 또는 'MSS 조정' 없음
조건 2: 고정 경로가 Null0을 가리키면 MSS가 조정되지 않음
조건 3: Null0 및 MSS 조정 모두 활성화됨

소프트웨어 및 하드웨어 버전

- Cisco IOS XE 17.3.4 버전을 실행하는 Catalyst 9300 및 9400
- 트래픽 생성을 위한 IXIA



구성 요구 사항

- 구성된 'ip tcp adjust-mss' 및 'null0 경로'가 없습니다.
- 'null0 경로'만 구성된 경우
- 'ip tcp adjust-mss' 및 'null0 경로'가 구성된 경우
  'ip tcp adjust-mss value'(MTU(Maximum Transmission Unit) 미만의 값)(터널 인터페이스 또는 SVI(Switch Virtual Interface)(인그레스)
  'ip 경로 X.X.X.X X.X.X Null0'(Null0을 가리키는 고정 경로)

설명한 조건에 따라 직접 연결된 BGP(Border Gateway Protocol) 피어 및 동일한 디바이스 또는 직접 연결된 피어에 구성된 SVI와의 연결이 간헐적으로 관찰됩니다. CoPP(컨트롤 플레인 정책) 명령 및 디버그를 실행하는 동안 소프트웨어(SW) 전달 대기열에 삭제 카운터가 지속적으로 증가하고 있습니다. 조사 결과 Null0을 위한 트래픽이 대신 CPU로 전달됩니다. 이 동작은 TCP 3-way 핸드셰이크 완료를 방지하여 BGP 프로토콜을 중단했습니다. 또한 스위치에 구성된 SVI IP 주소에 대한 ping이 실패했습니다.

시나리오

사례 1. 'Null0' 또는 'MSS 조정'이 없는 경우

'ip tcp adjust-mss' 또는 'null 경로'가 구성되지 않은 경우, 예상대로 IXIA에서 생성된 트래픽 후에

SW 전달 대기열의 삭제 카운터가 '0'에 유지됩니다.

다음 로그를 참조하십시오.

```
Cat-9400-1# 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)
--------------------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 0 0>>>>>>>>>>>>>>>>>>>>>>>>>>>>No increment
```

사례 2. 고정 경로가 Null0을 가리키면 MSS가 조정되지 않음

Null0 경로만 구성된 경우 예상대로 IXIA에서 생성된 트래픽 후에 SW 전달 대기열의 삭제 카운터가 '0'에 유지됩니다.

다음 로그를 참조하십시오.

```
Cat-9400-1# 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)
--------------------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 0 0>>>>>>>>>>>>>>>>>>>>>>>>>>>>No increment
```

사례 3. 'Null0' 및 'MSS Adjust'가 모두 사용됨

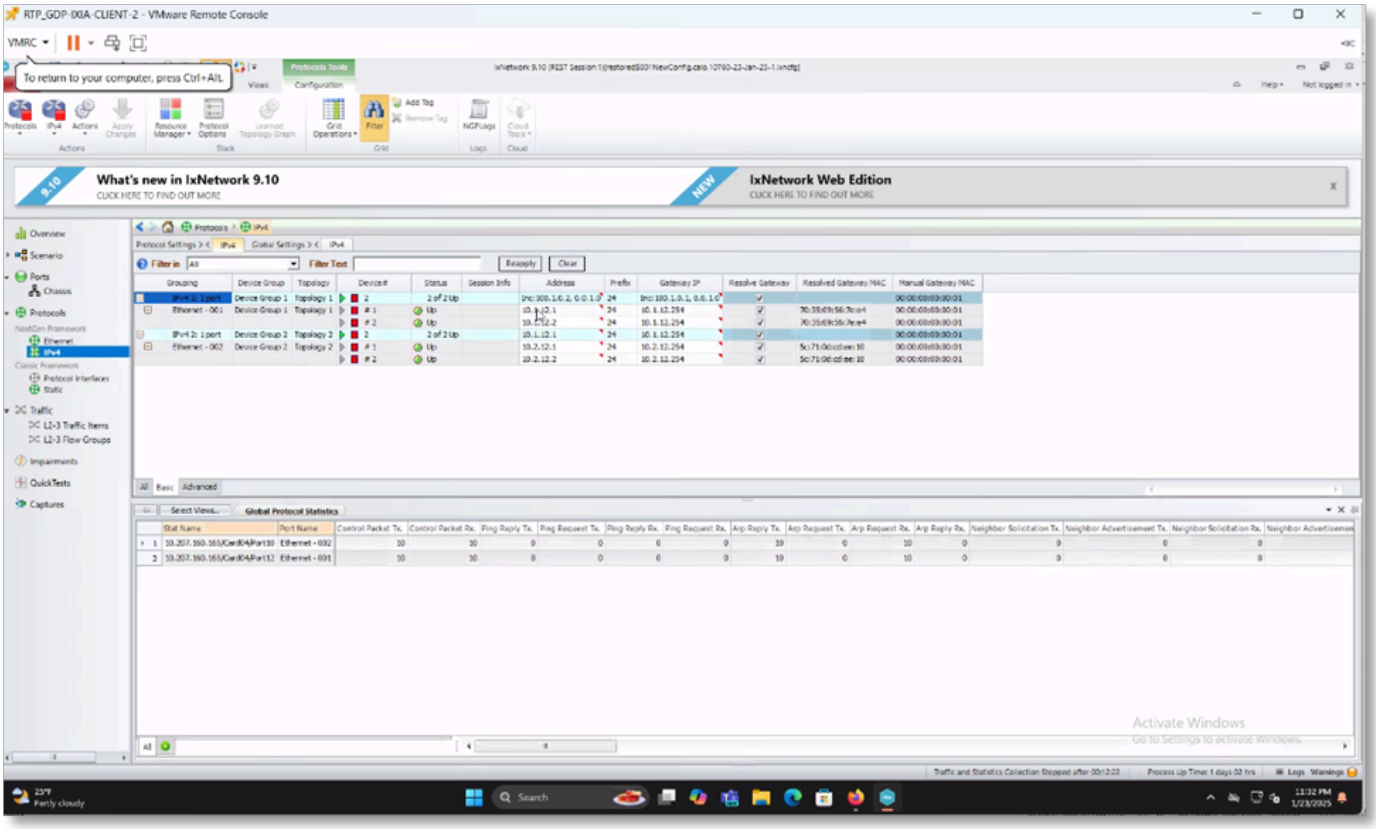
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
Configuration:

On Cat 9300:
Cat-9300-1#show run interface twoGigabitEthernet 1/0/1
interface TwoGigabitEthernet1/0/1 (Interface connected to IXIA)
no switchport
ip address 10.1.12.xx 255.255.255.0
end
Cat-9300-1#show run interface tenGigabitEthernet 1/1/3
interface TenGigabitEthernet1/1/3 (Physical interface connected to C9400)
no switchport
mtu 9000
ip address 203.63.147.xx 255.255.255.0
```

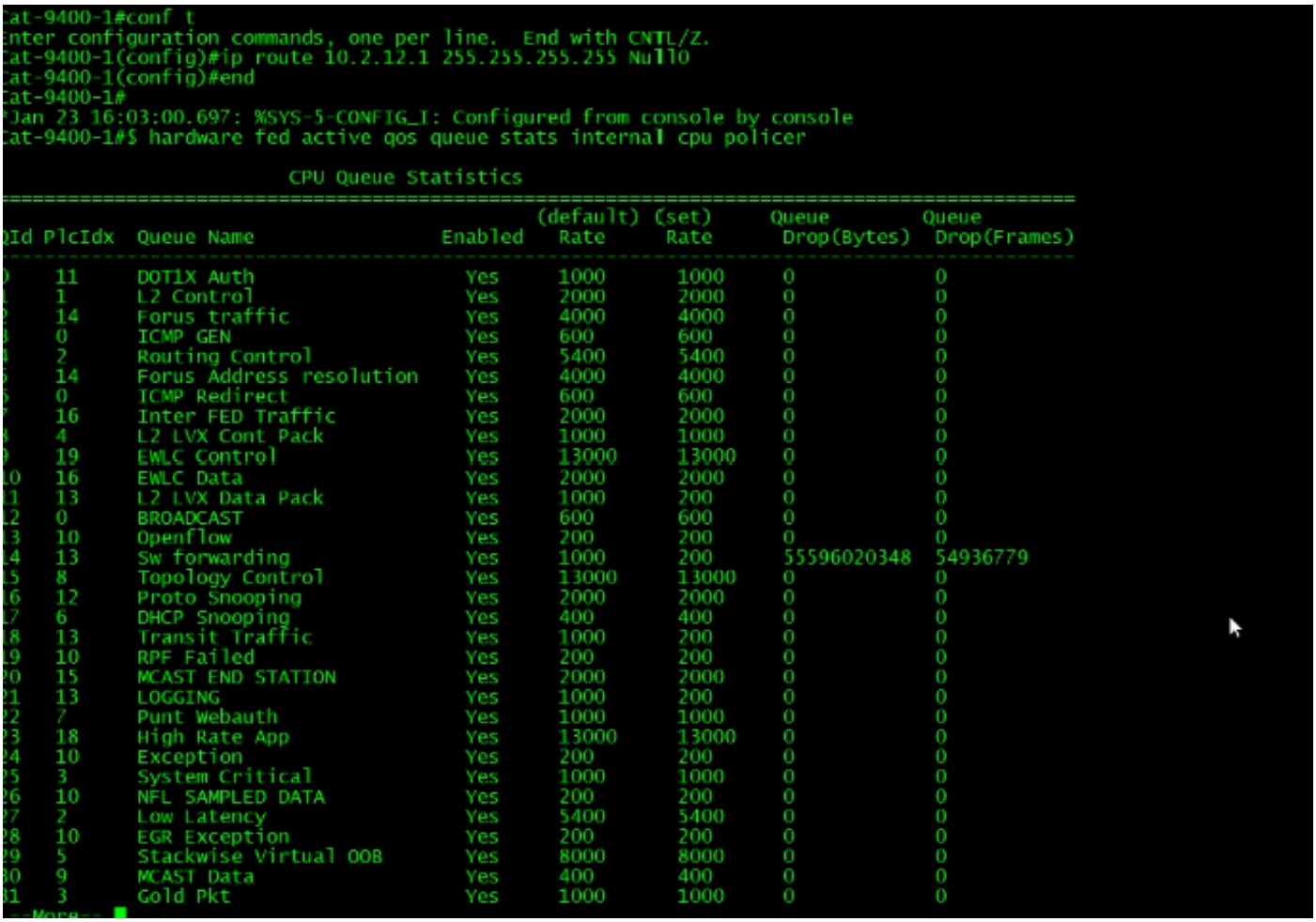
```
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

Cat-9300-1#show run interface tunnel421
interface Tunnel421
description Tunnel 421 to Scrubbing Center - SYD EDGE 1 and 2 - AR1 Tunnel 30
ip address 10.88.178.xx 255.255.255.0
ip mtu 1470
load-interval 30
Cisco Confidential
keepalive 10 3
tunnel source 203.63.147.xx
tunnel destination 203.63.147.xx
end

On cat 9400:
Cat-9400-1#show run interface tenGigabitEthernet 1/0/3
interface TenGigabitEthernet1/0/3 (Interface connected to C9300)
description CN,ISP,S1 AAPT, Superloop Circuit ID SID565199 - AAPT Circuit ID 5804194
no switchport
mtu 9000
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

interface Tunnel421
description Tunnel 421 to Scrubbing Center - SYD EDGE 1 and 2 - AR1 Tunnel 30
ip address 10.88.178.xx 255.255.255.0
ip mtu 1470
ip tcp adjust-mss 500>>>>>>>>>>>>
load-interval 30
keepalive 10 3
tunnel source 203.63.147.xx
tunnel destination 203.63.147.xx
end

Null0 Routes:
ip route 10.2.12.xx 255.255.255.255 null0>>>>>>>>Destination IP is of IXIA connected to 9300

Cat-9400-1#show ip route
Gateway of last resort is 203.63.147.xx to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 203.63.147.xx
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.2.12.0/24 [1/0] via 192.168.12.xx
S 10.2.12.xx/32 is directly connected, Null0
C 10.88.178.0/24 is directly connected, Tunnel421
L 10.88.178.xx/32 is directly connected, Tunnel421
```

Null0 경로 및 MSS가 C9400의 인그레스 터널 인터페이스의 컨피그레이션을 조정한 후 IXIA에서 트래픽이 생성되었으며 다음 이미지와 같이 CPU QID(Queue Identity) 14에 대한 삭제 카운터가 증가합니다.

IXIA



C9400 CoPP 출력:



```
Cat-9400-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat-9400-1(config)#ip route 10.2.12.1 255.255.255.255 Null0
Cat-9400-1(config)#end
Cat-9400-1#
Jan 23 16:03:00.697: %SYS-5-CONFIG_I: Configured from console by console
Cat-9400-1#$ 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      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
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      200       0             0
12   0      BROADCAST                 Yes      600       600       0             0
13   10     Openflow                  Yes      200       200       0             0
14   13     Sw forwarding             Yes      1000      200       55596020348   54936779
15   8      Topology Control          Yes      13000     13000     0             0
16   12     Proto Snooping            Yes      2000      2000      0             0
17   6      DHCP Snooping             Yes      400       400       0             0
18   13     Transit Traffic           Yes      1000      200       0             0
19   10     RPF Failed                Yes      200       200       0             0
20   15     MCAST END STATION         Yes      2000      2000      0             0
21   13     LOGGING                   Yes      1000      200       0             0
22   7      Punt Webauth              Yes      1000      1000      0             0
23   18     High Rate App             Yes      13000     13000     0             0
24   10     Exception                 Yes      200       200       0             0
25   3      System Critical           Yes      1000      1000      0             0
26   10     NFL SAMPLED DATA          Yes      200       200       0             0
27   2      Low Latency               Yes      5400      5400      0             0
28   10     EGR Exception             Yes      200       200       0             0
29   5      Stackwise Virtual OOB     Yes      8000      8000      0             0
30   9      MCAST Data                Yes      400       400       0             0
31   3      Gold Pkt                  Yes      1000      1000      0             0
--More--
```

```
Cat-9400-1# show platform hardware fed active qos queue stats internal cpu policer
============================================================================================
(default) (set) Queue Queue
QId PlcIdx Queue Name Enabled Rate Rate Drop(Bytes) Drop(Frames)
--------------------------------------------------------------------------------------------
14 13 Sw forwarding Yes 1000 200 3252568000 3214000>>>>>> Drops increasing in this Queue

Cat-9400-1# 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      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
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    200     0              0
12   0     BROADCAST                   Yes    600     600     0              0
13   10    Openflow                    Yes    200     200     0              0
14   13    Sw forwarding               Yes    1000    200     40147794808 39671734>>>>>>With MSS a
15   8     Topology Control            Yes    13000   13000   0              0
16   12    Proto Snooping              Yes    2000    2000    0              0
17   6     DHCP Snooping               Yes    400     400     0              0
```

Null0 고정 경로 및 MSS 클램핑 설명

이론에 따르면 브로드캐스트 트래픽과 같은 원치 않는 트래픽을 처리하거나 특정 서브넷에 대한 액세스를 차단하기 위해 한 가지 옵션은 트래픽을 Null0으로 보내는 고정 경로를 설정하는 것입니다. 이렇게 하면 라우터가 해당 네트워크에 대한 모든 트래픽을 버립니다.

Null0에 대한 명령

```
ip route <destination-network> <subnet-mask> null 0

For an example:

ip route 10.2.12.xx 255.255.255.255 null0>>>>>>Destination IP is of IXIA connected to 9300
```

Null 0 구문은 10.2.12.1/32이 아무 곳에서도 전달되지 않도록 합니다. 이는 대상 네트워크로 향하는 모든 트래픽이 Null0에서 폐기(삭제)됨을 의미합니다.

TCP MSS

반면, TCP MSS 조정:

MSS 조정은 TCP 패킷의 MSS를 수정합니다. MTU 불일치가 발생할 경우(대개 MTU 설정이 다른 장치 간에 또는 VPN과 같은 터널을 통해) 패킷이 조각화될 수 있습니다.

프래그먼트화는 패킷 손실 또는 성능 저하로 이어질 수 있으므로 TCP 트래픽에는 바람직하지 않습니다. MSS 클램핑은 TCP 세그먼트의 크기를 조정하여 경로 MTU에 맞게 패킷이 충분히 작도록 하여 프래그먼트화를 방지합니다. TCP 연결에 대해 값이 1360으로 설정된 터널 인터페이스 및 SVI에 MSS 조정을 적용하면 세그먼트 크기가 경로 MTU보다 작아지므로 프래그먼트화가 방지됩니다.

이상적인 시나리오

Null0은 해당 곳으로 향하는 모든 트래픽을 삭제하는 가상 '블랙홀' 인터페이스입니다. 라우팅 루프 또는 원치 않는 트래픽을 방지하는 것이 좋습니다.
TCP MSS adjust는 MTU가 더 작은 디바이스 또는 터널을 통과할 때 TCP 세그먼트가 프래그먼트화를 방지할 수 있을 만큼 작은지 확인하는 명령입니다.

조건

이 두 기능은 일반적으로 서로 다른 용도로 사용되지만, 트래픽 흐름을 관리하고 단편화를 방지하고 성능을 최적화하기 위해 전반적인 네트워크 설계에서 모두 역할을 할 수 있습니다. 그러나 Catalyst 9K 스위치에서 Null0과 MSS 조정을 함께 사용하면 충돌이 발생하여 CPU에 과부하가 걸리고 CoPP 정책이 마비될 수 있습니다.

확인

```
Show platform hardware fed active qos queue stats internal cpu policer
Identify the QID where the drop counters increments. After finding the QID (for example, QID 14), run th
#debug platform software fed switch active punt packet-capture set-filter "fed.queue == 14"
#debug platform software fed switch active punt packet-capture start
#debug platform software fed switch active punt packet-capture stop
#show platform software fed switch active punt packet-capture brief
#show platform software fed switch active punt packet-capture detailed
```

debug 명령을 사용하여 다음 형식의 로그를 확인하여 Null0 경로가 구성된 경우에도 CPU에서 펀트하는 공격자의 IP 주소를 식별합니다.

```
------ Punt Packet Number: XX, Timestamp: 2024/12/14 12:54:57.508 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel411 [if-id: 0x000000d2]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
Cisco Confidential
ipv4 hdr : dest ip: XX.XX.XX.XX, src ip: XX.XX.XX.XX
ipv4 hdr : packet len: 44, ttl: 242, protocol: 6 (TCP)
tcp hdr : dest port: 777, src port: 41724
```

디버그

```
Cat-9400-1# debug platform software fed active punt packet-capture set-filter "fed.queue == 14"
Filter setup successful. Captured packets will be cleared

Cat-9400-1#debug platform software fed active punt packet-capture start
Punt packet capturing started.

Cat-9400-1#debug platform software fed active punt packet-capture stop
Punt packet capturing stopped. Captured 4096 packet(s)

Cat-9400-1#show platform software fed active punt packet-capture brief
Total captured so far: 4096 packets. Capture capacity : 4096 packets
Capture filter : "fed.queue == 14"
------ Punt Packet Number: 1, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
------ Punt Packet Number: 2, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
------ Punt Packet Number: 3, Timestamp: 2025/01/23 16:16:54.978 ------
interface : physical: [if-id: 0x00000000], pal: Tunnel421 [if-id: 0x0000002e]
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : Partial ether header, ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.2.12.xx, src ip: 10.1.12.xx >>>10.2.12.xx is IXIA
Cisco Confidential
ipv4 hdr : packet len: 1006, ttl: 63, protocol: 6 (TCP)
tcp hdr : dest port: 60, src port: 60
```

결론

CPU 대기열이 원치 않는 트래픽에 압도되어 TCP/SSH(Secure Shell) 통신에 영향을 주지 않도록 하려면 이러한 IP 주소가 Catalyst 9K 스위치에 도달하기 전에 차단하거나 인그레스(ingress)에서 MSS 조정을 제거하십시오.

일반적으로 TCP 동기화(SYN) 패킷은 CPU 대기열에 푸시됩니다. MSS는 TCP 헤더의 옵션으로서 TCP/IP 헤더를 제외하고 수신자가 허용할 수 있는 최대 세그먼트 크기를 나타냅니다. 일반적으로 3방향 핸드셰이크에 대해 설정되며, 특히 SYN 패킷에서 설정됩니다.

이 문제를 해결하려면 RADWARE/Security Gateway에서 악의적인 IP를 지오차단하여 CPU 폴리서 대기열에 과부하가 발생하지 않도록 하고 BGP 피어링 및 TCP 연결을 안정화시킵니다.

해결

Radware/보안 게이트웨이에서 악성 IP가 성공적으로 차단되면 트래픽이 CPU 대기열에서 압도적으로 멈춥니다.

관련 정보

- https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/222338-troubleshoot-tcp-slowness-issues-due-to.html
- 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.