Problemen oplossen met scenario's met Null0 en MSS-klemmen

Inhoud

Inleiding

Dit document beschrijft de implicaties van het hebben van maximale segmentgrootte (MSS) aanpassing en statische routes die wijzen naar Null 0 op Catalyst 9K.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- Conceptuele kennis over TCP en MSS aanpassen
- Platform begrip van Cisco Catalyst 9K voor controle vliegtuig doorsturen en debugs.

Ondersteunde platforms

Dit document is van toepassing op alle Catalyst 9K-platforms waarop Cisco IOS® XE 17.3.x en hoger wordt uitgevoerd.

Gebruikt onderdeel

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

- Catalyst 9300 serie switches met IOS-XE 17.3.4 versie
- Catalyst 9400 serie switches met IOS-XE 17.3.4 versie
- IXIA voor het genereren van verkeer

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

aanpak van probleemoplossing

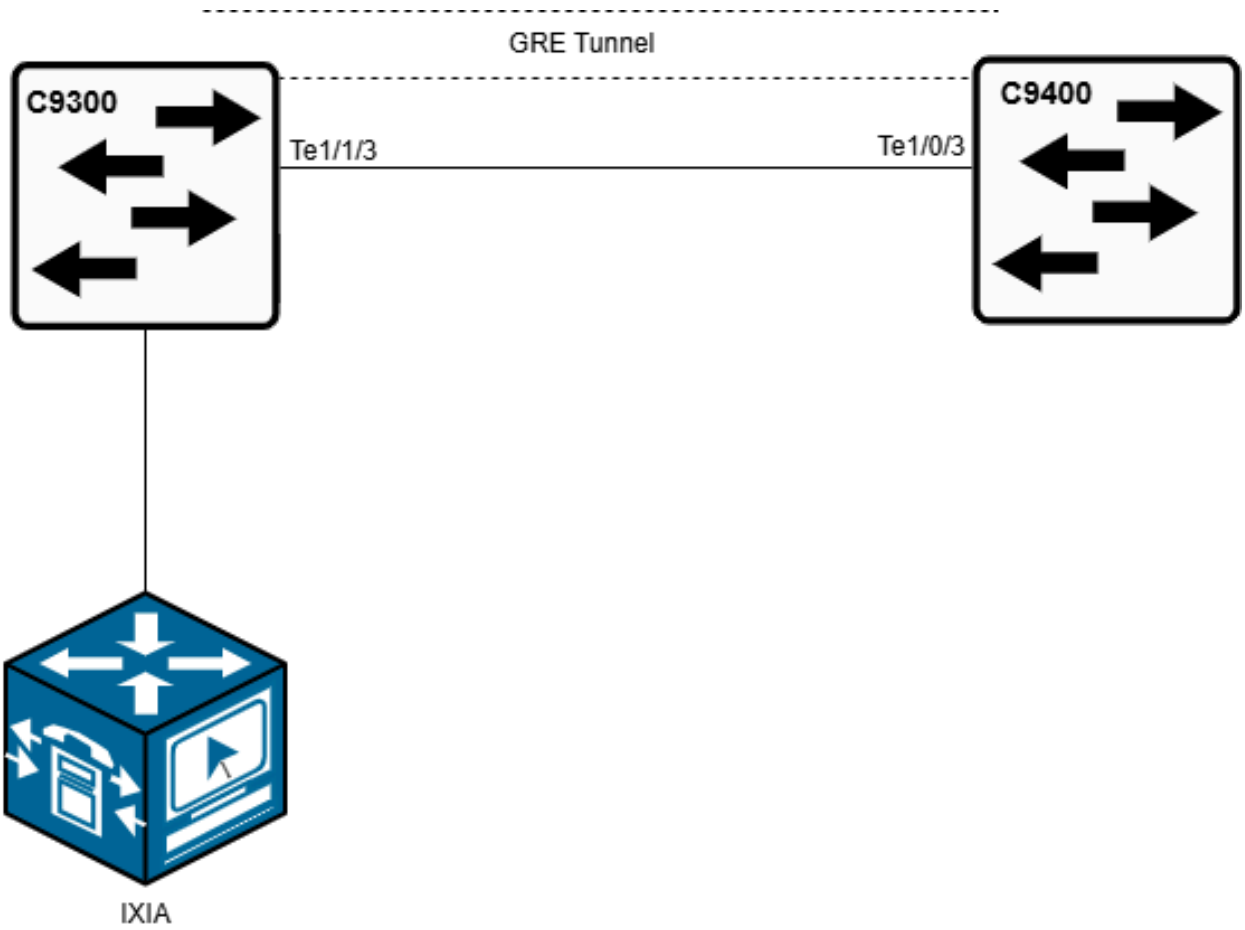
Topologie

De opstelling bestaat uit C9000-switches met een verkeersgenerator om het probleem te reproduceren. Inbegrepen testen voor verdere isolatie:

Voorwaarde 1: Zonder 'Null0' of 'MSS-aanpassen'
Toestand 2: met een statische route die naar Null0 wijst, geen MSS-aanpassing
Conditie 3: zowel Null0 als MSS aanpassen ingeschakeld

Software- en hardwareversies

- Catalyst 9300 en 9400 met Cisco IOS XE 17.3.4-versie
- IXIA voor het genereren van verkeer



Configuratievereisten

- Geen 'ip tcp adjust-mss' en geen 'null0 route' geconfigureerd
- Met alleen 'null0 route' geconfigureerd
- Met 'ip tcp adjust-mss' en 'null0 route' geconfigureerd
  'ip tcp-adjust-mss value' (waarde kleiner dan Maximum Transmission Unit (MTU)) (On Tunnel interface of Switch Virtual Interface (SVI) (Ingress))
  'ip route X.X.X.X.X.X.X.X Null0' (Statische routes die naar Null0 wijzen)

Op basis van de beschreven omstandigheden kunt u intermitterende connectiviteit waarnemen met direct verbonden Border Gateway Protocol (BGP)-peers en met SVI's die op hetzelfde apparaat of op direct verbonden peers zijn geconfigureerd. Er is ook een consistente toename van drop-tellers in de software (SW) Forwarding-wachtrij tijdens het uitvoeren van Control Plane Policing (CoPP) -opdrachten en debugs. Onderzoek toont aan dat verkeer dat bedoeld is voor Null0 in plaats daarvan naar de CPU wordt geleid. Dit gedrag verstoorde het BGP-protocol door de voltooiing van de TCP 3-weg handshake te voorkomen. Bovendien zijn pings naar de SVI IP-adressen die op de switch zijn geconfigureerd mislukt.

Scenario's

Situatie 1. Zonder 'Null0' of 'MSS Adjust'

Als noch 'ip tcp adjust-mss' noch een 'null route' is geconfigureerd, blijft de dropcounter in de SW forwarding queue op '0' staan na verkeer dat is gegenereerd vanuit IXIA, zoals verwacht.

Verwijs deze logs:

```
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
```

Situatie 2. Met een statische routepunten naar Null0, geen MSS aanpassen

Als alleen de Null0-route is geconfigureerd, blijft de valteller in de SW-wachtrij voor doorsturen op '0' na verkeer dat is gegenereerd vanuit IXIA, zoals verwacht.

Verwijs deze logs:

```
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
```

Situatie 3. Zowel 'Null0' als 'MSS Adjust' zijn ingeschakeld

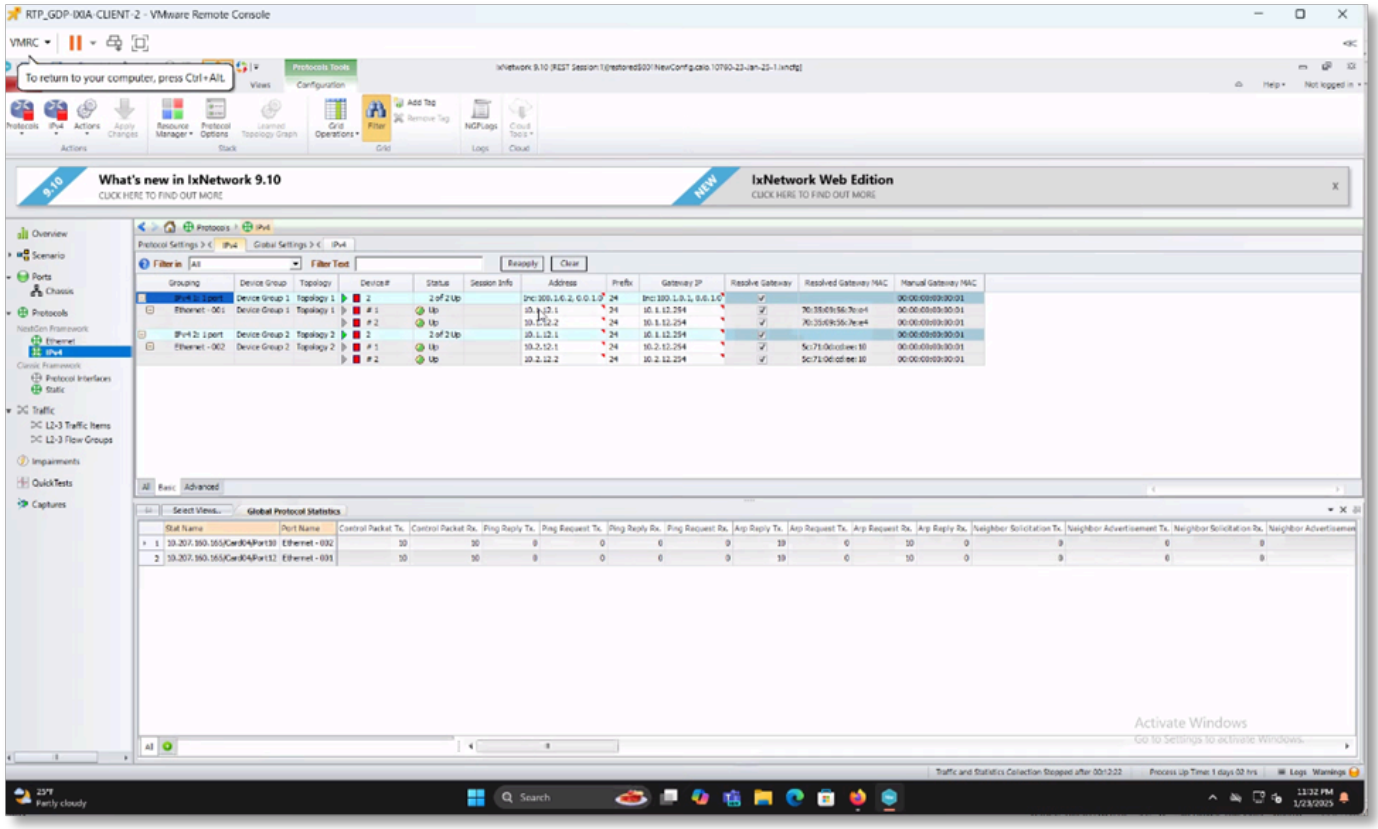
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
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
```

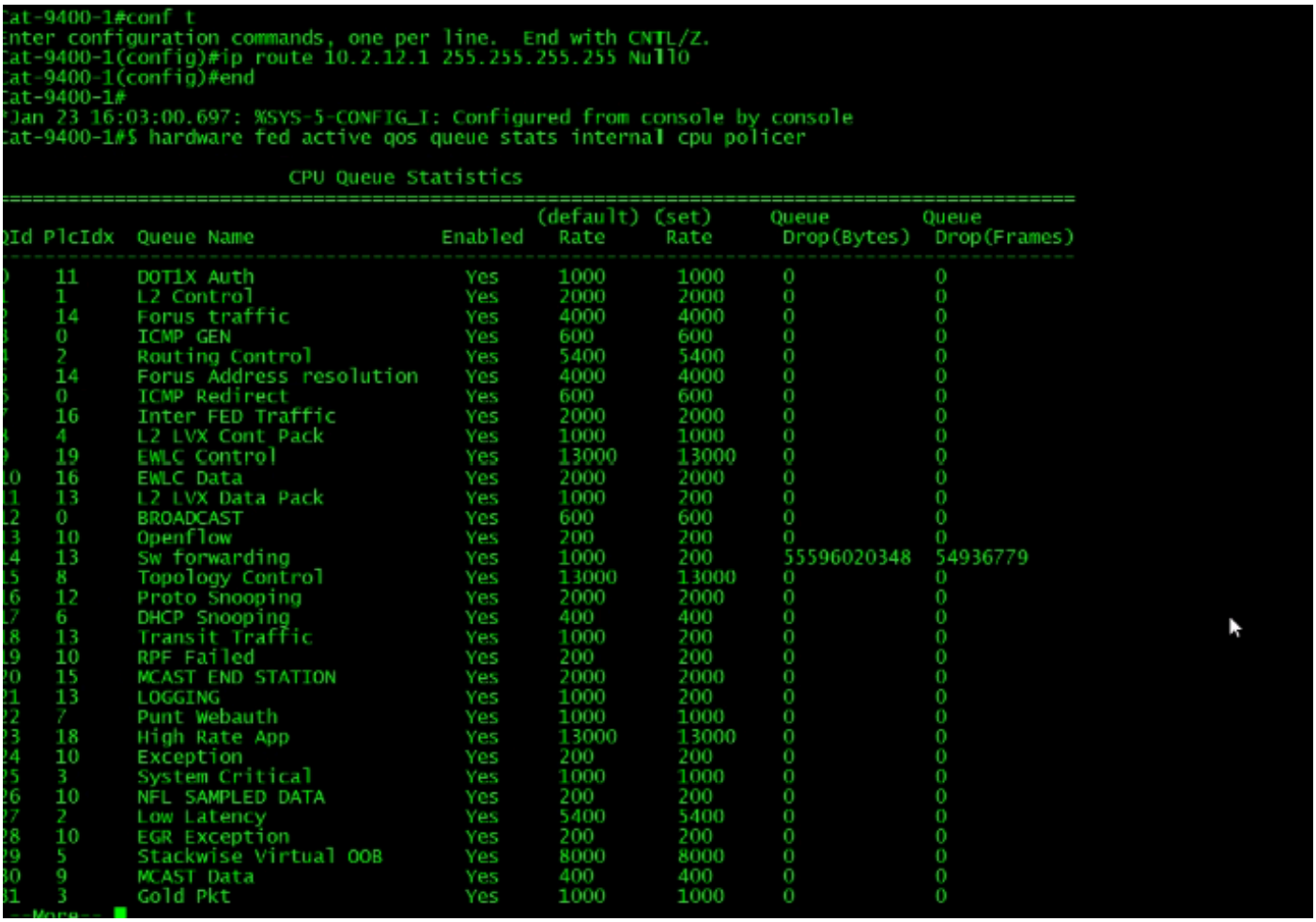
```
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

Nadat Null0-routes en MSS de configuratie op de ingangstunnelinterface van de C9400 hadden aangepast, werd verkeer gegenereerd vanuit IXIA en werden de valtellers voor CPU Queue Identity (QID) 14 verhoogd, zoals weergegeven in de volgende afbeelding.

IXIA



C9400 CoPP-uitgang:



```
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
```

Uitleg van Null0 statische routes en MSS-klemmen

Volgens de theorie, om ongewenst verkeer zoals uitzendverkeer te verwerken of de toegang tot specifieke subnetten te blokkeren, is een optie om een statische route in te stellen die het verkeer naar Null0 leidt. Dit zorgt ervoor dat de router alle verkeer weggooit dat voor dat netwerk is bedoeld.

Opdracht voor Null0

```
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 syntaxis zorgt ervoor dat de 10.2.12.1/32 nergens worden doorgestuurd. Dit betekent dat alle verkeer dat bestemd is voor het bestemmingsnetwerk, wordt weggegooid (gedropt) bij Null0.

TCP MSS

Aan de andere kant, TCP MSS-aanpassing:

MSS-aanpassing wijzigt de MSS voor TCP-pakketten. Wanneer een MTU-mismatch optreedt, vaak tussen apparaten met verschillende MTU-instellingen of via tunnels zoals VPN's, kunnen pakketten worden gefragmenteerd.

Fragmentatie is ongewenst voor TCP-verkeer omdat het kan leiden tot pakketverlies of prestatievermindering. MSS-klemmen pakt dit probleem aan door de grootte van TCP-segmenten aan te passen, zodat pakketten klein genoeg zijn om binnen het MTU-pad te passen en fragmentatie wordt voorkomen. Wanneer MSS-aanpassing wordt toegepast op tunnelinterfaces en SVI's met een waarde die is ingesteld op 1360 voor TCP-verbindingen, zorgt dit ervoor dat de segmentgrootte kleiner is dan het pad MTU, wat fragmentatie voorkomt.

Ideaal scenario

Null0 is een virtuele 'black hole'-interface die elk verkeer dat ernaar toe wordt gericht, laat vallen. Het is nuttig om routeringslussen of ongewenst verkeer te voorkomen.
TCP MSS-aanpassing is een opdracht die ervoor zorgt dat TCP-segmenten klein genoeg zijn om fragmentatie te voorkomen bij het passeren van apparaten of tunnels met kleinere MTU's.

Voorwaarde

Hoewel deze twee functies over het algemeen voor verschillende doeleinden worden gebruikt, kunnen ze beide een rol spelen in een algemeen netwerkontwerp om de verkeersstroom te beheren, fragmentatie te voorkomen en de prestaties te optimaliseren. Op Catalyst 9K-switches kan het gebruik van zowel Null0- als MSS-aanpassing echter leiden tot conflicten, overbelasting van de CPU en overweldiging van het CoPP-beleid.

Verificatie

```
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 t
#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
```

Met behulp van de foutopsporingsopdrachten controleert u de logs in de volgende indeling om het IP-adres van de aanvallers te identificeren die op de CPU worden geplaatst, zelfs als de Null0-routes zijn geconfigureerd:

```
------ 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
```

Debugs

```
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
```

Conclusie

Om te voorkomen dat CPU-wachtrijen worden overspoeld door ongewenst verkeer en de TCP/Secure Shell (SSH)-communicatie beïnvloeden, blokkeert u deze IP-adressen voordat ze de Catalyst 9K-switches bereiken of verwijdert u MSS-instellingen bij binnendringen.

Doorgaans synchroniseert het TCP-pakket (SYN) met de CPU-wachtrij. MSS is een optie in de TCP-header die de maximale segmentgrootte aangeeft die de ontvanger kan accepteren, behalve TCP/IP-headers. Het wordt meestal ingesteld voor de 3-weg handshake, met name in het SYN-

pakket.

Om dit probleem op te lossen, kunt u de kwaadaardige IP's op de RADWARE/Security Gateway geoblocken om te voorkomen dat de CPU-policer-wachtrij overweldigd raakt en om BGP-peering en TCP-verbindingen te stabiliseren.

resolutie

Zodra kwaadaardige IP's met succes op de Radware/security gateway waren geblokkeerd, stopte het verkeer met het overweldigen van de CPU-wachtrij.

Gerelateerde informatie

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

Over deze vertaling

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