Resolución de Problemas de Escenarios con Null0 y MSS Clamping

Contenido

Introducción

Este documento describe las implicaciones de tener un ajuste de tamaño máximo de segmento (MSS) y rutas estáticas que apuntan a Null 0 en Catalyst 9K.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Ajuste del conocimiento conceptual sobre TCP y MSS
- Información sobre la plataforma de Cisco Catalyst 9K para reenvío y depuraciones del plano de control.

Plataformas Soportadas

Este documento es aplicable a todas las plataformas Catalyst 9K que ejecutan Cisco IOS® XE 17.3.x y posteriores.

Componente utilizado

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9300 Series Switches que ejecutan IOS XE versión 17.3.4
- Switches Catalyst de la serie 9400 que ejecutan la versión 17.3.4 del IOS-XE
- IXIA para generar tráfico

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Enfoque de Troubleshooting

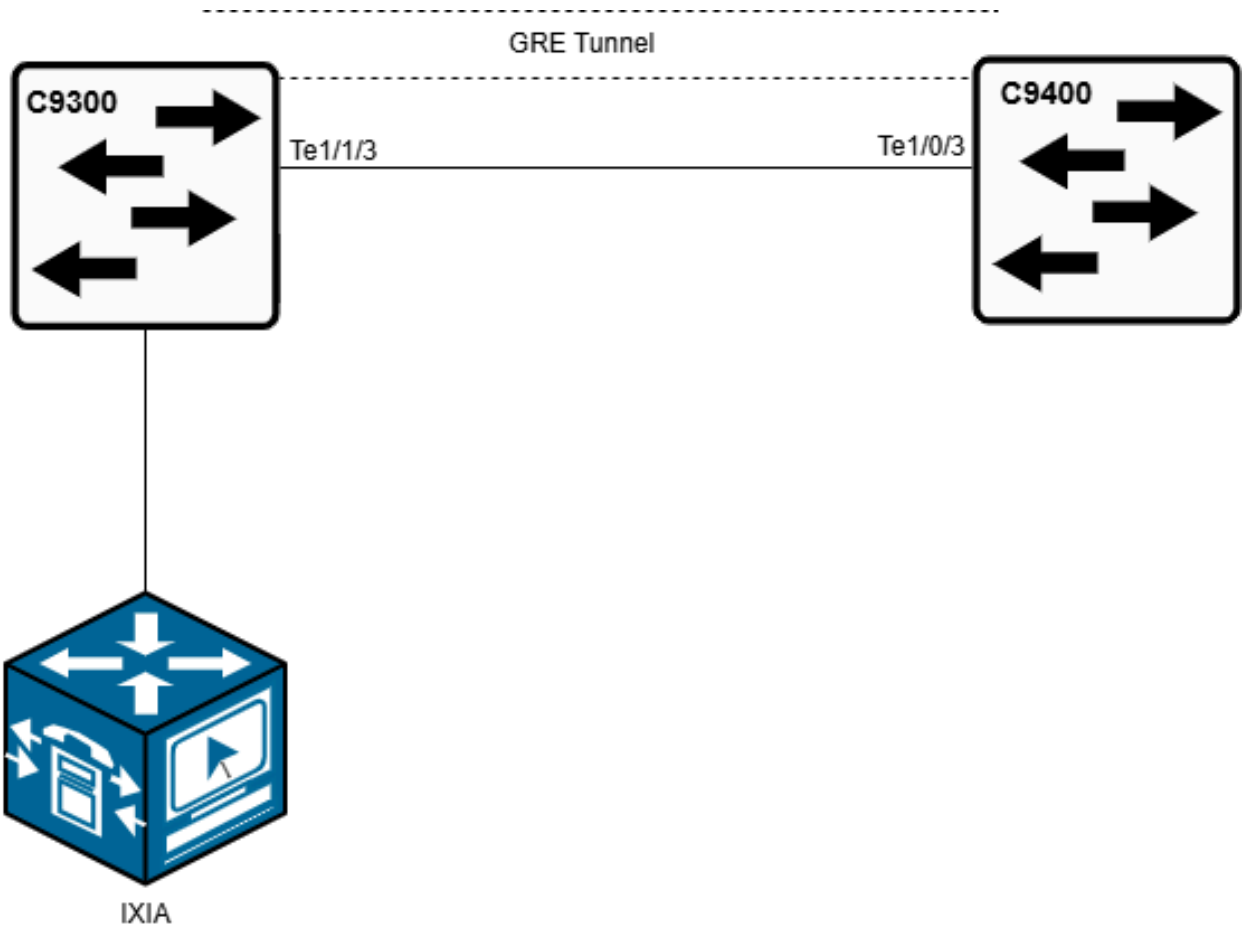
Topología

La configuración consta de switches C9000 con un generador de tráfico para reproducir el problema. Pruebas incluidas para un mayor aislamiento:

Condición 1: Sin 'Null0' o 'MSS adjust'
Condición 2: Con una ruta estática que señala a Null0, no se ajusta MSS
Condición 3: Null0 y MSS adjust enabled

Versiones de software y hardware

- Catalyst 9300 y 9400 que ejecutan Cisco IOS XE versión 17.3.4
- IXIA para generar tráfico



Requisitos de configuración

- No 'ip tcp adjust-mss' ni 'null0 route' configurados
- Con solo 'ruta null0' configurada
- Con 'ip tcp adjust-mss' y 'null0 route' configurados
  'ip tcp adjust-mss value' (valor inferior a la unidad de transmisión máxima (MTU)) (en interfaz de túnel o interfaz virtual de switch (SVI) (entrada))
  'ip route X.X.X.X X.X.X.X Null0' (Rutas estáticas que apuntan a Null0)

En función de las condiciones descritas, observará conectividad intermitente con los pares BGP (del inglés Border Gateway Protocol, protocolo de gateway fronterizo) conectados directamente y con las SVI configuradas en el mismo dispositivo o en pares conectados directamente. También hay un aumento constante en los contadores de caídas en la cola de reenvío de software (SW) mientras se ejecutan los comandos y depuraciones de Control Plane Policing (CoPP). La investigación muestra que el tráfico destinado a Null0 se dirige a la CPU. Este comportamiento interrumpió el protocolo BGP al impedir la finalización del protocolo de enlace de 3 vías TCP. Además, los pings a las direcciones IP SVI configuradas en el switch fallaron.

Escenarios

Caso 1. Sin 'Null0' o 'MSS Adjust'

Si no se configura 'ip tcp adjust-mss' ni 'null route', el contador de caídas de la cola de reenvío de SW permanece en '0' después del tráfico generado desde IXIA, como se esperaba.

Consulte estos registros:

```
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
```

Caso 2. Con una ruta estática apunta a Null0, sin ajuste de MSS

Con solo la ruta Null0 configurada, el contador de caídas en la cola de reenvío de SW permanece en '0' después del tráfico generado desde IXIA, como se esperaba.

Consulte estos registros:

```
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
```

Caso 3. Habilitados 'Null0' y 'MSS Adjust'

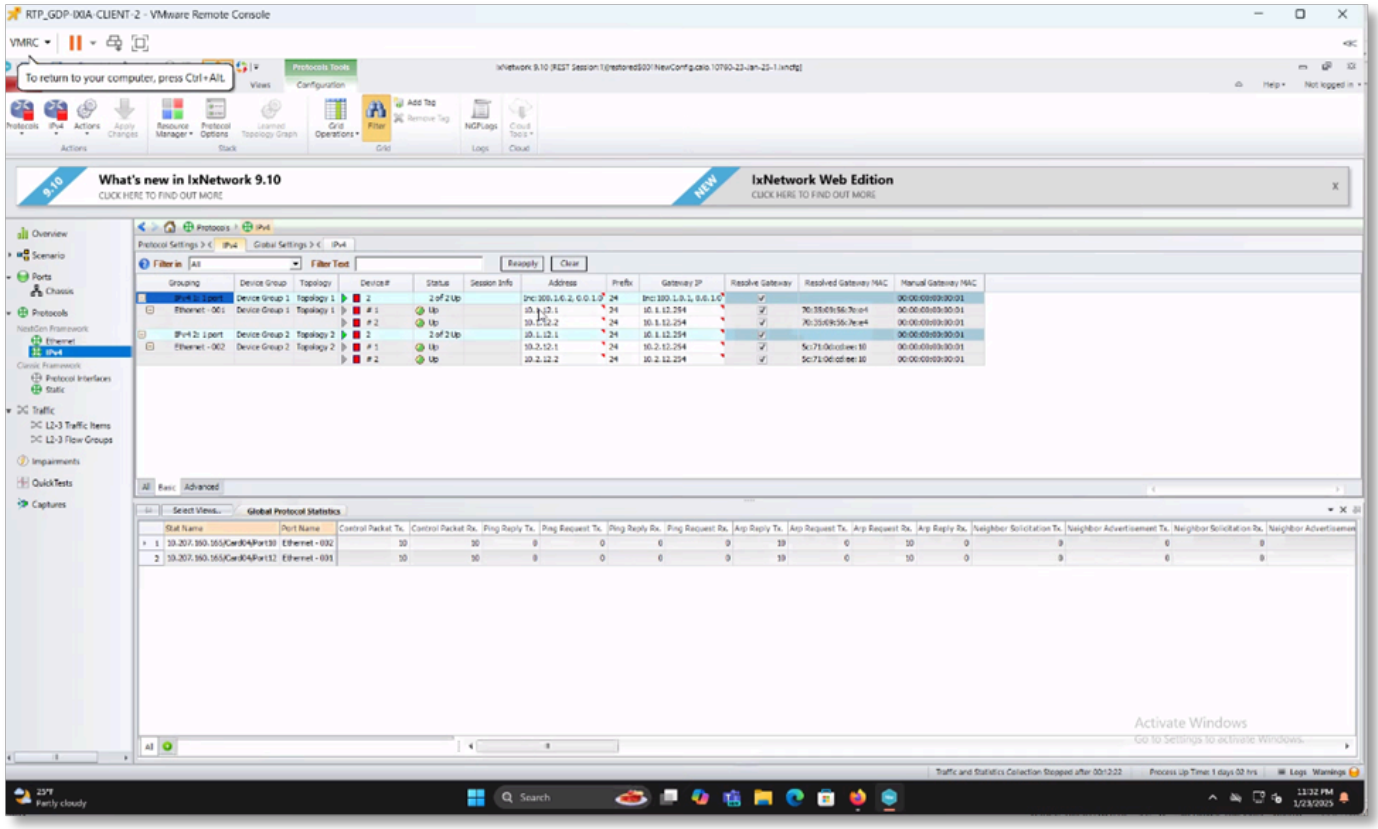
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
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
```

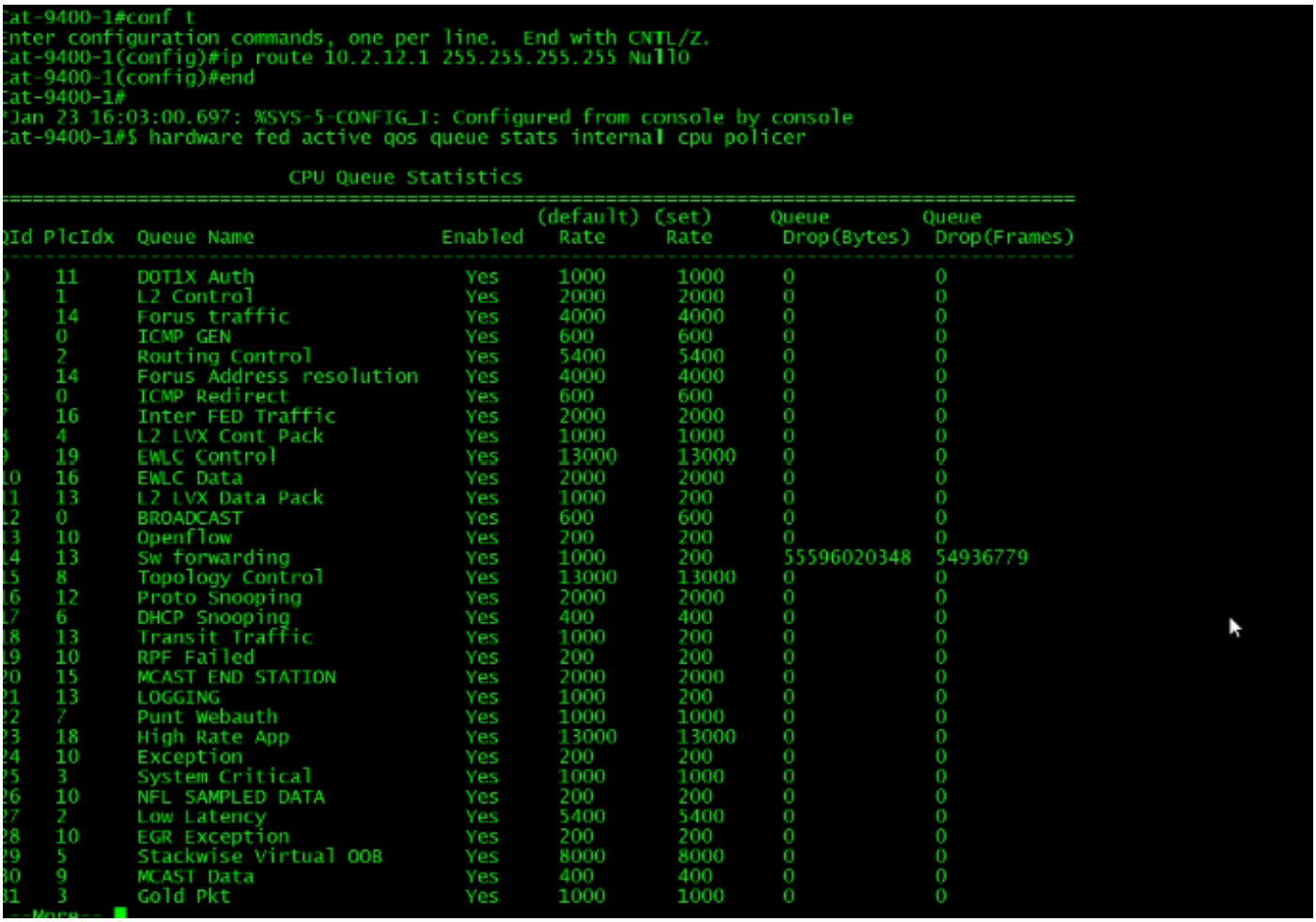
```
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

Después de que las rutas Null0 y MSS ajustaran la configuración en la interfaz de túnel de entrada del C9400, se generó tráfico desde IXIA y el contador de caídas aumenta para la identidad de cola de CPU (QID) 14, como se muestra en la siguiente imagen.

IXIA



Salida de CoPP de C9400:



```
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
```

Explicación de las Rutas Estáticas Nulas y la Sujeción MSS

Según la teoría, para manejar el tráfico no deseado como el tráfico de broadcast o bloquear el acceso a subredes específicas, una opción es configurar una ruta estática que dirija el tráfico a Null0. Esto hace que el router descarte cualquier tráfico destinado a esa red.

Comando para 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
```

La sintaxis nula 0 garantiza que 10.2.12.1/32 no se reenvíe a ninguna parte. Lo que significa que cualquier tráfico destinado a la red de destino se descarta (descarta) en Null0.

TCP MSS

Por otro lado, TCP MSS Adjustment:

El ajuste de MSS modifica el MSS para los paquetes TCP. Cuando se produce una discordancia de MTU (a menudo entre dispositivos con diferentes configuraciones de MTU o a través de túneles como VPN), los paquetes se pueden fragmentar.

La fragmentación no es deseable para el tráfico TCP porque puede llevar a la pérdida de paquetes o a la degradación del rendimiento. La sujeción MSS resuelve este problema ajustando el tamaño de los segmentos TCP, asegurando que los paquetes sean lo suficientemente pequeños como para caber dentro de la MTU de la trayectoria y, por lo tanto, evita la fragmentación. Cuando el ajuste MSS se aplica a las interfaces de túnel y SVI con un valor establecido en 1360 para las conexiones TCP, garantiza que el tamaño del segmento sea menor que la MTU de la trayectoria, lo que evita la fragmentación.

Situación ideal

Null0 es una interfaz virtual "agujero negro" que descarta cualquier tráfico dirigido hacia ella. Resulta útil para evitar bucles de routing o tráfico no deseado.
TCP MSS adjust es un comando que garantiza que los segmentos TCP son lo suficientemente pequeños como para evitar la fragmentación al pasar a través de dispositivos o túneles con MTU más pequeñas.

Condición

Aunque estas dos funciones se utilizan generalmente para fines diferentes, ambas pueden desempeñar un papel en un diseño de red general para administrar el flujo de tráfico, evitar la fragmentación y optimizar el rendimiento. Sin embargo, en los switches Catalyst 9K, el uso conjunto del ajuste Null0 y MSS puede conducir a conflictos, sobrecarga la CPU y sobrecarga la política CoPP.

Verificación

```
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
```

Usando los comandos debug, verifique los registros en el siguiente formato para identificar la dirección IP de los atacantes punts en la CPU, incluso con las rutas Null0 configuradas:

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

Depuraciones

```
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
```

Conclusión

Para evitar que las colas de CPU se vean saturadas por tráfico no deseado y que afecten a la comunicación TCP/Secure Shell (SSH), bloquee estas direcciones IP antes de que alcancen los switches Catalyst 9K o quite el ajuste MSS en el ingreso.

Normalmente, el paquete de sincronización TCP (SYN) se dirige a la cola de la CPU. MSS es una opción del encabezado TCP que indica el tamaño máximo de segmento que el receptor puede

aceptar, excepto los encabezados TCP/IP. Normalmente se configura para el protocolo de enlace de 3 vías, específicamente en el paquete SYN.

Para resolver este problema, bloquee geográficamente las IP maliciosas en el gateway de seguridad/RADWARE para evitar que la cola del regulador de CPU se agote y estabilice el peering BGP y las conexiones TCP.

Resolución

Una vez que las IP malintencionadas se bloquearon correctamente en el gateway de seguridad/firmware, el tráfico dejó de saturar la cola de la CPU.

Información Relacionada

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).