Risoluzione dei problemi relativi agli scenari con blocco Null0 e MSS

Sommario

Introduzione

In questo documento vengono descritte le implicazioni di una regolazione del valore MSS (Maximum Segment Size) e di route statiche con valore Null 0 su Catalyst 9K.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Correzione delle conoscenze concettuali su TCP e MSS
- Comprensione della piattaforma di Cisco Catalyst 9K per l'inoltro e il debug del control plane.

Piattaforme supportate

Questo documento è valido per tutte le piattaforme Catalyst 9K con Cisco IOS® XE 17.3.x e versioni successive.

Componente utilizzato

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Catalyst serie 9300 con IOS-XE versione 17.3.4
- Switch Catalyst serie 9400 con IOS-XE versione 17.3.4
- IXIA per la generazione del traffico

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Approccio per la risoluzione dei problemi

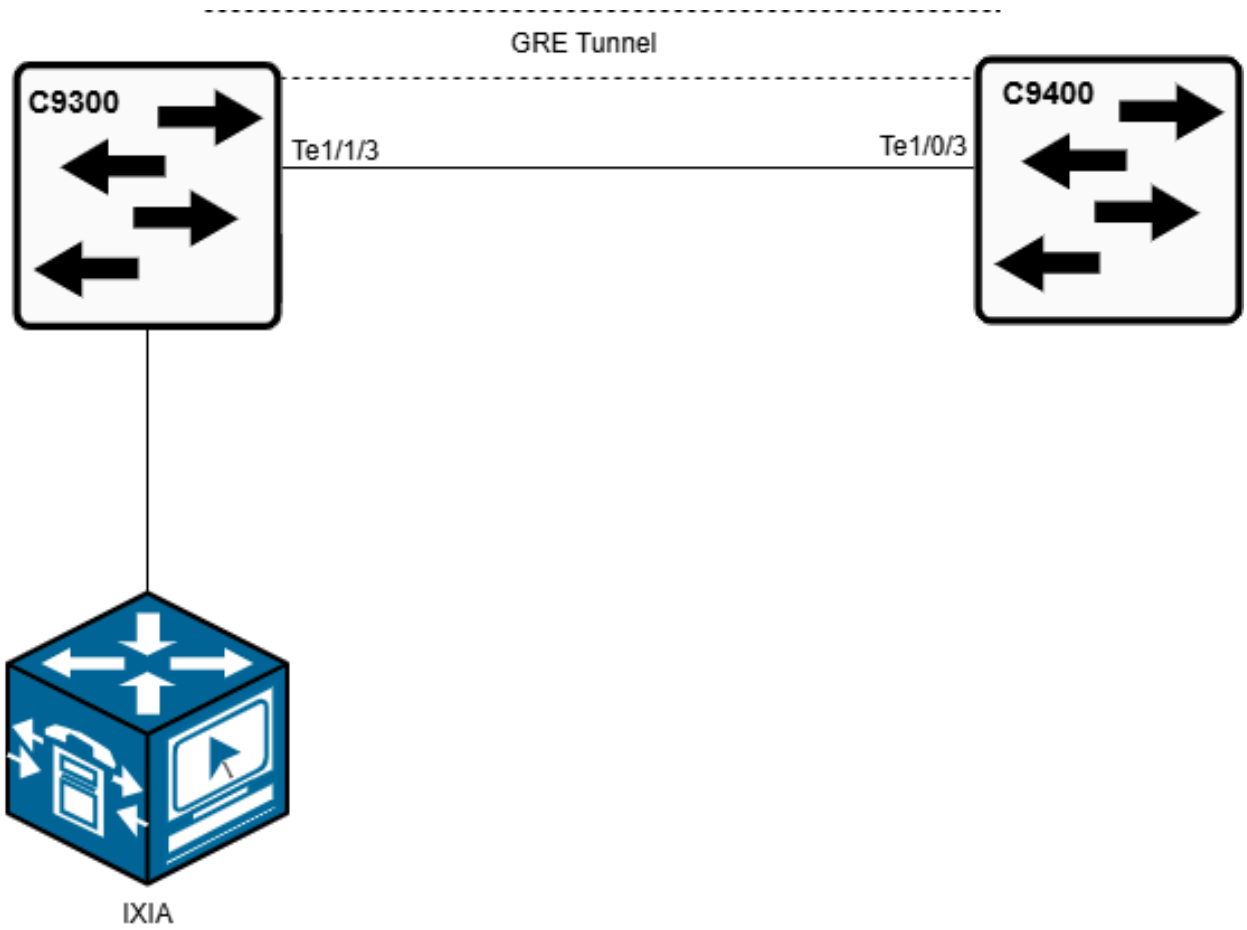
Topologia

La configurazione è costituita da switch C9000 con un generatore di traffico per riprodurre il problema. Prove incluse per un ulteriore isolamento:

Condizione 1: Senza 'Null0' o 'MSS adjust'
Condizione 2: Con una route statica che punta a Null0, non è possibile regolare il valore MSS
Condizione 3: Regolazione sia Null0 che MSS abilitata

Versioni software e hardware

- Catalyst 9300 e 9400 con Cisco IOS XE versione 17.3.4
- IXIA per la generazione del traffico



Requisiti di configurazione

- Nessun 'ip tcp adjust-mss' e nessuna 'route null0' configurati
- Con solo 'null0 route' configurato
- Con 'ip tcp adjust-mss' e 'null0 route' configurati
  'valore ip tcp adjust-mss' (valore inferiore al valore MTU (Maximum Transmission Unit))
  (sull'interfaccia tunnel o sull'interfaccia virtuale dello switch (SVI) (in entrata)
  'ip route X.X.X.X X.X.X.X Null0' (route statiche che puntano a Null0)

In base alle condizioni descritte, si osserverà una connettività intermittente ai peer Border Gateway Protocol (BGP) connessi direttamente e alle SVI configurate sullo stesso dispositivo o su peer connessi direttamente. È inoltre presente un aumento consistente dei contatori di rilascio nella coda di inoltro software (SW) durante l'esecuzione di comandi e debug CoPP (Control Plane Policing). L'analisi mostra che il traffico destinato a Null0 viene invece indirizzato alla CPU. Questo comportamento ha interrotto il protocollo BGP impedendo il completamento dell'handshake TCP a 3 vie. Inoltre, il ping sugli indirizzi IP SVI configurati sullo switch non è riuscito.

Scenari

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

Se non è configurato né 'ip tcp adjust-mss' né un 'percorso nullo', il contatore di rilascio nella coda di inoltro del software rimane su '0' dopo il traffico generato da IXIA, come previsto.

Fare riferimento ai seguenti registri:

```
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 route statica punta a Null0, nessun adeguamento MSS

Con solo la route Null0 configurata, il contatore di rilascio nella coda di inoltro del software rimane impostato su '0' dopo il traffico generato da IXIA, come previsto.

Fare riferimento ai seguenti registri:

```
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. Entrambe le opzioni 'Null0' e 'MSS Adjust' abilitate

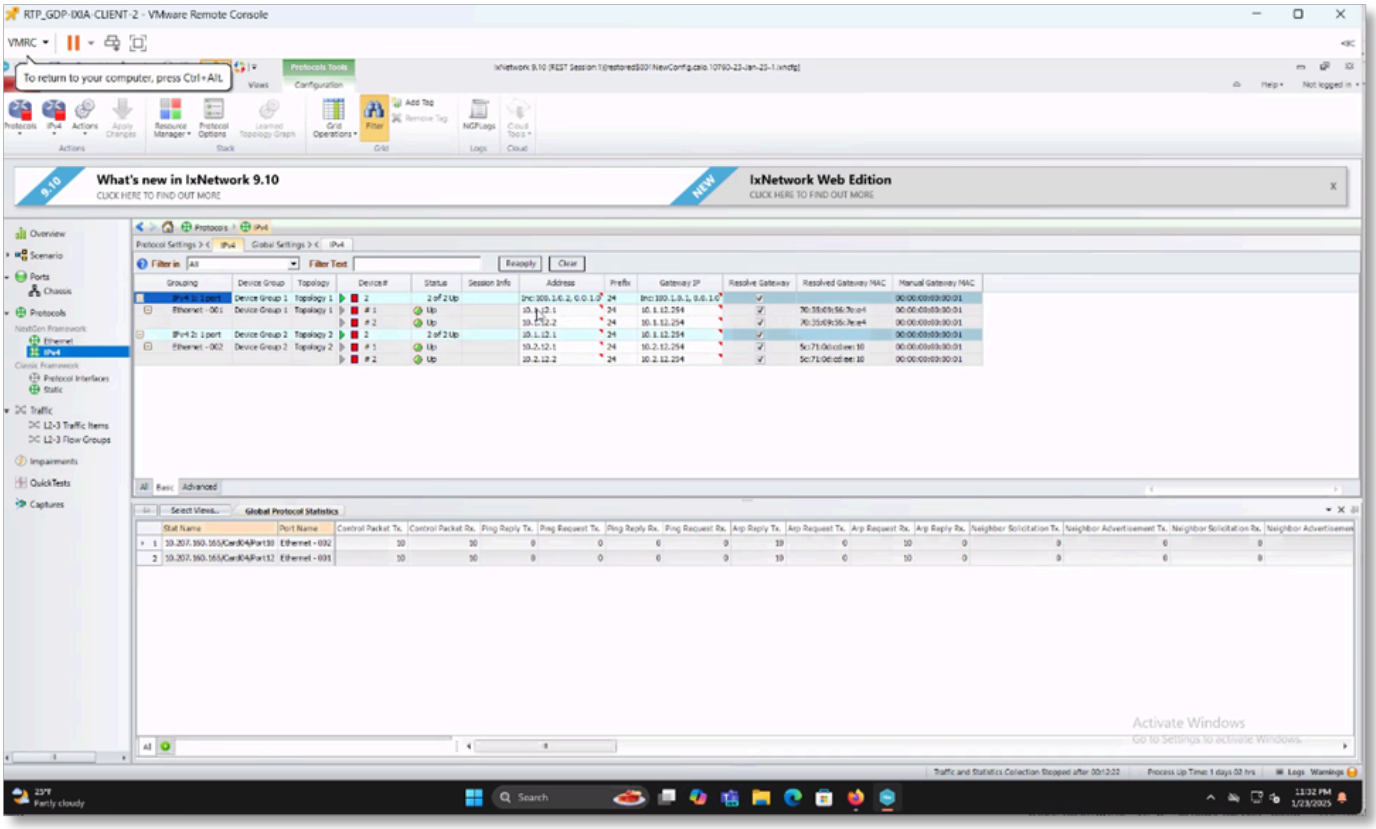
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
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
```

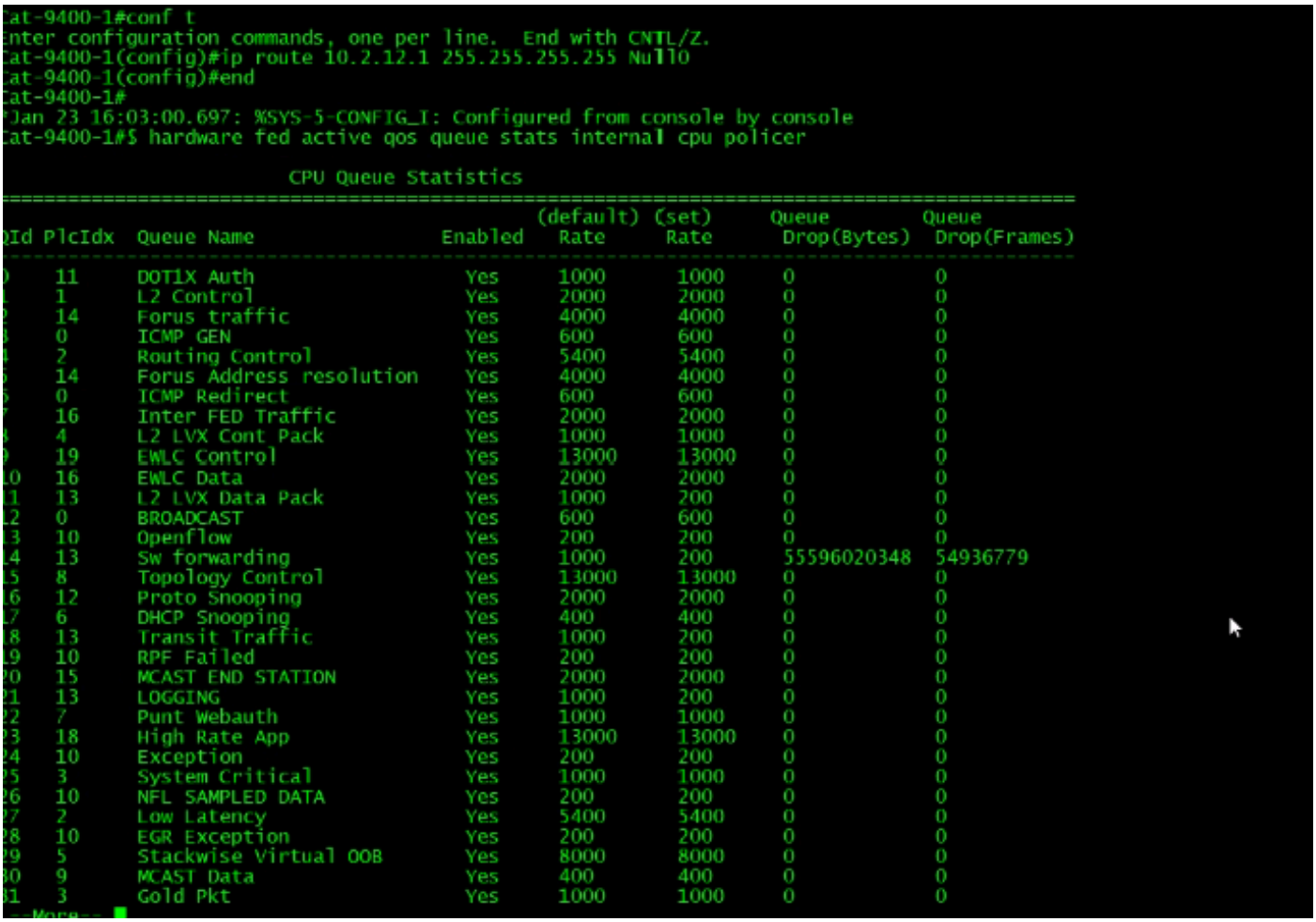
```
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

Dopo instradamenti Null0 e la regolazione della configurazione MSS sull'interfaccia del tunnel in entrata del C9400, il traffico è stato generato da IXIA e gli incrementi del contatore di rilascio per l'identità della coda della CPU (QID) 14, come mostrato nell'immagine seguente.

IXIA



Output C9400 CoPP:



```
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
```

Spiegazione delle route statiche Null0 e del blocco MSS

In teoria, per gestire traffico indesiderato, ad esempio il traffico di trasmissione o l'accesso bloccato a subnet specifiche, è possibile configurare una route statica che indirizzi il traffico a Null0. In questo modo, il router scarta il traffico destinato alla rete.

Comando per 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 sintassi 0 Null garantisce che 10.2.12.1/32 non venga inoltrato in nessuna posizione. Ciò significa che qualsiasi traffico destinato alla rete di destinazione verrà scartato (scartato) a Null0.

TCP MSS

D'altra parte, la regolazione TCP MSS:

La regolazione MSS modifica il valore MSS per i pacchetti TCP. Quando si verifica una mancata corrispondenza MTU, spesso tra dispositivi con impostazioni MTU diverse o tramite tunnel come i VPN, i pacchetti possono essere frammentati.

La frammentazione non è desiderabile per il traffico TCP in quanto può causare la perdita dei pacchetti o il peggioramento delle prestazioni. Il blocco MSS risolve questo problema regolando le dimensioni dei segmenti TCP, garantendo che i pacchetti siano sufficientemente piccoli da poter essere inseriti nella MTU del percorso, e quindi prevenendo la frammentazione. Quando si applica la regolazione MSS alle interfacce tunnel e alle SVI con un valore impostato su 1360 per le connessioni TCP, questa funzione assicura che le dimensioni del segmento siano inferiori alla MTU del percorso, il che impedisce la frammentazione.

Scenario ideale

Null0 è un'interfaccia virtuale 'black hole' che scarta qualsiasi traffico diretto verso di essa. È utile per evitare loop di routing o traffico indesiderato.
La regolazione TCP MSS è un comando che assicura che i segmenti TCP siano sufficientemente piccoli da evitare la frammentazione quando passano attraverso dispositivi o tunnel con MTU inferiori.

Condizione

Sebbene queste due funzionalità siano in genere utilizzate per scopi diversi, possono entrambe svolgere un ruolo nella progettazione di una rete complessiva al fine di gestire il flusso del traffico, evitare la frammentazione e ottimizzare le prestazioni. Tuttavia, sugli switch Catalyst 9K, l'uso congiunto di Null0 e MSS può causare conflitti, sovraccaricare la CPU e sovraccaricare la policy CoPP.

Verifica

```
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 i comandi di debug, controllare i log nel formato successivo per identificare l'indirizzo IP dei punt degli aggressori sulla CPU, anche con le route Null0 configurate:

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

Debug

```
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
```

Conclusioni

Per evitare che le code della CPU vengano sovraccaricate da traffico indesiderato e influiscano sulle comunicazioni TCP/Secure Shell (SSH), bloccare questi indirizzi IP prima che raggiungano gli switch Catalyst 9K o rimuovere la regolazione MSS all'ingresso.

In genere, il pacchetto di sincronizzazione TCP (SYN) si adatta alla coda della CPU. Nell'intestazione TCP, il valore MSS è un'opzione che indica le dimensioni massime del segmento

che il ricevitore può accettare, ad eccezione delle intestazioni TCP/IP. In genere è impostato per l'handshake a 3 vie, in particolare nel pacchetto SYN.

Per risolvere il problema, bloccare tramite geoblocco gli IP dannosi sul gateway RADWARE/Security per evitare che la coda del policer della CPU venga sovraccaricata e stabilizzare il peering BGP e le connessioni TCP.

Risoluzione

Una volta che gli IP dannosi sono stati bloccati correttamente sul gateway Radware/Security, il traffico ha smesso di sopraffare la coda della CPU.

Informazioni correlate

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).