Dépannage des scénarios avec le serrage Null0 et MSS

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Plates-formes prises en charge
  - Composant utilisé
- Approche de dépannage
  - Topologie
  - Versions logicielles et matérielles
- Configuration requise
- Scénarios
  - Cas 1. Sans « Null0 » ou « MSS Adjust »
  - Cas 2. Avec une route statique qui pointe vers Null0, aucun ajustement MSS
  - Cas 3. 'Null0' et 'MSS Adjust' activés
  - IXIA
- Explication des routes statiques Null0 et du verrouillage MSS
  - Commande pour Null0
  - MSS TCP
  - Scénario idéal
- Condition
- Vérification
- Déboguages
- Conclusion
- Résolution
- Informations connexes

Introduction

Ce document décrit les implications du réglage de la taille de segment maximale (MSS) et des routes statiques pointant vers Null 0 sur Catalyst 9K.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- Connaissances conceptuelles sur l'ajustement TCP et MSS
- Compréhension de la plate-forme Cisco Catalyst 9K pour le transfert et les débogages du plan de contrôle.

Plates-formes prises en charge

Ce document s'applique à toutes les plates-formes Catalyst 9K exécutant Cisco IOS® XE 17.3.x et versions ultérieures.

Composant utilisé

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Catalyst 9300 exécutant la version IOS-XE 17.3.4
- Commutateurs de la gamme Catalyst 9400 exécutant la version IOS-XE 17.3.4
- IXIA pour générer du trafic

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Approche de dépannage

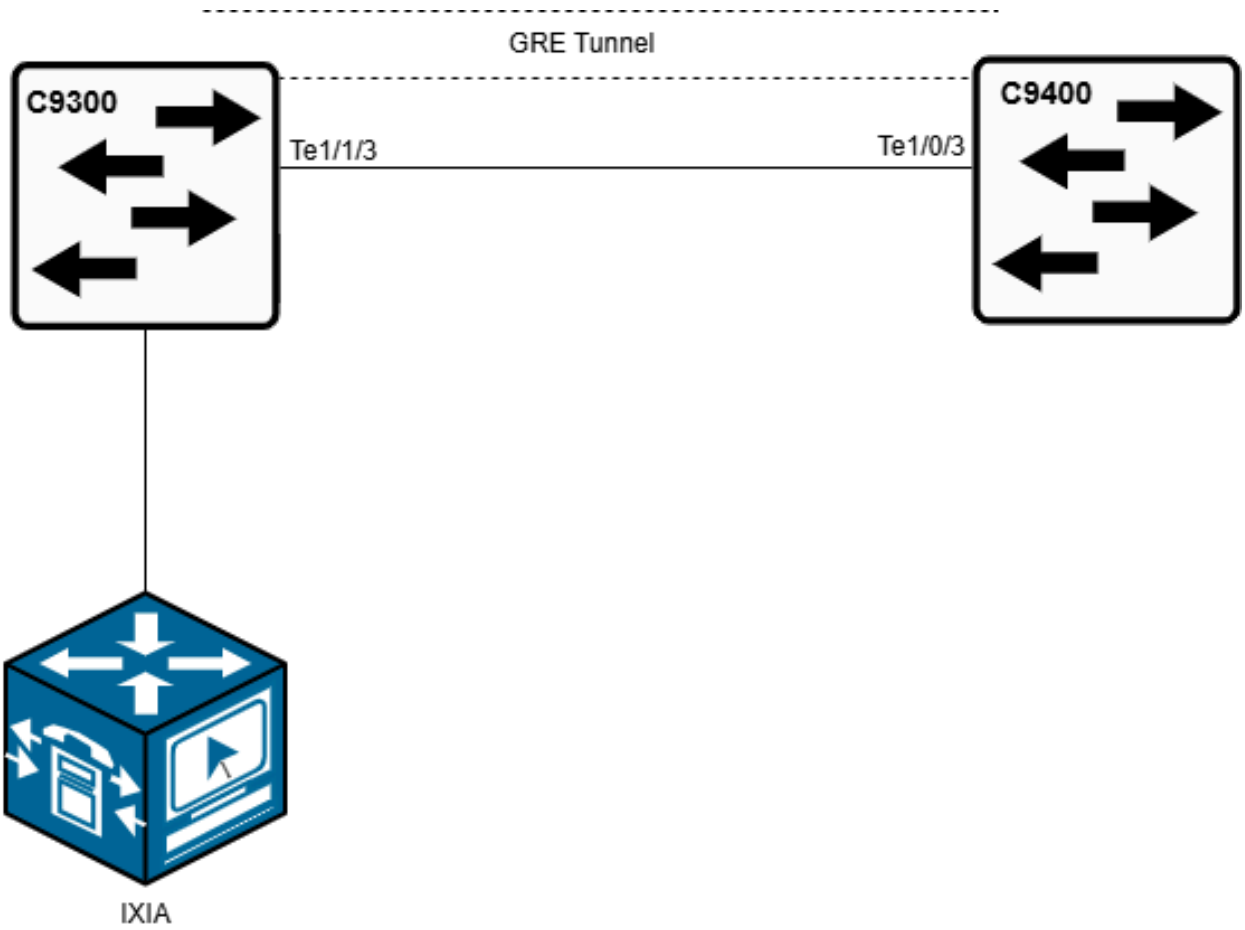
Topologie

La configuration se compose de commutateurs C9000 avec un générateur de trafic afin de reproduire le problème. Tests inclus pour une isolation plus poussée :

Condition 1 : Sans 'Null0' ou 'MSS adjust'
Condition 2 : Avec une route statique pointant vers Null0, aucun ajustement MSS
Condition 3 : Null0 et ajustement MSS activés

Versions logicielles et matérielles

- Catalyst 9300 et 9400 exécutant Cisco IOS XE 17.3.4 version
- IXIA pour générer du trafic



Configuration requise

- Aucun paramètre « ip tcp adjust-mss » ni aucune route « null0 » n'est configuré
- Avec seulement 'null0 route' configuré
- Avec 'ip tcp adjust-mss' et 'null0 route' configurés
  'ip tcp adjust-mss value' (valeur inférieure à l'unité de transmission maximale (MTU)) (sur l'interface de tunnel ou l'interface virtuelle de commutateur (SVI) (entrée))
  « ip route X.X.X.X X.X.X.X Null0 » (routes statiques pointant vers Null0)

Selon les conditions décrites, vous observez une connectivité intermittente aux homologues BGP (Border Gateway Protocol) connectés directement et aux interfaces SVI configurées sur le même périphérique ou sur des homologues connectés directement. Il y a également une augmentation constante des compteurs d'abandon dans la file d'attente de transfert du logiciel (SW) lors de l'exécution des commandes et des débogages CoPP (Control Plane Policing). L'enquête montre que le trafic destiné à Null0 est plutôt dirigé vers le processeur. Ce comportement a perturbé le protocole BGP en empêchant la connexion TCP en trois étapes. En outre, les requêtes ping vers les adresses IP SVI configurées sur le commutateur ont échoué.

Scénarios

Cas 1. Sans « Null0 » ou « MSS Adjust »

Si ni « ip tcp adjust-mss » ni « null route » n'est configuré, le compteur d'abandon dans la file d'attente de transfert du logiciel reste à « 0 » après le trafic généré à partir d'IXIA, comme prévu.

Reportez-vous aux journaux suivants :

```
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
```

Cas 2. Avec une route statique qui pointe vers Null0, aucun ajustement MSS

Lorsque seule la route Null0 est configurée, le compteur d'abandon de la file d'attente de transfert logicielle reste à « 0 » après le trafic généré à partir d'IXIA, comme prévu.

Reportez-vous aux journaux suivants :

```
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
```

Cas 3. 'Null0' et 'MSS Adjust' activés

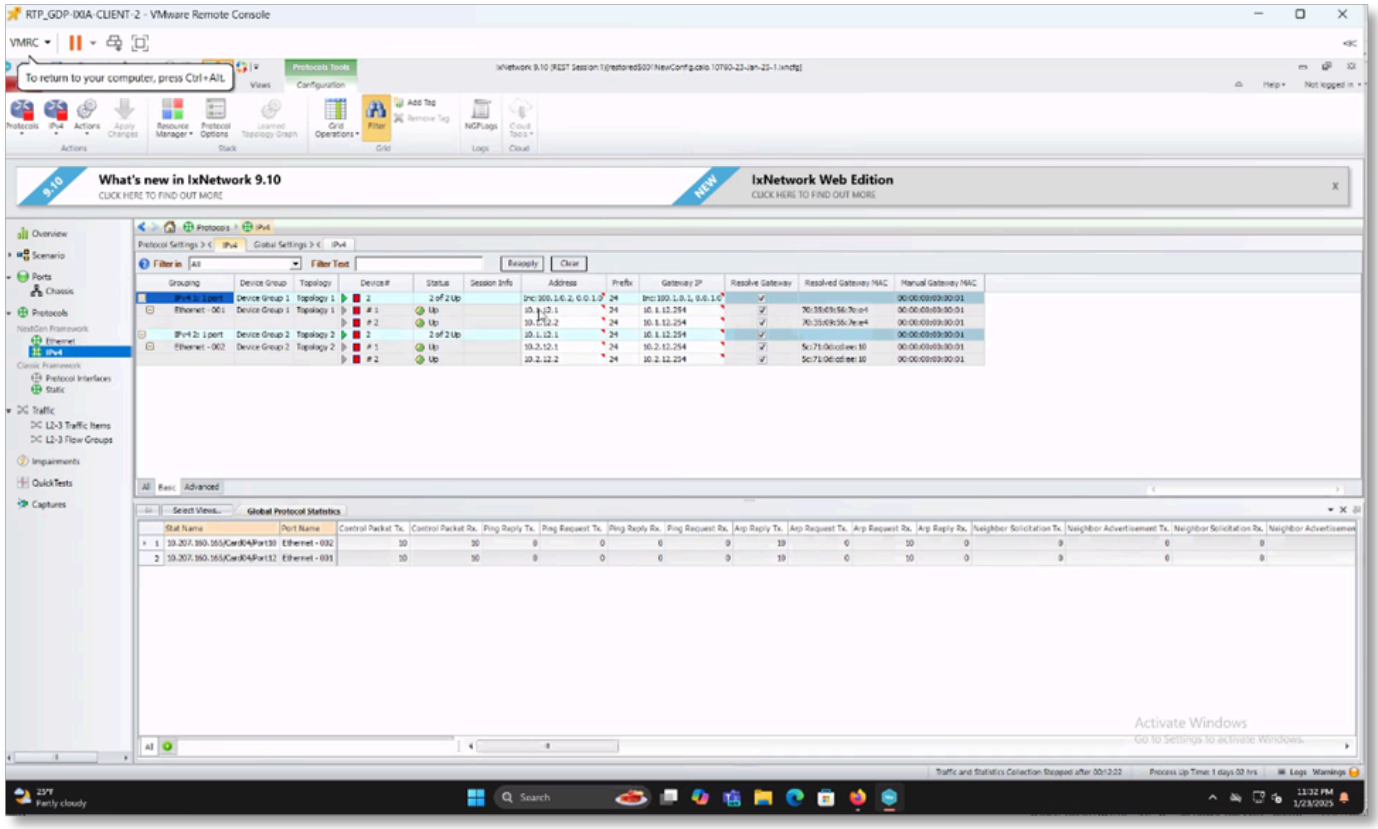
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
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
```

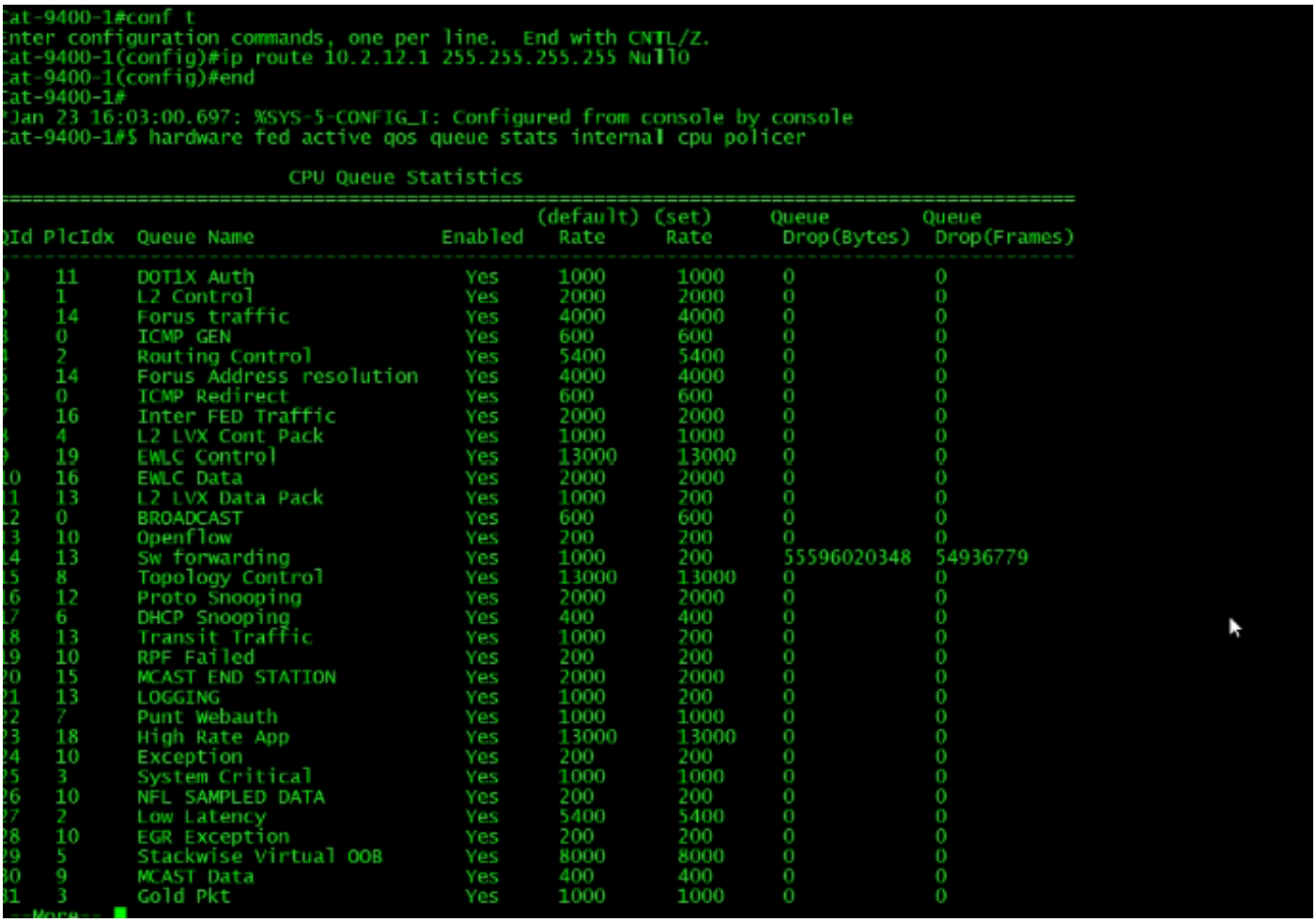
```
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

Une fois que les routes Null0 et MSS ont ajusté la configuration sur l'interface du tunnel d'entrée du C9400, le trafic a été généré à partir d'IXIA et le compteur d'abandon s'incrémente pour l'identité de file d'attente CPU (QID) 14, comme illustré dans l'image suivante.

IXIA



Sortie CoPP 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
```

Explication des routes statiques Null0 et du verrouillage MSS

Selon la théorie, afin de gérer le trafic indésirable tel que le trafic de diffusion ou de bloquer l'accès à des sous-réseaux spécifiques, une option consiste à configurer une route statique qui dirige le trafic vers Null0. Cela entraîne l'abandon par le routeur de tout trafic destiné à ce réseau.

Commande pour 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 syntaxe Null 0 garantit que le fichier 10.2.12.1/32 ne sera transféré nulle part. Ce qui signifie que tout trafic destiné au réseau de destination est rejeté (abandonné) à Null0.

MSS TCP

D'autre part, l'ajustement MSS TCP :

L’ajustement MSS modifie le MSS pour les paquets TCP. Lorsqu’une non-concordance de MTU se produit (souvent entre des périphériques avec des paramètres MTU différents ou via des tunnels tels que des VPN), les paquets peuvent être fragmentés.

La fragmentation n’est pas souhaitable pour le trafic TCP, car elle peut entraîner une perte de paquets ou une dégradation des performances. Le verrouillage MSS résout ce problème en ajustant la taille des segments TCP, en s'assurant que les paquets sont suffisamment petits pour tenir dans le MTU du chemin, et empêche ainsi la fragmentation. Lorsque l'ajustement MSS est appliqué aux interfaces de tunnel et aux SVI avec une valeur définie sur 1360 pour les connexions TCP, il garantit que la taille du segment est inférieure au MTU du chemin, ce qui empêche la fragmentation.

Scénario idéal

Null0 est une interface « black hole » virtuelle qui abandonne tout trafic dirigé vers elle. Il est utile d’empêcher les boucles de routage ou le trafic indésirable.
TCP MSS adjust est une commande qui garantit que les segments TCP sont suffisamment petits pour éviter la fragmentation lors du passage à travers des périphériques ou des tunnels avec des MTU plus petites.

Condition

Bien que ces deux fonctionnalités soient généralement utilisées à des fins différentes, elles peuvent toutes deux jouer un rôle dans la conception globale d’un réseau afin de gérer le flux de trafic, d’éviter la fragmentation et d’optimiser les performances. Cependant, sur les commutateurs Catalyst 9K, l'utilisation conjointe de Null0 et de MSS peut entraîner des conflits, surcharger le CPU et submerger la politique CoPP.

Vérification

```
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
```

À l'aide des commandes debug, vérifiez les journaux au format suivant afin d'identifier l'adresse IP des points de l'attaquant sur le CPU, même avec les routes Null0 configurées :

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

Déboguages

```
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
```

Conclusion

Afin d'éviter que les files d'attente de CPU ne soient saturées par le trafic indésirable et n'affectent la communication TCP/Secure Shell (SSH), bloquez ces adresses IP avant qu'elles n'atteignent les commutateurs Catalyst 9K ou supprimez le réglage MSS en entrée.

En général, le paquet SYN (TCP synchronize) est envoyé à la file d'attente du processeur. MSS est une option de l'en-tête TCP qui indique la taille maximale de segment que le récepteur peut

accepter, à l'exception des en-têtes TCP/IP. Il est généralement défini pour la connexion en trois étapes, en particulier dans le paquet SYN.

Afin de résoudre ce problème, géo-bloquez les adresses IP malveillantes sur le RADWARE/Security Gateway pour empêcher la file d'attente du contrôleur de CPU de devenir saturée et stabiliser l'appairage BGP et les connexions TCP.

Résolution

Une fois que les adresses IP malveillantes ont été bloquées sur la passerelle Radware/de sécurité, le trafic a cessé de saturer la file d'attente du processeur.

Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.