# Null0およびMSSのクランプのシナリオのトラブルシューティング

## 内容



## はじめに

このドキュメントでは、Catalyst 9Kで最大セグメントサイズ(MSS)調整を行い、Null 0を指すスタティックルートを設定することの影響について説明します。

## 前提条件

### 要件

次の項目に関する知識があることを推奨しています。

- TCPとMSSの調整に関する概念的な知識
- コントロールプレーンの転送とデバッグに関するCisco Catalyst 9Kのプラットフォームの理解

### 対応プラットフォーム

このドキュメントは、Cisco IOS® XE 17.3.x以降を実行するすべてのCatalyst 9000プラットフォームに適用されます。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS-XE 17.3.4バージョンが稼働するCatalyst 9300シリーズスイッチ
- IOS-XE 17.3.4バージョンが稼働するCatalyst 9400シリーズスイッチ
- トラフィック生成用のIXIA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## トラブルシューティングアプローチ

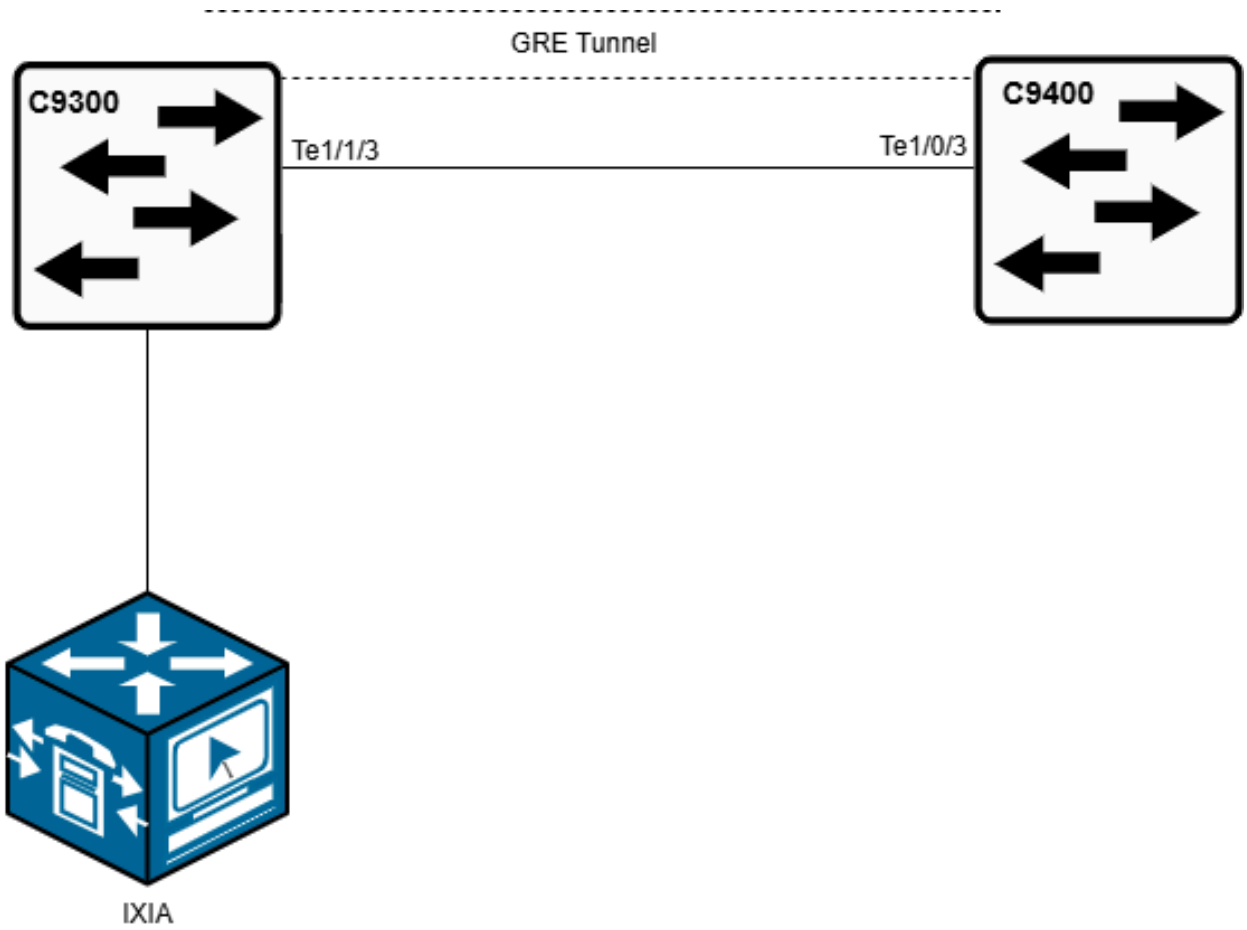
### トポロジ

この設定は、問題を再現するためのトラフィックジェネレータを備えたC9000スイッチで構成されています。さらなる分離のために含まれるテスト：

条件1: 'Null0'または'MSS調整'なし
条件2:Null0を指すスタティックルートを使用して、MSS調整を行わない
条件3: Null0とMSSの両方の調整が有効です

### ソフトウェアおよびハードウェアバージョン

- Cisco IOS XE 17.3.4バージョンを実行するCatalyst 9300および9400
- トラフィック生成用のIXIA




## 設定要件

- 「ip tcp adjust-mss」および「null0 route」が設定されていない
- 「null0 route」のみが設定されている
- 「ip tcp adjust-mss」および「null0 route」が設定されている
  「ip tcp adjust-mss value」(最大伝送ユニット(MTU)未満の値)(トンネルインターフェイスまたはスイッチ仮想インターフェイス(SVI)（入力）)
  「ip route X.X.X.X X.X.X.X Null0」（Null0を指すスタティックルート）

説明した条件に基づいて、直接接続されたボーダーゲートウェイプロトコル(BGP)ピア、および同じデバイスまたは直接接続されたピアで設定されたSVIへの接続が断続的になることが確認されます。また、コントロールプレーンポリシング(CoPP)コマンドおよびデバッグの実行中は、ソフトウェア(SW)のフォワーディングキューのドロップカウンタが増加し続けます。 調査によれば、Null0宛てのトラフィックはCPUに転送されます。この動作により、TCP 3ウェイハンドシェイクの完了が妨げられ、BGPプロトコルが中断されました。 さらに、スイッチに設定されているSVIのIPアドレスに対するpingが失敗しました。

## シナリオ

Case 1.'Null0'または'MSS Adjust'なし

「ip tcp adjust-mss」と「null route」のどちらも設定されていない場合、SW転送キューのドロップカウンタは、IXIAから生成されたトラフィックの後も予想通り「0」のままになります。

次のログを参照してください。

```
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
```

## Case 2.Null0を指すスタティックルートを使用して、MSS調整なし

Null0ルートのみが設定されている場合、IXIAから生成されたトラフィックの後、SW転送キューのドロップカウンタは期待どおりに「0」のままになります。

次のログを参照してください。

```
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
```

## Case 3.'Null0'と'MSS調整'の両方が有効

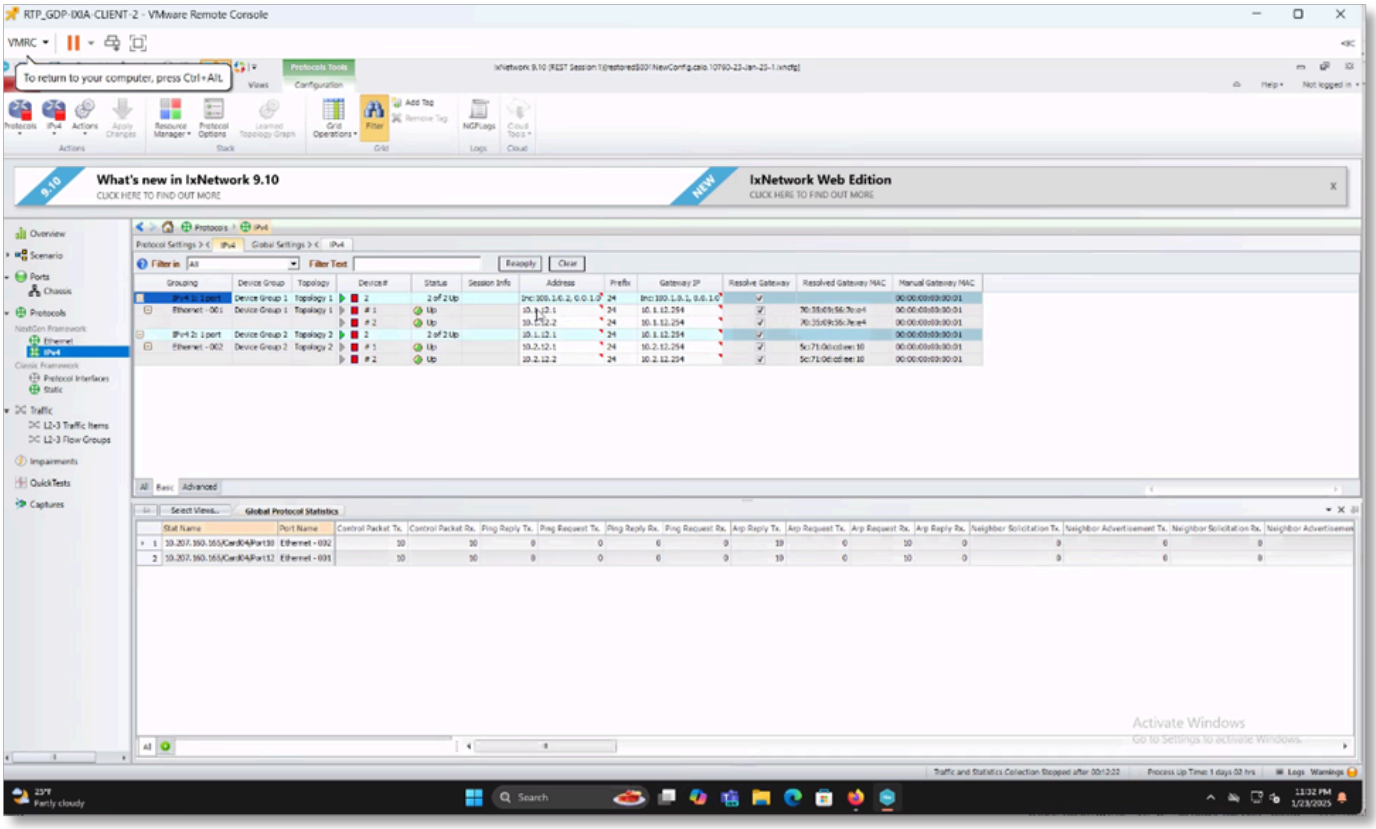
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
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
```

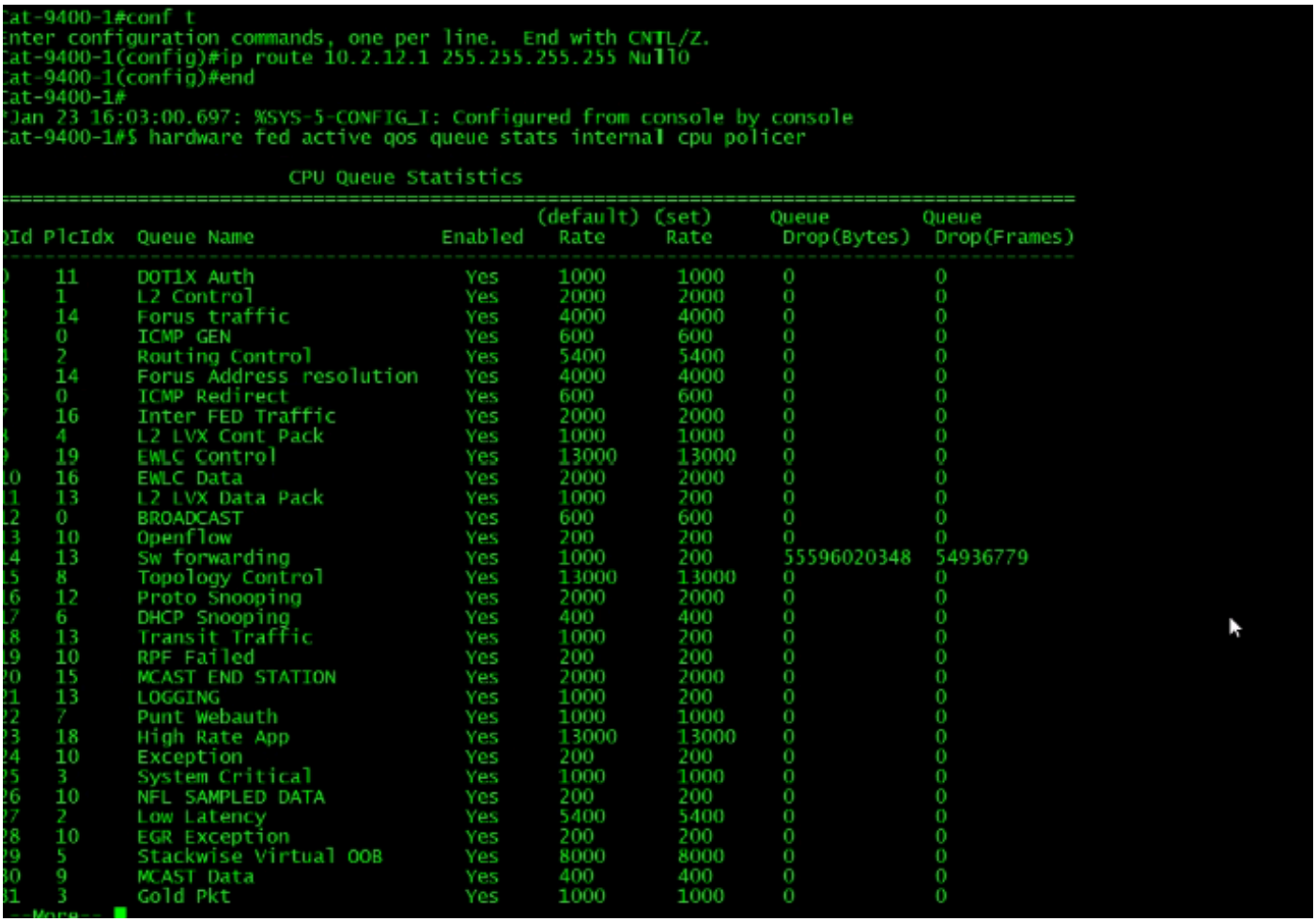
```
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

C9400の入力トンネルインターフェイスでNull0ルートとMSSの設定が調整された後、トラフィックはIXIAから生成され、次の図に示すようにCPUキューID(QID)14のドロップカウンタが増加します。

イクシア




C9400 CoPP出力：



```
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スタティックルートとMSSクランプの説明

理論的には、ブロードキャストトラフィックや特定のサブネットへのアクセスをブロックするなどの不要なトラフィックを処理するには、トラフィックをNull0に転送するスタティックルートを設定するという選択肢があります。これにより、ルータはそのネットワーク宛てのトラフィックを廃棄します。

## Null0のコマンド

```
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構文は、10.2.12.1/32がどこにも転送されないことを保証します。つまり、宛先ネットワーク宛てのトラフィックはNull0で廃棄（ドロップ）されます。

## TCP MSS

一方、TCP MSS調整：

MSSの調整により、TCPパケットのMSSが変更されます。 MTUの不一致が発生すると（多くの場合、MTU設定が異なるデバイス間またはVPNなどのトンネルを通じて）、パケットがフラグメント化される可能性があります。

フラグメンテーションは、パケットの損失やパフォーマンスの低下を引き起こす可能性があるため、TCPトラフィックには望ましくありません。MSSクランプでは、TCPセグメントのサイズを調整し、パケットがパスMTU内に収まるように十分小さくなるようにすることで、この問題に対処し、フラグメンテーションを防止します。 MSS調整をトンネルインターフェイスとSVIに適用し、TCP接続の値を1360に設定すると、セグメントサイズがパスMTUより小さくなり、フラグメンテーションが防止されます。

### 理想的なシナリオ

Null0は仮想「ブラックホール」インターフェイスで、このインターフェイスに向かうトラフィックはすべて廃棄されます。ルーティングループや不要なトラフィックを防ぐのに便利です。
TCP MSS adjustは、より小さなMTUのデバイスまたはトンネルを通過する際に、フラグメンテーションを回避できるほどTCPセグメントを小さくするコマンドです。

## 条件

これらの2つの機能は、通常はさまざまな目的で使用されますが、トラフィックフローの管理、フラグメンテーションの回避、およびパフォーマンスの最適化を行うために、ネットワーク設計全体で両方とも役割を果たすことができます。ただし、Catalyst 9Kスイッチでは、Null0とMSSの両方の調整を一緒に使用すると、競合が発生し、CPUが過負荷になり、CoPPポリシーが圧迫される可能性があります。

## 検証

```
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コマンドを使用して、次の形式でログをチェックし、Null0ルートが設定されていても、攻撃者がCPUにパントするIPアドレスを特定します。

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

# デバッグ

```
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
```

# 結論

CPUキューが不要なトラフィックによって過大な負荷を受け、TCP/Secure Shell(SSH)通信に影響を与えないようにするには、これらのIPアドレスがCatalyst 9Kスイッチに到達する前にそれらをブロックするか、入力時にMSS調整を削除します。

通常、TCP同期(SYN)パケットはCPUキューにパントされます。MSSは、TCP/IPヘッダーを除き、受信側が受け入れ可能な最大セグメントサイズ(MSS)を示すTCPヘッダー内のオプションです。通常は3ウェイハンドシェイクに対して、特にSYNパケット内に設定されます。

この問題を解決するには、RADWARE/Security Gatewayで悪意のあるIPをジオブロックして、CPUポリサーキューが過負荷になるのを防ぎ、BGPピアリングとTCP接続を安定させます。

## 解決方法

悪意のあるIPがRadware/セキュリティゲートウェイで正常にブロックされると、トラフィックがCPUキューを圧倒しなくなりました。

## 関連情報

- https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/222338-troubleshoot-tcp-slowness-issues-due-to.html
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。