

使用Null0和MSS夹排除故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[支持的平台](#)

[使用的组件](#)

[故障排除方法](#)

[拓扑](#)

[软件和硬件版本](#)

[配置要求](#)

[场景](#)

[案例1.不使用“Null0”或“MSS Adjust”](#)

[案例2.使用静态路由指向Null0，无MSS调整](#)

[案例3.同时启用“Null0”和“MSS Adjust”](#)

[IXIA](#)

[Null0静态路由和MSS钳位的说明](#)

[Null0命令](#)

[TCP MSS](#)

[理想情景](#)

[条件](#)

[确认](#)

[调试](#)

[结论](#)

[分辨率](#)

[相关信息](#)

简介

本文档介绍在Catalyst 9K上使用最大分段大小(MSS)调整和指向Null 0的静态路由的意义。

先决条件

要求

Cisco 建议您了解以下主题：

- 有关TCP和MSS调整的概念知识
- 平台了解Cisco Catalyst 9K，用于控制平面转发和调试。

支持的平台

本文档适用于运行Cisco IOS® XE 17.3.x及更高版本的所有Catalyst 9K平台。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行IOS-XE 17.3.4版的Catalyst 9300系列交换机
- 运行IOS-XE 17.3.4版的Catalyst 9400系列交换机
- 用于生成流量的IXIA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除方法

拓扑

设置包含带流量发生器的C9000交换机，用于重现问题。包含用于进一步隔离的测试：

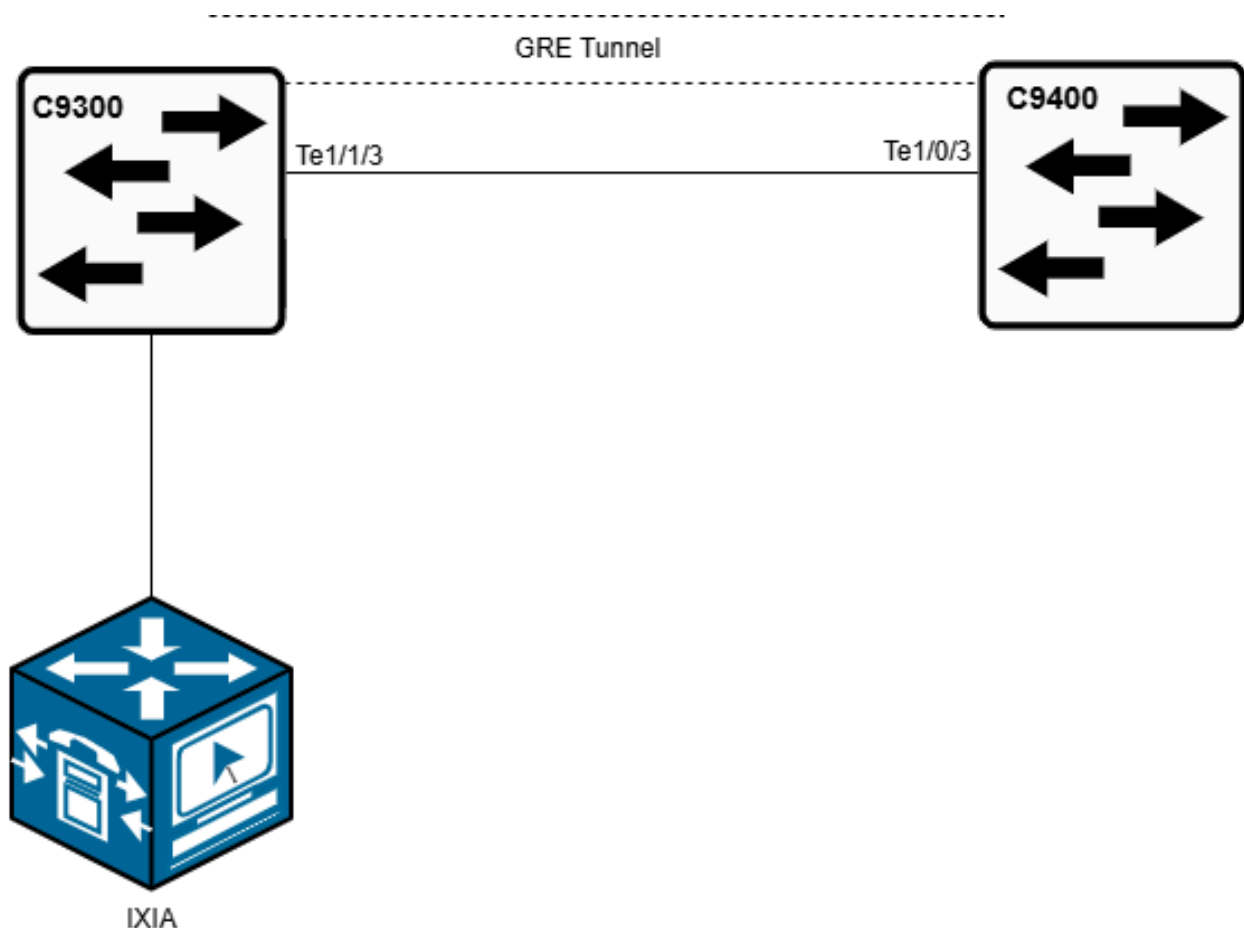
条件1:不使用“Null0”或“MSS adjust”

条件2:对于指向Null0的静态路由，无MSS调整

条件3:Null0和MSS调整均启用

软件和硬件版本

- 运行Cisco IOS XE 17.3.4版的Catalyst 9300和9400
- 用于生成流量的IXIA



配置要求

- 未配置“ip tcp adjust-mss”和“null0路由”
- 仅配置了“null0路由”
- 配置了“ip tcp adjust-mss”和“null0路由”

'ip tcp adjust-mss value'(小于最大传输单位(MTU)的值)(在隧道接口或交换机虚拟接口(SVI)上 (入口))

'ip route X.X.X.X X.X.X Null0' (指向Null0的静态路由)

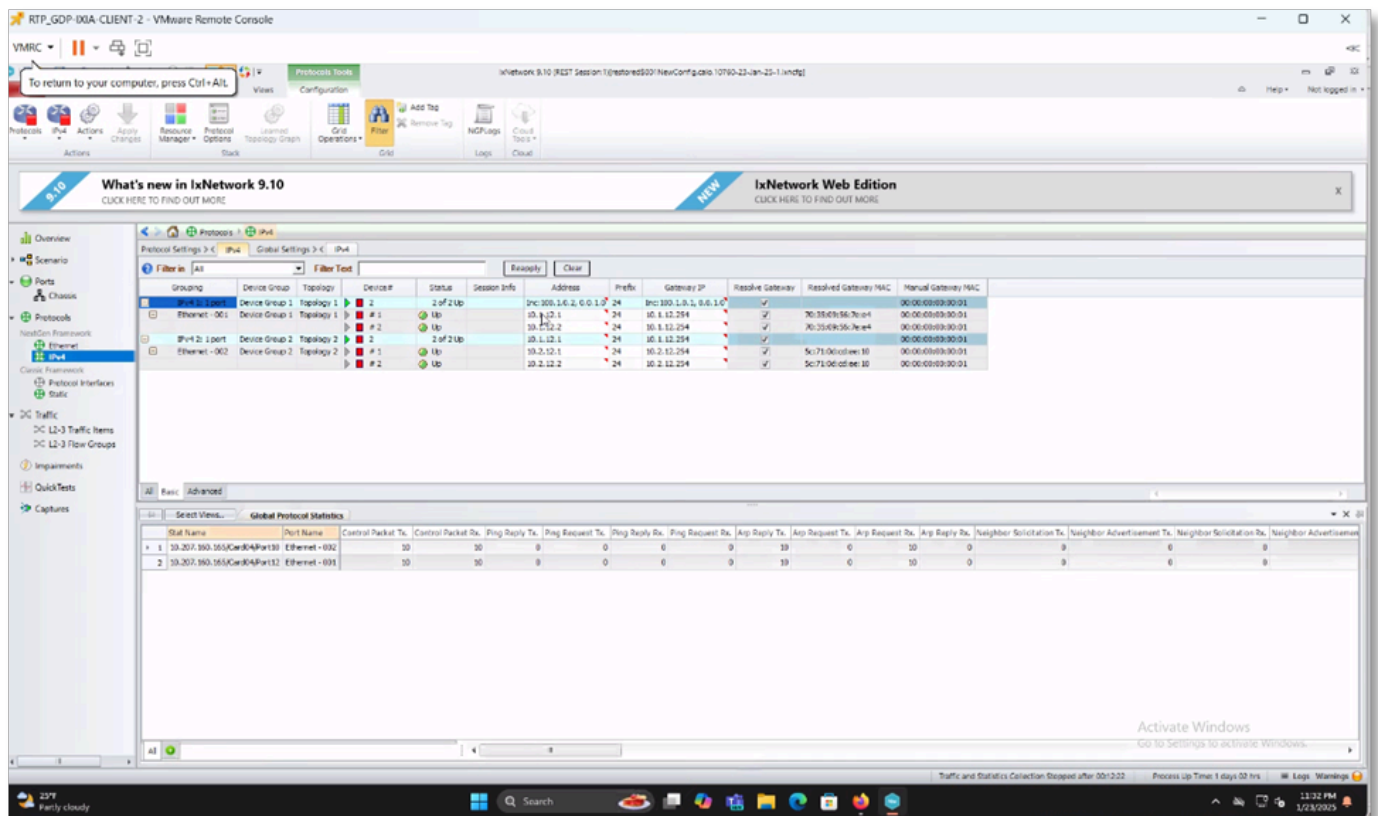
根据所述的条件，您会观察到与直接连接的边界网关协议(BGP)对等体以及与同一设备上或直接连接对等体上配置的SVI的间歇性连接。在运行控制平面策略(CoPP)命令和调试时，软件(SW)转发队列中的丢弃计数器也会一致增加。调查显示指向Null0的流量将改为指向CPU。此行为通过阻止TCP三次握手完成，中断了BGP协议。此外，对交换机上配置的SVI IP地址执行ping操作失败。

场景

案例1.不使用“Null0”或“MSS Adjust”

如果未配置“ip tcp adjust-mss”或“null route”，则在从IXIA生成流量后，SW转发队列中的丢弃计数器将如预期一样保留为“0”。

请参阅以下日志：



C9400 CoPP输出：

```

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
=====
Qid PlCidx Queue Name Enabled (default) (set) Queue Drop(Bytes) Queue 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静态路由和MSS钳位的说明

根据理论，为了处理不需要的流量（例如广播流量或阻止对特定子网的访问），一个选项是设置静

态路由，将流量定向到Null0。这会导致路由器丢弃任何预定用于该网络的流量。

Null0命令

```
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语法确保不会将10.2.12.1/32转发到任何位置。这意味着在Null0处丢弃（丢弃）所有发往目的网络的流量。

TCP MSS

另一方面，TCP MSS调整：

MSS调整会修改TCP数据包的MSS。当发生MTU不匹配时（通常是在具有不同MTU设置的设备之间或通过VPN等隧道），可以对数据包进行分段。

TCP流量不需要分段，因为它可能导致数据包丢失或性能下降。MSS钳位通过调整TCP段的大小来解决此问题，确保数据包足够小以便适合路径MTU，从而防止分段。当MSS调整应用于隧道接口和SVI（对于TCP连接，其值设置为1360）时，它确保段大小小于路径MTU，从而防止分段。

理想情景

Null0是虚拟“黑洞”接口，可丢弃任何指向它的流量。它有助于防止路由环路或不需要的流量。TCP MSS adjust命令用于确保TCP数据段足够小，以便通过具有较小MTU的设备或隧道时避免分段。

条件

虽然这两种功能通常用于不同的目的，但它们在整体网络设计中均可发挥作用，以便管理流量、避免分段和优化性能。但是，在Catalyst 9K交换机上，同时使用Null0和MSS调整可能会导致冲突、超载CPU并使CoPP策略不堪重负。

确认

```
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
```

使用debug命令，检查下一个格式的日志，以标识攻击者在CPU上发送的IP地址，即使已配置了Null0路由：

```
----- 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
```

调试

```
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: 0x00000002e]
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: 0x00000002e]
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: 0x00000002e]
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
```

结论

为了防止CPU队列被不需要的流量淹没，并影响TCP/安全外壳(SSH)通信，请在这些IP地址到达Catalyst 9K交换机之前阻止它们，或者删除入口上的MSS调整。

通常，TCP同步(SYN)数据包会传送到CPU队列。MSS是TCP报头中的一个选项，指示接收方可以接受的最大数据段大小，但TCP/IP报头除外。它通常设置为三次握手，特别是在SYN数据包中。

为了解决此问题，请对RADWARE/安全网关上的恶意IP进行地理阻塞，以防止CPU监察器队列变得不堪重负，并稳定BGP对等和TCP连接。

分辨率

在Radware/安全网关上成功阻止恶意IP后，流量停止并会超过CPU队列。

相关信息

- <https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/222338-troubleshoot-tcp-slowness-issues-due-to.html>
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。