Fehlerbehebung bei Szenarien mit Null0- und MSS-Klemmung

Inhalt

Einleitung

In diesem Dokument werden die Auswirkungen einer Anpassung der maximalen Segmentgröße (Maximum Segment Size, MSS) und statischer Routen beschrieben, die auf Catalyst 9000 auf Null zeigen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Konzeptkenntnisse über TCP- und MSS-Anpassung
- Plattformverständnis von Cisco Catalyst 9000 für die Weiterleitung und Fehlerbehebung auf Kontrollebene.

Unterstützte Plattformen

Dieses Dokument gilt für alle Catalyst 9000-Plattformen mit Cisco IOS® XE 17.3.x und höher.

Verwendete Komponente

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Switches der Serie 9300 mit IOS-XE 17.3.4
- Catalyst Switches der Serie 9400 mit IOS-XE 17.3.4
- IXIA zur Generierung von Datenverkehr

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Fehlerbehebung

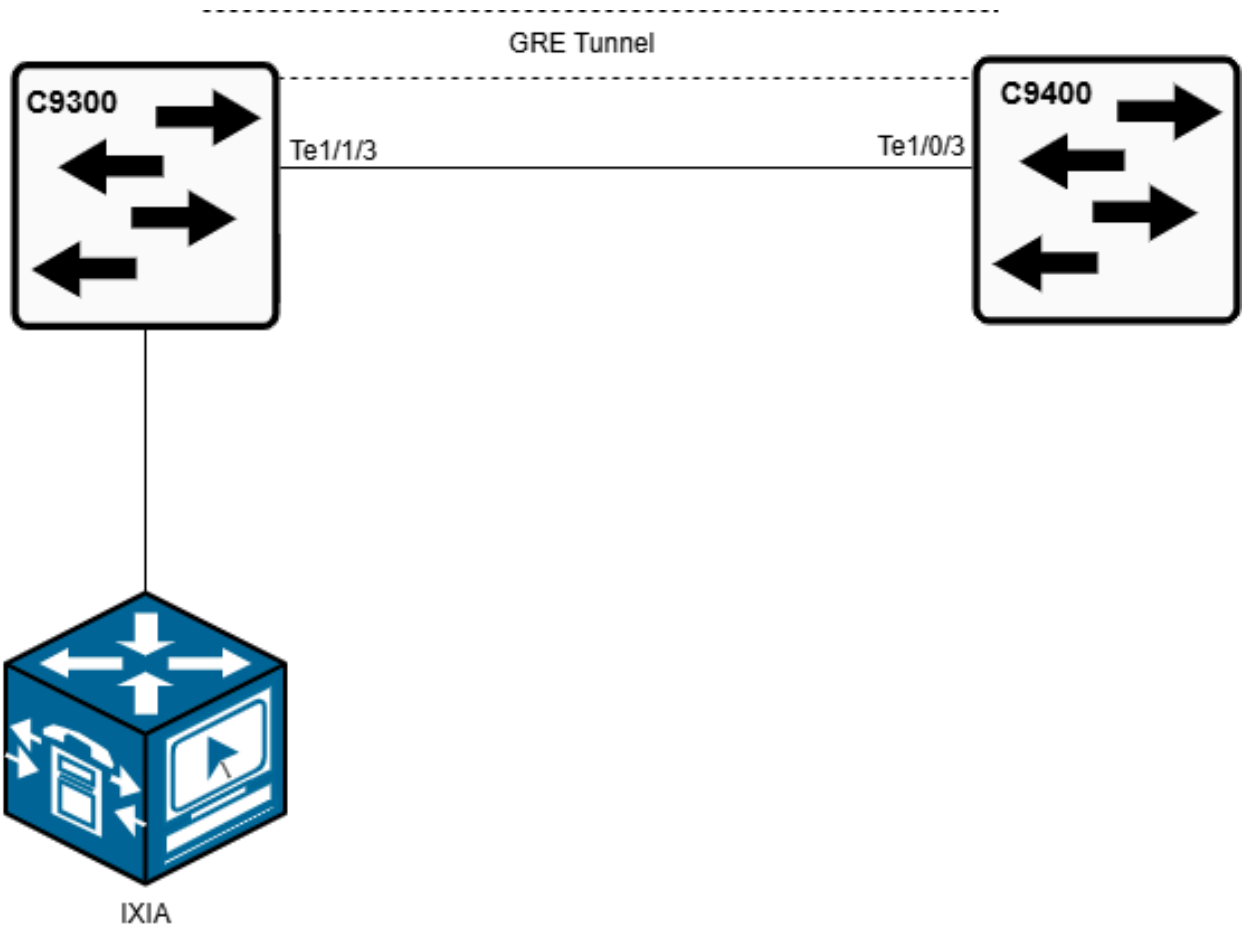
Topologie

Die Konfiguration besteht aus C900-Switches mit einem Datenverkehrsgenerator, um das Problem zu reproduzieren. Tests für weitere Isolierung enthalten:

Bedingung 1: Ohne 'Null0' oder 'MSS anpassen'
Bedingung 2: Mit einer statischen Route, die auf Null0 zeigt, keine MSS-Anpassung
Bedingung 3: Sowohl Null0 als auch MSS-Anpassung aktiviert

Software- und Hardwareversionen

- Catalyst 9300 und 9400 mit Cisco IOS XE 17.3.4
- IXIA zur Generierung von Datenverkehr



Konfigurationsanforderungen

- Keine "ip tcp adjust-mss" und keine "null0 route" konfiguriert
- Nur "null0 route" konfiguriert
- Bei Konfiguration von "ip tcp adjust-mss" und "null0 route"
  'ip tcp adjust-mss value' (Wert kleiner als Maximum Transmission Unit (MTU)) (On Tunnel Interface oder Switch Virtual Interface (SVI) (Eingang))
  'ip route X.X.X.X.X.X Null0' (Statische Routen zeigen auf Null0)

Basierend auf den beschriebenen Bedingungen beobachten Sie eine zeitweilige Verbindung zu direkt verbundenen Border Gateway Protocol (BGP)-Peers und zu SVIs, die auf demselben Gerät oder auf direkt verbundenen Peers konfiguriert sind. Es gibt auch eine konsistente Zunahme an Drop-Zählern in der Software (SW) Forwarding-Warteschlange, während Control Plane Policing (CoPP)-Befehle ausgeführt und Debug-Vorgänge ausgeführt werden. Untersuchungen zeigen, dass Datenverkehr, der für Null0 bestimmt ist, stattdessen an die CPU weitergeleitet wird. Durch dieses Verhalten wurde das BGP-Protokoll unterbrochen, da der TCP-3-Wege-Handshake nicht abgeschlossen werden konnte. Außerdem sind Pings an die auf dem Switch konfigurierten SVI-IP-Adressen fehlgeschlagen.

Szenarien

Fall 1: Ohne 'Null0' oder 'MSS Adjust'

Wenn weder "ip tcp adjust-mss" noch "null route" konfiguriert ist, bleibt der Zähler für das Verwerfen von Nachrichten in der SW-Weiterleitungswarteschlange erwartungsgemäß auf "0", nachdem der Datenverkehr von IXIA generiert wurde.

Verweisen Sie auf folgende Protokolle:

```
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
```

Fall 2: Statische Route verweist auf Null0, keine MSS-Anpassung

Wenn nur die Null0-Route konfiguriert ist, bleibt der Zähler für das Verwerfen von Nachrichten in der SW-Weiterleitungswarteschlange erwartungsgemäß bei '0', nachdem der Datenverkehr von IXIA generiert wurde.

Verweisen Sie auf folgende Protokolle:

```
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
```

Fall 3: 'Null0' und 'MSS Adjust' aktiviert

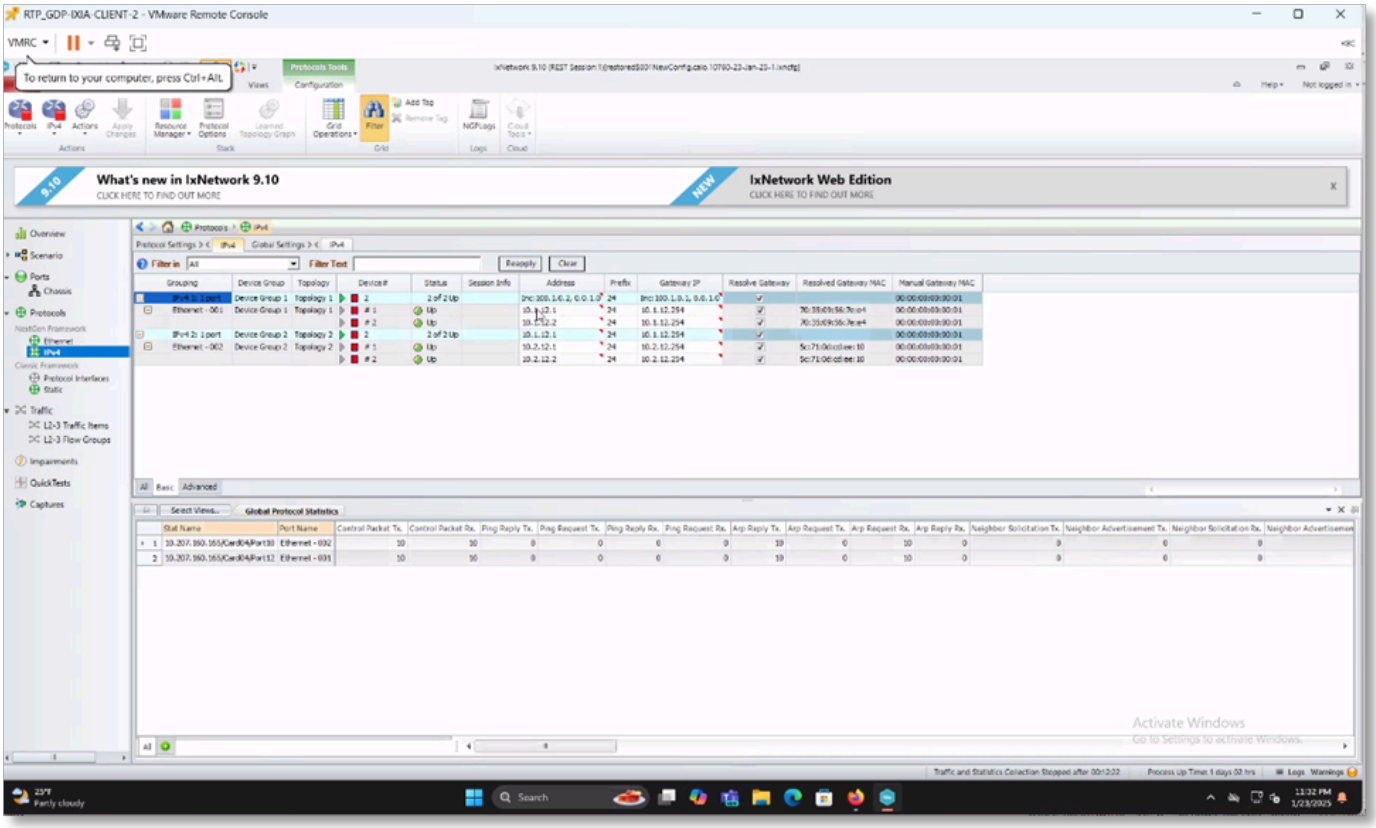
```
With both "ip tcp adjust-mss" and a "null route" configured:
```

```
Configuration:

On Cat 9300:
Cat-9300-1#show run interface twoGigabitEthernet 1/0/1
interface TwoGigabitEthernet1/0/1 (Interface connected to IXIA)
no switchport
```

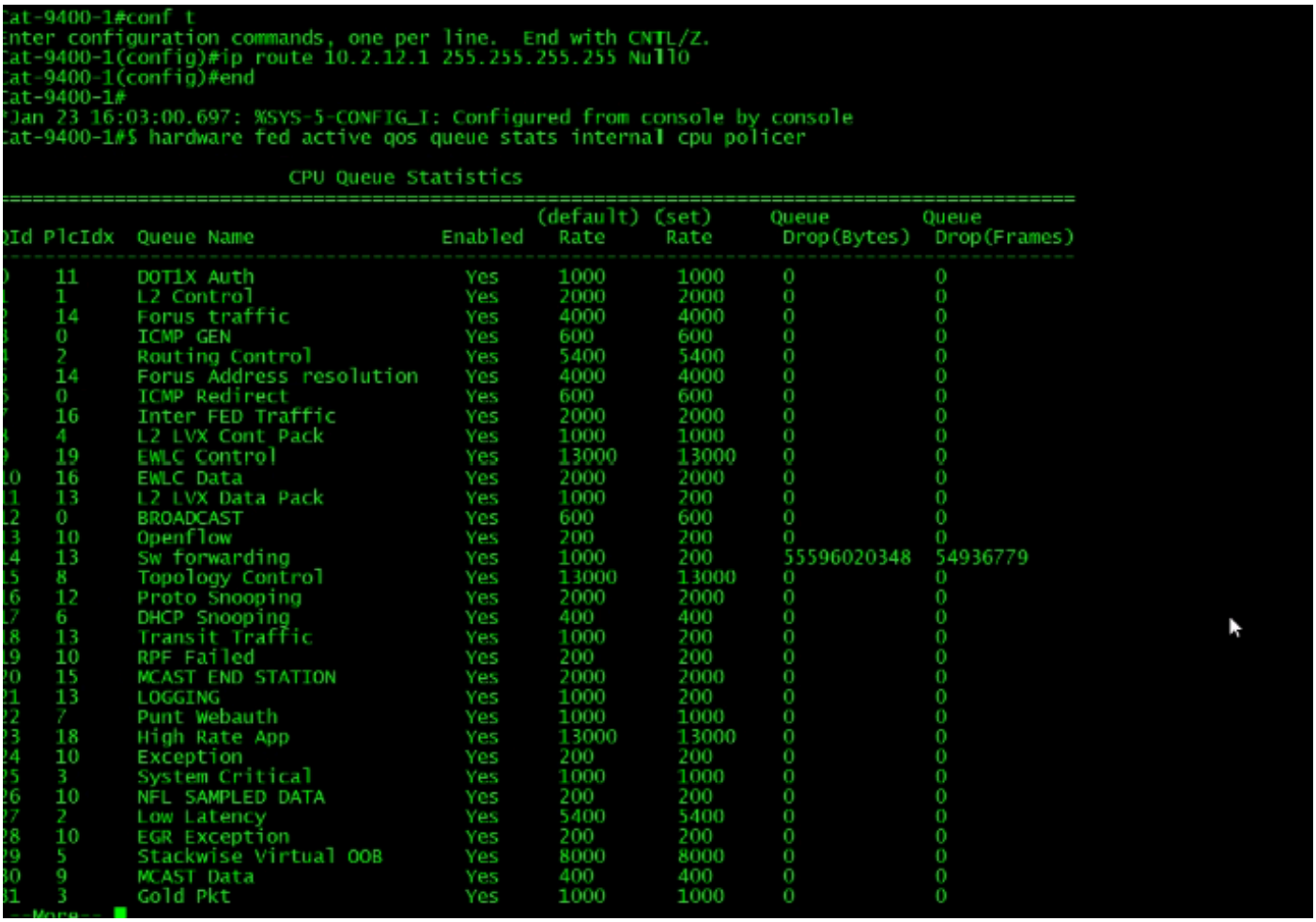
```
ip address 10.1.12.xx 255.255.255.0
end
Cat-9300-1#show run interface tenGigabitEthernet 1/1/3
interface TenGigabitEthernet1/1/3 (Physical interface connected to C9400)
no switchport
mtu 9000
ip address 203.63.147.xx 255.255.255.0
no ip redirects
no ip unreachables
ip mtu 1500
load-interval 30
end

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
```

Nachdem Null0-Routen und MSS die Konfiguration an der Eingangstunnel-Schnittstelle des C9400 angepasst hatten, wurde Datenverkehr von IXIA generiert, und der Zähler für das Löschen wird für die CPU-Warteschlangenidentität (QID) 14 inkrementiert, wie im nächsten Bild gezeigt.

IXIA



C9400 CoPP-Ausgabe:



```
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
```

Erläuterung von statischen Null0-Routen und MSS-Klemmung

Um unerwünschten Datenverkehr wie Broadcast-Datenverkehr oder den Blockzugriff auf bestimmte Subnetze zu verarbeiten, besteht eine Option laut Theorie darin, eine statische Route einzurichten, die den Datenverkehr auf Null0 umleitet. Dies führt dazu, dass der Router den für dieses Netzwerk vorgesehenen Datenverkehr verwirft.

Befehl für 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
```

Mit der Null-0-Syntax wird sichergestellt, dass 10.2.12.1/32 nirgends weitergeleitet wird. Das bedeutet, dass jeglicher Datenverkehr, der für das Zielnetzwerk bestimmt ist, bei Null0 verworfen (verworfen) wird.

TCP-MSS

TCP-MSS-Anpassung:

Durch die MSS-Anpassung wird die MSS für TCP-Pakete geändert. Tritt eine MTU-Diskrepanz auf - häufig zwischen Geräten mit unterschiedlichen MTU-Einstellungen oder über Tunnel wie VPNs - können Pakete fragmentiert werden.

Eine Fragmentierung ist für den TCP-Datenverkehr unerwünscht, da sie zu Paketverlusten oder Leistungseinbußen führen kann. MSS-Klemmung löst dieses Problem, indem die Größe der TCP-Segmente angepasst wird, sichergestellt wird, dass die Pakete klein genug sind, um in die Pfad-MTU zu passen, und somit eine Fragmentierung verhindert wird. Wenn MSS-Anpassung auf Tunnelschnittstellen und SVIs mit einem Wert von 1360 für TCP-Verbindungen angewendet wird, wird sichergestellt, dass die Segmentgröße kleiner ist als die Pfad-MTU, wodurch eine Fragmentierung verhindert wird.

Ideales Szenario

Null0 ist eine virtuelle Schnittstelle mit schwarzen Löchern, die jeglichen darauf gerichteten Datenverkehr verwirft. Es ist hilfreich, Routing-Schleifen oder unerwünschten Datenverkehr zu verhindern.
TCP MSS adjust ist ein Befehl, der sicherstellt, dass die TCP-Segmente klein genug sind, um eine Fragmentierung zu vermeiden, wenn sie Geräte oder Tunnel mit kleineren MTUs passieren.

Bedingung

Diese beiden Funktionen werden im Allgemeinen für unterschiedliche Zwecke verwendet. Sie können jedoch beide in einem umfassenden Netzwerkdesign eine Rolle spielen, um den Datenverkehrsfluss zu verwalten, eine Fragmentierung zu vermeiden und die Leistung zu optimieren. Bei Catalyst Switches der Serie 9000 kann die Verwendung von Null0 und einer MSS-Anpassung jedoch zu Konflikten, einer Überlastung der CPU und einer Überlastung der CoPP-Richtlinie führen.

Verifizierung

```
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
```

Überprüfen Sie mithilfe der Debug-Befehle die Protokolle im nächsten Format, um die IP-Adresse der Angreifer zu identifizieren, die auf die CPU durchsucht werden, selbst wenn die Null0-Routen konfiguriert sind:

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

Fehlerbehebung

```
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
```

Schlussfolgerung

Um zu verhindern, dass CPU-Warteschlangen durch unerwünschten Datenverkehr überlastet werden und die TCP/Secure Shell (SSH)-Kommunikation beeinträchtigen, sperren Sie diese IP-Adressen, bevor sie die Catalyst Switches der Serie 9K erreichen, oder entfernen Sie die MSS-

Anpassung beim Eintritt.

Normalerweise wird das TCP-Synchronisierungspaket (SYN) an die CPU-Warteschlange gesendet. MSS ist eine Option im TCP-Header, die die maximale Segmentgröße angibt, die der Empfänger akzeptieren kann, außer TCP/IP-Headern. Er wird normalerweise für den 3-Wege-Handshake eingestellt, insbesondere im SYN-Paket.

Um dieses Problem zu beheben, sperren Sie die schädlichen IPs auf dem RADWARE/Security Gateway, um zu verhindern, dass die CPU-Richtlinienwarteschlange überlastet wird, und stabilisieren Sie BGP-Peering und TCP-Verbindungen.

Auflösung

Sobald schädliche IPs auf dem Radware/Security-Gateway erfolgreich blockiert wurden, wurde die CPU-Warteschlange nicht mehr durch den Datenverkehr überlastet.

Zugehörige Informationen

- https://www.cisco.com/c/en/us/support/docs/ip/transmission-control-protocol-tcp/222338-troubleshoot-tcp-slowness-issues-due-to.html
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.