Problemen met TCP-vertraging als gevolg van MSS-aanpassing in Catalyst 9K-Switches oplossen

Inhoud

Inleiding

Dit document beschrijft hoe een Catalyst 9K Switch de TCP MSS-aanpassing uitvoert en hoe TCP-traagheid aan deze functie is gekoppeld.

Informatie over TCP MSS-aanpassing

De aanpassingsfunctie Transmission Control Protocol (TCP) Maximum Segment Size (MSS) maakt de configuratie van de maximale segmentgrootte voor tijdelijke pakketten die een router oversteken mogelijk, met name TCP-segmenten met de SYN-bitset. Het`ip tcp adjust-mss`bevel wordt gebruikt op de wijze van de interfaceconfiguratie om de waarde MSS op de middenrouter van de pakketten te specificeren SYN om beknotting te vermijden.

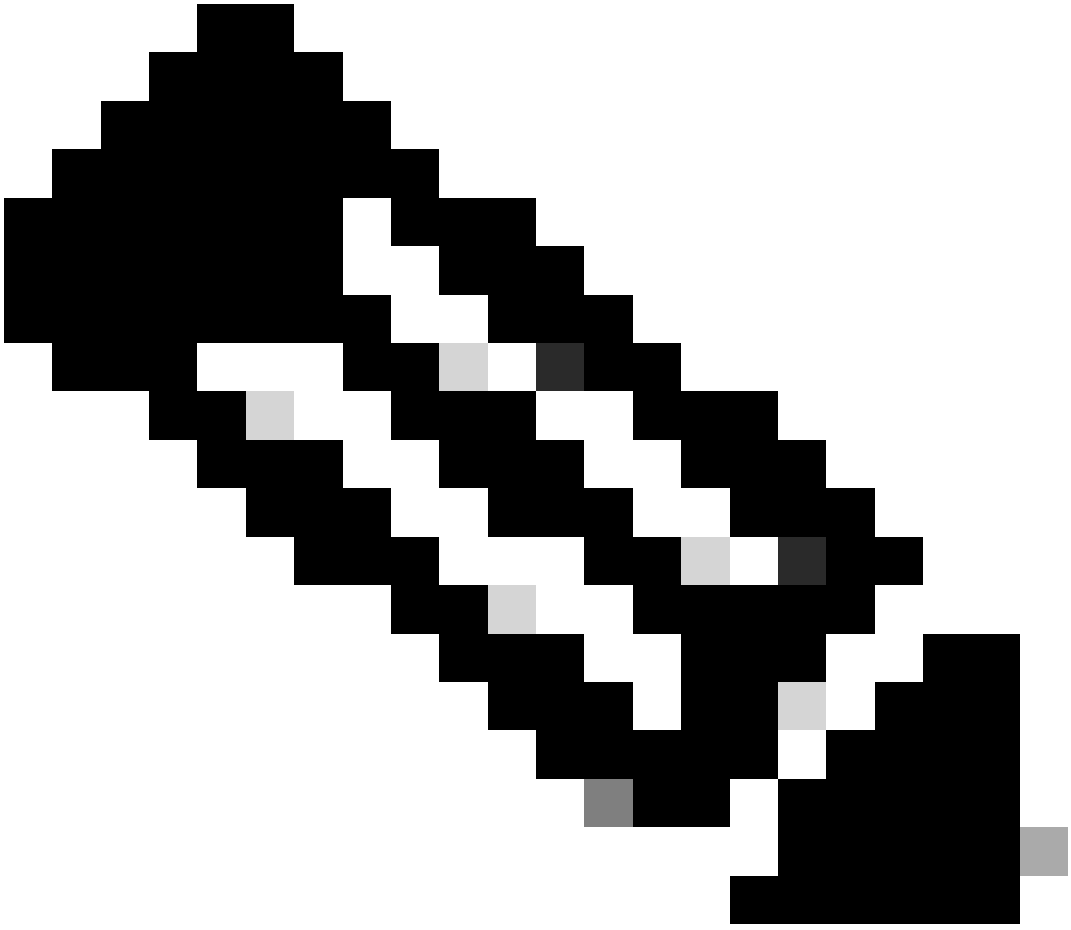
Wanneer een host (meestal een PC) een TCP sessie met een server start, bespreekt het de IP segmentgrootte met behulp van het MSS optieveld in het TCP SYN pakket. De configuratie MTU op de host bepaalt de waarde van het MSS veld. De standaard MTU waarde voor een NIC van de PC is 1500 bytes met een TCP MSS waarde van 1460 (1500 bytes - 20 bytes IP header - 20 bytes TCP header).

De PPP over Ethernet (PPPoE)-standaard ondersteunt een MTU van slechts 1492 bytes.

De discrepantie tussen de host en de grootte van PPPoE MTU kan ertoe leiden dat de router tussen de host en de server 1500-bytepakketten laat vallen en TCP-sessies via het PPPoE-netwerk beëindigt.

Zelfs als het pad MTU (dat de juiste MTU over het pad detecteert) is ingeschakeld op de host, kunnen sessies worden verbroken omdat systeembeheerders soms het Internet Control Message Protocol (ICMP)-foutmeldingen uitschakelen die van de host moeten worden doorgegeven om MTU te laten werken.

De opdracht ip tcp adjust-mss helpt voorkomen dat TCP-sessies worden gedropt door de MSS waarde van de TCP/SYN-pakketten aan te passen. De opdracht Aanpassen-mss van IP TCP is alleen effectief voor TCP-verbindingen die door de router worden doorgegeven. In de meeste gevallen is de optimale waarde voor het max-segment-size argument van de ip tcp adjust-mss opdracht 1452 bytes.
Deze waarde plus de 20-byte IP-header, de 20-byte TCP-header en de 8-byte PPPoE-header worden toegevoegd aan een 1500-byte pakket dat overeenkomt met de MTU-grootte voor de Ethernet-link.



Opmerking: op TCP MSS-aanpassing gebaseerd verkeer is software switched in Catalyst 9K Switches. Dit document verklaart scenario's waarin wordt aangenomen dat het op TCP/MSS-aanpassing gebaseerde verkeer softwareswitched is. Raadpleeg de Configuratiehandleiding om te bevestigen of een specifieke HW/SW-software het op

---

TCP/MSS-aanpassing gebaseerde verkeer switches.

Gedrag

Zoals eerder vermeld, is TCP MSS op aanpassing gebaseerd verkeer altijd software-switched. Dit betekent dat als u TCP-aanpassing probeert uit te voeren, de Switch het TCP-verkeer naar de CPU stuurt voor de MSS-wijziging.

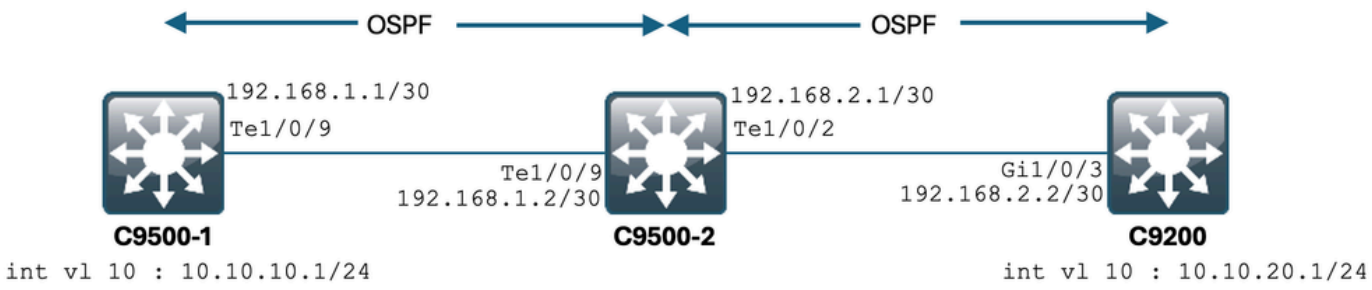
Als u bijvoorbeeld de TCP MSS-waarde op een interface wijzigt, wordt al het TCP-verkeer dat op die interface wordt ontvangen, gestraft naar de CPU.
De CPU verandert vervolgens de MSS-waarde en verstuurt het verkeer naar de gewenste interface waar het TCP-pakket naartoe ging.

Om deze reden, als er een enorme hoeveelheid TCP-verkeer met MSS-aanpassing, dan dit overbelast de CPU-wachtrij.
Wanneer een CPU-wachtrij is overbelast, controleert de Control Plane Policer (COPP) het verkeer en laat pakketten vallen om de wachtrij te handhaven. Hierdoor worden de TCP-pakketten gedropt.

Vandaar dat er problemen zoals traagheid van bestandsoverdracht, het creëren van SSH-sessies en traagheid van Citrix-toepassing (bij gebruik van TCP) worden gezien.

Hier is een voorbeeld uit de praktijk van hoe dit gebeurt.

Topologie



Scenario

U gaat naar SSH in de C9200 van de C9500-1.
SSH met C950-1 VLAN 10 (10.10.10.1) als bron.
De bestemming van de SSH is VLAN 20 van C9200 (10.10.20.1/24).
SSH is op TCP gebaseerd, vandaar dat elke traagheid in TCP ook van invloed is op deze SSH-sessie.

Er is een transit L3 Switch (C9500-2) tussen C9500-1 en C9200.
Er zijn twee transit/30 L3 verbindingen, één tussen C9500-1 en C9500-2, en één tussen C9500-2 en C9200.
OSPF wordt gebruikt voor bereikbaarheid via alle drie de Switches en alle/30-subnetten en SVI's worden geadverteerd in OSPF.
Alle IP's die eerder worden getoond, zijn onderling bereikbaar.

In C9500-2 Te1/0/9 wordt de TCP MSS-waarde aangepast.
Wanneer SSH vanaf de C9500-1 wordt gestart, vindt een TCP 3-weg handshake plaats.
Het SYN-pakket raakt de C9500-2 Te1/0/9 (Ingress), waar de TCP MSS-aanpassing wordt uitgevoerd.

Eerste configuratie en gedrag

Er is een EPC-opname op C9500-2 Te1/0/9 (beide richtingen) genomen en de SSH is gestart van C9500-1 tot C9200.

Hier is de EPC - configuratie:

```
C9500-2#show monitor capture mycap
Status Information for Capture mycap
Target Type:
Interface: TenGigabitEthernet1/0/9, Direction: BOTH
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 80
File Details:
File not associated
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)
C9500-2#
```

De EPC wordt gestart:

```
C9500-2#monitor capture mycap start
Started capture point : mycap
C9500-2#
```

De SSH starten van C9500-1 tot C9200:

```
C9500-1#ssh -l admin 10.10.20.1
Password:
```

Stoppen met de EPC:

```
C9500-2#monitor capture mycap stop
Capture statistics collected at software:
Capture duration - 6 seconds
Packets received - 47
Packets dropped - 0
Packets oversized - 0
Bytes dropped in asic - 0
Capture buffer will exists till exported or cleared
Stopped capture point : mycap
C9500-2#
```

En dit zijn de door de EPC opgenomen pakketten:

```
C9500-2#show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
1 0.000000 10.10.10.1 -> 10.10.20.1 TCP 60 44274 -> 22 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2 0.001307 10.10.20.1 -> 10.10.10.1 TCP 60 22 -> 44274 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=536
3 0.001564 10.10.10.1 -> 10.10.20.1 TCP 60 44274 -> 22 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4 0.003099 10.10.20.1 -> 10.10.10.1 SSH 73 Server: Protocol (SSH-2.0-Cisco-1.25)
5 0.003341 10.10.10.1 -> 10.10.20.1 SSH 73 Client: Protocol (SSH-2.0-Cisco-1.25)
6 0.003419 10.10.10.1 -> 10.10.20.1 TCP 118 [TCP segment of a reassembled PDU]
7 0.003465 10.10.10.1 -> 10.10.20.1 TCP 118 44274 -> 22 [ACK] Seq=84 Ack=20 Win=4109 Len=64 [TCP segmen
8 0.003482 10.10.10.1 -> 10.10.20.1 TCP 118 44274 -> 22 [ACK] Seq=148 Ack=20 Win=4109 Len=64 [TCP segme
9 0.003496 10.10.10.1 -> 10.10.20.1 TCP 118 44274 -> 22 [ACK] Seq=212 Ack=20 Win=4109 Len=64 [TCP segme
10 0.003510 10.10.10.1 -> 10.10.20.1 TCP 118 44274 -> 22 [ACK] Seq=276 Ack=20 Win=4109 Len=64 [TCP segm
11 0.003525 10.10.10.1 -> 10.10.20.1 TCP 118 44274 -> 22 [ACK] Seq=340 Ack=20 Win=4109 Len=64 [TCP segm
12 0.004719 10.10.20.1 -> 10.10.10.1 TCP 60 22 -> 44274 [ACK] Seq=20 Ack=84 Win=4045 Len=0
~ Output Cut ~
```

Je kunt de TCP handdruk zien gebeuren in pakketnummer 1.2.3.
Packet nr. 1 is het SYN-pakket.
Je kunt zien dat het een MSS-waarde van 536 heeft.
Het SYN, ACK pakket (Packet No.2) wordt ook gezien komend van C9200 met een MSS waarde van 536.
Hier blijft de MSS-waarde intact en wordt deze niet gewijzigd door de Switch.

Gedrag na TCP/MSS-aanpassing

Hier is de TCP MSS aanpassingsconfiguratie op C9500-2 Te1/0/9:

```
C9500-2#sh run int te1/0/9
Building configuration...
Current configuration : 119 bytes
!
interface TenGigabitEthernet1/0/9
no switchport
ip address 192.168.1.2 255.255.255.252
ip tcp adjust-mss 512 ------------------> Here we are changing the MSS value to 512.
```

Neem nu een EPC-opname op C9500-2 Te1/0/9 (beide richtingen) en start SSH van C9500-1 tot C9200.

Hier is de EPC - configuratie:

```
C9500-2#show monitor capture mycap
Status Information for Capture mycap
Target Type:
Interface: TenGigabitEthernet1/0/9, Direction: BOTH
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 80
File Details:
File not associated
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Maximum number of packets to capture per second: 1000
Packet sampling rate: 0 (no sampling)
C9500-2#
```

Start de opname, SSH van C9500-1 tot C9200, en stop de opname.

Hier zijn de CPU-opgenomen pakketten:

```
C9500-2#show monitor capture mycap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
1 0.000000 b8:a3:77:ec:ba:f7 -> 01:00:0c:cc:cc:cc CDP 398 Device ID: C9500-1.cisco.com Port ID: TenGiga
2 0.636138 10.10.10.1 -> 10.10.20.1 TCP 60 53865 -> 22 [SYN] Seq=0 Win=4128 Len=0 MSS=536
3 0.637980 10.10.20.1 -> 10.10.10.1 TCP 60 22 -> 53865 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=512
4 0.638214 10.10.10.1 -> 10.10.20.1 TCP 60 53865 -> 22 [ACK] Seq=1 Ack=1 Win=4128 Len=0
5 0.639997 10.10.20.1 -> 10.10.10.1 SSH 73 Server: Protocol (SSH-2.0-Cisco-1.25)
6 0.640208 10.10.10.1 -> 10.10.20.1 SSH 73 Client: Protocol (SSH-2.0-Cisco-1.25)
7 0.640286 10.10.10.1 -> 10.10.20.1 TCP 118 [TCP segment of a reassembled PDU]
8 0.640341 10.10.10.1 -> 10.10.20.1 TCP 118 53865 -> 22 [ACK] Seq=84 Ack=20 Win=4109 Len=64 [TCP segmen
9 0.640360 10.10.10.1 -> 10.10.20.1 TCP 118 53865 -> 22 [ACK] Seq=148 Ack=20 Win=4109 Len=64 [TCP segme
10 0.640375 10.10.10.1 -> 10.10.20.1 TCP 118 53865 -> 22 [ACK] Seq=212 Ack=20 Win=4109 Len=64 [TCP segm
11 0.640390 10.10.10.1 -> 10.10.20.1 TCP 118 53865 -> 22 [ACK] Seq=276 Ack=20 Win=4109 Len=64 [TCP segm
12 0.640410 10.10.10.1 -> 10.10.20.1 TCP 118 53865 -> 22 [ACK] Seq=340 Ack=20 Win=4109 Len=64 [TCP segm
```

```
~ Output Cut ~
```

Je kan de TCP handdruk zien gebeuren in pakketnummer 2.3.4.
Packet nr. 2 is het SYN-pakket.
Je kunt zien dat het een MSS-waarde van 536 heeft.
Maar het SYN, ACK pakket (Packet No.3) wordt gezien komend van C9200 met een waarde van MSS van 512.
Dit komt doordat wanneer het SYN-pakket de C9500-2 Te1/0/9 bereikt, het wordt verzonden naar de C9500-2 CPU voor TCP MSS wijziging van 536 naar 512.
De CPU van de C9500-2 verandert de MSS in 512 en verstuurt het SYN-pakket vanuit Te1/0/2 naar C9200.
Dan gebruiken alle volgende TCP-transacties dezelfde aangepaste MSS-waarde.

Laten we nu eens diep nadenken over hoe het SYN-pakket door de Switch gaat en hoe de MSS-wijziging plaatsvindt.
Zodra dit SYN-pakket de interface van de C9500-2 bereikt, wordt het naar de CPU verzonden voor MSS-wijziging.
Het gaat eerst door de FED (waar je het kunt opnemen), en dan naar de CPU (waar je het ook kunt opnemen).

Laten we eerst een FED Punt-opname nemen op C9500-2.

Hier is de configuratie van het FED punt:

```
C9500-2#debug platform software fed switch 1 punt packet-capture buffer limit 16384
Punt PCAP buffer configure: one-time with buffer size 16384...done
```

Het FED punt beginnen te vatten:

```
C9500-2#debug platform software fed switch 1 punt packet-capture start
Punt packet capturing started.
```

De SSH starten van C9500-1 tot C9200:

```
C9500-1#ssh -l admin 10.10.20.1
Password:
```

Stop het FED-punt om vast te leggen:

```
C9500-2#debug platform software fed switch 1 punt packet-capture stop
Punt packet capturing stopped. Captured 3 packet(s)
```

En hier zijn de pakketjes van het FED-punt:

```
C9500-2#show platform software fed switch active punt packet-capture brief
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 3 packets. Capture capacity : 16384 packets

------ Punt Packet Number: 1, Timestamp: 2024/07/31 01:29:46.373 ------
interface : physical: TenGigabitEthernet1/0/9[if-id: 0x00000040], pal: TenGigabitEthernet1/0/9 [if-id: 
metadata : cause: 55 [For-us control], sub-cause: 0, q-no: 4, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: 0100.5e00.0005, src mac: b8a3.77ec.baf7
ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 224.0.0.5, src ip: 192.168.1.1
ipv4 hdr : packet len: 100, ttl: 1, protocol: 89

------ Punt Packet Number: 2, Timestamp: 2024/07/31 01:29:47.432 ------
interface : physical: TenGigabitEthernet1/0/9[if-id: 0x00000040], pal: TenGigabitEthernet1/0/9 [if-id: 
metadata : cause: 11 [For-us data], sub-cause: 1, q-no: 14, linktype: MCP_LINK_TYPE_IP [1]
ether hdr : dest mac: 00a3.d144.4bf7, src mac: b8a3.77ec.baf7
ether hdr : ethertype: 0x0800 (IPv4)
ipv4 hdr : dest ip: 10.10.20.1, src ip: 10.10.10.1
ipv4 hdr : packet len: 44, ttl: 254, protocol: 6 (TCP)
tcp hdr : dest port: 22, src port: 35916

------ Punt Packet Number: 3, Timestamp: 2024/07/31 01:29:48.143 ------
interface : physical: TenGigabitEthernet1/0/1[if-id: 0x00000009], pal: TenGigabitEthernet1/0/1 [if-id: 
metadata : cause: 96 [Layer2 control protocols], sub-cause: 0, q-no: 1, linktype: MCP_LINK_TYPE_LAYER2
ether hdr : dest mac: 0100.0ccc.cccc, src mac: 78bc.1a27.c203
ether hdr : length: 443
```

Je kunt zien dat Packet No. 2 het TCP SYN-pakket is van 10.10.10.1 tot 10.10.20.1, dat binnenkomt van Te1/0/9.
Het 'q-nee' is hier van belang. Je kunt zien dat de regering wachtrij nr. 14 kiest om van de FED naar de CPU te gaan.

Hier zie je alle 32 wachtrijen voor verkeer om van de FED naar de CPU te gaan:

```
C9500-2#show platform hardware fed switch 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 1000 0 0
12 0 BROADCAST Yes 600 600 0 0
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 0 0
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 1000 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 1000 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
```

Zoals u overhead kunt zien, is wachtrij nr. 14 de 'Sw Forwarding'-wachtrij.
In dit geval wordt deze wachtrij door het TCP-verkeer gebruikt om naar de CPU te worden gestraft.

Laten we nu een CPU (Control-Plane) vastleggen op de C9500-2.

Hier is de CPU-opnameconfiguratie:

```
C9500-2#sh mon cap test
Status Information for Capture test
Target Type:
Interface: Control Plane, Direction: BOTH
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 80
File Details:
File not associated
Limit Details:
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)
C9500-2#
```

U start de opname, SSH van C9500-1 tot C9200, en stopt de opname.

Hier zijn de CPU-opgenomen pakketten:

```
C9500-2#show monitor capture test buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
1 0.000000 00:a3:d1:44:4b:81 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
2 0.000010 00:a3:d1:44:4b:a3 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
3 0.000013 00:a3:d1:44:4b:a4 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
4 0.000016 00:a3:d1:44:4b:a6 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
5 0.000019 00:a3:d1:44:4b:a7 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
6 0.000022 00:a3:d1:44:4b:a8 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost = 0
7 0.055470 c0:8b:2a:04:f0:6c -> 01:80:c2:00:00:0e LLDP 117 TTL = 120 SysName = bgl18-cx-amx-b02-2.cisco
9 0.220331 28:63:29:20:31:39 -> 00:01:22:53:74:20 0x3836 30 Ethernet II
10 0.327316 192.168.1.1 -> 224.0.0.5 OSPF 114 Hello Packet
11 0.442986 c0:8b:2a:04:f0:68 -> 01:80:c2:00:00:0e LLDP 117 TTL = 120 SysName = bgl18-cx-amx-b02-2.cisc
12 1.714121 10.10.10.1 -> 10.10.20.1 TCP 60 23098 -> 22 [SYN] Seq=0 Win=4128 Len=0 MSS=536
13 1.714375 10.10.10.1 -> 10.10.20.1 TCP 60 [TCP Out-Of-Order] 23098 -> 22 [SYN] Seq=0 Win=4128 Len=0 M
14 2.000302 00:a3:d1:44:4b:81 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost =
15 2.000310 00:a3:d1:44:4b:a3 -> 01:80:c2:00:00:00 STP 60 RST. Root = 32768/1/00:a3:d1:44:4b:80 Cost =
~ Output Cut ~
```

Packet nr. 12 is het TCP/SYN-pakket dat in de CPU (punt) komt, met de standaard MSS-waarde van 536.
Packet nr. 13 is het TCP/SYN-pakket dat door de CPU (injecteren) wordt verzonden, na de MSS-waarde te hebben gewijzigd in 512.

U kunt ook een snelle CPU debug maken om deze verandering te zien plaatsvinden.

Hier is de CPU-debugconfiguratie:

```
C9500-2#debug ip tcp adjust-mss
TCP Adjust Mss debugging is on
```

De SSH starten van C9500-1 tot C9200:

```
C9500-1#ssh -l admin 10.10.20.1
Password:
```

Voorkomen dat CPU debug:

```
C9500-2#undebug all
All possible debugging has been turned off
```

Kijkend naar de logboeken voor debugs:

```
C9500-2#show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0 overruns, xml disabl
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 230 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
File logging: disabled
Persistent logging: disabled
No active filter modules.
Trap logging: level informational, 210 message lines logged
Logging Source-Interface: VRF Name:
TLS Profiles:
Log Buffer (102400 bytes):
*Jul 31 01:46:32.052: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:32.893: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:36.136: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:41.318: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:42.412: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:43.254: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:43.638: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:45.783: TCPADJMSS: Input (process)
*Jul 31 01:46:45.783: TCPADJMSS: orig_mss = 536 adj mss = 512 src_ip = 10.10.10.1 dest_ip = 10.10.20.1
*Jul 31 01:46:45.783: TCPADJMSS: paktype = 0x7F83C7BCBF78
*Jul 31 01:46:50.456: TCPADJMSS: process_enqueue_feature
*Jul 31 01:46:51.985: TCPADJMSS: process_enqueue_feature
C9500-2#
```

U kunt zien dat de originele MSS waarde van 536 wordt aangepast aan 512.

Ten slotte kunt u een EPC-opname maken op C9200 Gi1/0/3 om te bevestigen dat het TCP SYN-pakket inderdaad met een MSS van 512 komt.

Hier is de EPC - configuratie:

```
C9200#sh mon cap mycap
Status Information for Capture mycap
Target Type:
Interface: GigabitEthernet1/0/3, Direction: BOTH
Status : Inactive
Filter Details:
Capture all packets
Buffer Details:
Buffer Type: LINEAR (default)
Buffer Size (in MB): 80
Limit Details:
Number of Packets to capture: 0 (no limit)
```

```
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packet sampling rate: 0 (no sampling)
C9200#
```

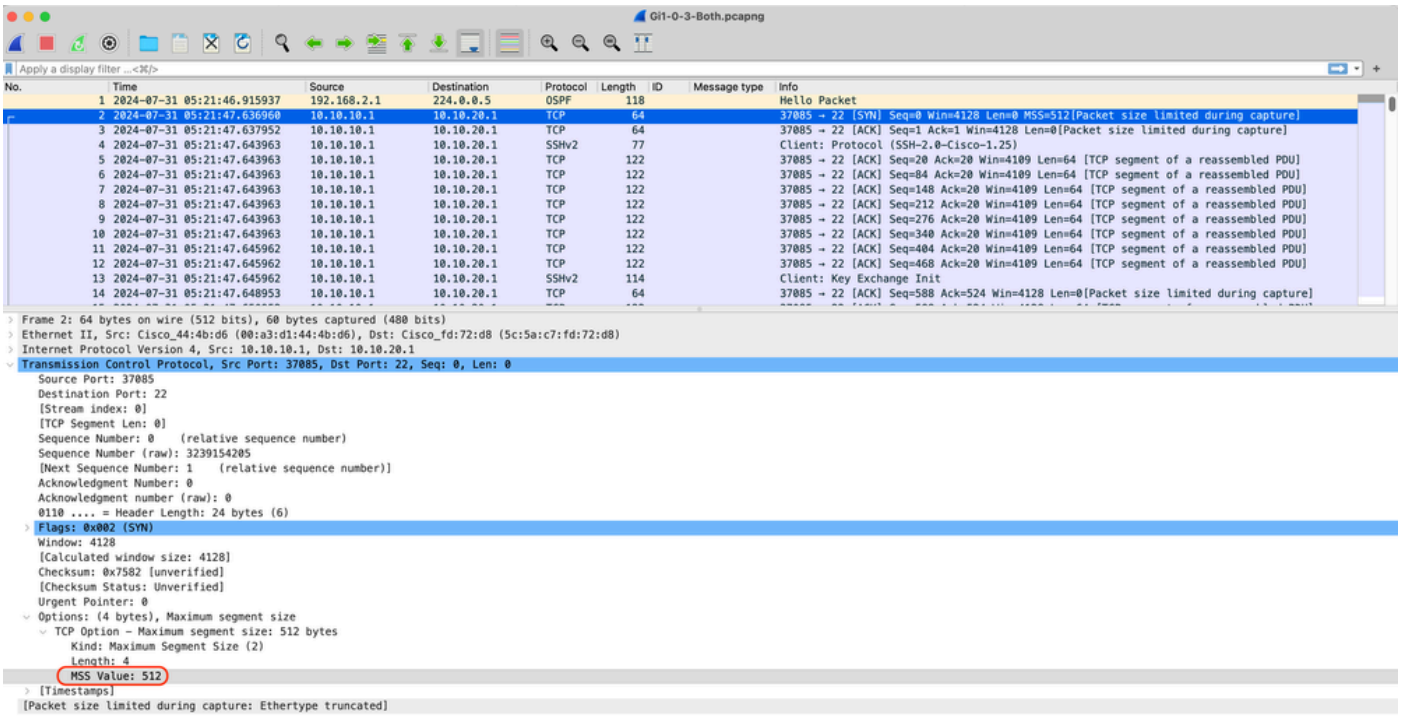
U start de opname, SSH van C9500-1 tot C9200, en stopt de opname.

Hier zijn de CPU-opgenomen pakketten:

```
C9200#sh mon cap mycap buff br
----------------------------------------------------------------------------
# size timestamp source destination dscp protocol
----------------------------------------------------------------------------
0 118 0.000000 192.168.2.1 -> 224.0.0.5 48 CS6 OSPF
1 64 0.721023 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
2 64 0.722015 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
3 77 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
4 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
5 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
6 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
7 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
8 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
9 122 0.728026 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
10 122 0.730025 10.10.10.1 -> 10.10.20.1 48 CS6 TCP
~ Output Cut ~
```

In C9200 kunt u de pakketdetails niet zien zoals in Wireshark, alleen de korte en hexadecimale details zijn beschikbaar.
Daarom kunt u de eerdere pakketten exporteren naar een pcap bestand in de flitser.
C9200#mon cap mycap export flash:Gi1-0-3-Both.pcapng
Met succes geëxporteerd

Vervolgens kunt u dit bestand via TFTP naar uw lokale pc kopiëren en het bestand in Wireshark openen.
Hier is de Wireshark-opname.



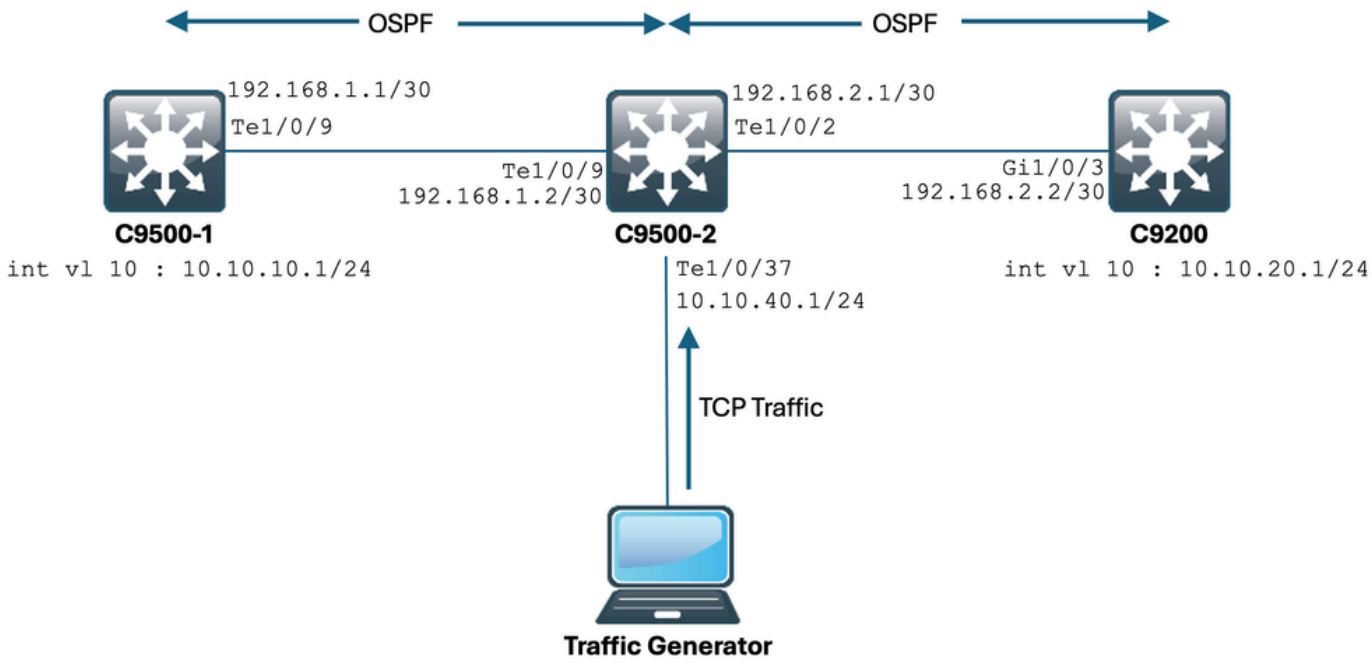
U kunt zien dat de TCP MSS waarde van het SYN pakket 512 is.

TCP/MSS-aanpassing veroorzaakt traagheid tijdens enorme hoeveelheid TCP-verkeer

Stel nu dat een netwerk meerdere apparaten heeft met TCP-verkeer.
Ze kunnen bijvoorbeeld bestanden overdragen of toegang krijgen tot een op TCP gebaseerde toepassing (zoals een Citrix Server).

U hebt het gesimuleerd door een IXIA (traffic generator) aan te sluiten op C9500-2 Te1/0/37 en TCP/SYN-pakketten met een hoge snelheid te verzenden.
Dit IXIA-apparaat fungeert als een netwerksegment waar meerdere gebruikers TCP-gebaseerde toepassingen gebruiken.
U hebt IP TCP-aanpassingsmodule CLI op TE1/0/37 geconfigureerd.
Hierdoor wordt al het TCP-verkeer op Te1/0/37 gestraft naar de CPU van de C9500-2.
Dit vergraaft op zijn beurt de 'Sw Forwarding'-wachtrij van de COPP Policer van de C9500-2, zoals eerder in het document vermeld.
Dit heeft gevolgen voor de instelling van de SSH-sessie van C9500-1 tot C9200.
Ofwel de SSH-sessie wordt niet gevormd, en krijgt een time-out, of wordt na een vertraging ingesteld.

Dit is hoe de topologie eruit ziet:



Laten we dit in actie zien.

Hier is de configuratie van C9500-2 Te1/0/37:

```
C9500-2#sh run int te1/0/37
Building configuration...
Current configuration : 135 bytes
interface TenGigabitEthernet1/0/37
no switchport
ip address 10.10.40.1 255.255.255.0
ip tcp adjust-mss 500
load-interval 30
end
```

Nu begint u enorm verkeer van IXIA naar de Te1/0/37 interface te sturen.
Laten we eens kijken naar het inkomende verkeerstarief:

```
C9500-2#sh int te1/0/37 | in rate
Queueing strategy: fifo
30 second input rate 6425812000 bits/sec, 12550415 packets/sec → We can see the enormous Input rate.
30 second output rate 0 bits/sec, 0 packets/sec
```

Laten we nu proberen om SSH van C9500-1 tot C9200 te maken:

```
C9500-1#ssh -l admin 10.10.20.1
% Connection timed out; remote host not responding
C9500-1#
```

U kunt duidelijk zien dat de C9500-1 niet in staat was om in de C9200 te SSH.
Dit komt doordat het TCP SYN-pakket dat door de C9500-1 wordt verzonden, werd gedropt door de 'Sw Forwarding'-wachtrij, die wordt gebombardeerd met verkeer van Te1/0/37.

Laten we eens kijken naar de wachtrij:

```
C9500-2#sh platform hardware fed switch 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 1000 0 0
12 0 BROADCAST Yes 600 600 0 0
13 10 Openflow Yes 200 200 0 0
14 13 Sw forwarding Yes 1000 1000 39683368064 620052629 → We can see the huge number of dropped packets in t
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 1000 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 1000 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
```

Laten we de output meerdere malen verzamelen om er zeker van te zijn dat het aantal gevallen tijdens het probleem toeneemt:

```
C9500-2#sh platform hardware fed switch active qos queue stats internal cpu policer | in Sw forwarding
14 13 Sw forwarding Yes 1000 1000 47046906560 735107915
14 13 21 Sw forwarding Yes
13 system-cpp-police-sw-forward : Sw forwarding/ LOGGING/ L2 LVX Data Pack/ Transit Traffic/
```

```
21 system-cpp-police-ios-feature : ICMP GEN/ BROADCAST/ ICMP Redirect/ L2 LVX Cont Pack/ Proto Snooping/
C9500-2#
!
C9500-2#sh platform hardware fed switch active qos queue stats internal cpu policer | in Sw forwarding
14 13 Sw forwarding Yes 1000 1000 47335535936 739617752
14 13 21 Sw forwarding Yes
13 system-cpp-police-sw-forward : Sw forwarding/ LOGGING/ L2 LVX Data Pack/ Transit Traffic/
21 system-cpp-police-ios-feature : ICMP GEN/ BROADCAST/ ICMP Redirect/ L2 LVX Cont Pack/ Proto Snooping/
C9500-2#
!
C9500-2#sh platform hardware fed switch active qos queue stats internal cpu policer | in Sw forwarding
14 13 Sw forwarding Yes 1000 1000 47666441088 744788145
14 13 21 Sw forwarding Yes
13 system-cpp-police-sw-forward : Sw forwarding/ LOGGING/ L2 LVX Data Pack/ Transit Traffic/
21 system-cpp-police-ios-feature : ICMP GEN/ BROADCAST/ ICMP Redirect/ L2 LVX Cont Pack/ Proto Snooping/
C9500-2#
```

Zoals u kunt zien, neemt het aantal gevallen toe en wordt het SSH-verkeer (TCP/SYN-pakket) hier gedropt.

Nu als u niet weet via welke interface/SVI u deze instroom van verkeer krijgt, hebt u een specifieke opdracht om te helpen.

```
C9500-2#show platform software fed switch active punt rates interfaces
Punt Rate on Interfaces Statistics
Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================================
| | Recv | Recv | Recv | Drop | Drop | Drop
Interface Name | IF_ID | 10s | 1min | 5min | 10s | 1min | 5min
================================================================================================
TenGigabitEthernet1/0/37 0x00000042 1000 1000 1000 0 0 0
------------------------------------------------------------------------------------------------
C9500-2#
```

De opdracht show platform software fed switch active punt rates interfaces geeft ons de lijst van interfaces die verantwoordelijk zijn voor het ontvangen van de enorme hoeveelheid verkeer die wordt gestraft naar de CPU.
Je kunt hier duidelijk Te1/0/37 zien, dat is de interface waardoor je het TCP verkeer krijgt.

Als u nu wilt zien hoeveel verkeer alle COPP Policer wachtrijen raakt (dat wordt ontvangen op de eerdere interface), kunt u gebruiken:
tonen platform software gevoed switch actieve punt tarieven interfaces <IF_ID van de bovengenoemde output>

Laten we eens kijken:

```
C9500-2#show platform software fed switch active punt rates interfaces 0x42
Punt Rate on Single Interfaces Statistics
Interface : TenGigabitEthernet1/0/37 [if_id: 0x42]
```

```
Received Dropped
-------- -------
Total : 2048742 Total : 0
10 sec average : 1000 10 sec average : 0
1 min average : 1000 1 min average : 0
5 min average : 1000 5 min average : 0

Per CPUQ punt stats on the interface (rate averaged over 10s interval)
=============================================================================
Q | Queue | Recv | Recv | Drop | Drop |
no | Name | Total | Rate | Total | Rate |
=============================================================================
0 CPU_Q_DOT1X_AUTH 0 0 0 0
1 CPU_Q_L2_CONTROL 7392 0 0 0
2 CPU_Q_FORUS_TRAFFIC 0 0 0 0
3 CPU_Q_ICMP_GEN 0 0 0 0
4 CPU_Q_ROUTING_CONTROL 0 0 0 0
5 CPU_Q_FORUS_ADDR_RESOLUTION 0 0 0 0
6 CPU_Q_ICMP_REDIRECT 0 0 0 0
7 CPU_Q_INTER_FED_TRAFFIC 0 0 0 0
8 CPU_Q_L2LVX_CONTROL_PKT 0 0 0 0
9 CPU_Q_EWLC_CONTROL 0 0 0 0
10 CPU_Q_EWLC_DATA 0 0 0 0
11 CPU_Q_L2LVX_DATA_PKT 0 0 0 0
12 CPU_Q_BROADCAST 0 0 0 0
13 CPU_Q_CONTROLLER_PUNT 0 0 0 0
14 CPU_Q_SW_FORWARDING 2006390 1000 0 0 -----> We can see high amount of traffic hitting the Sw forward
15 CPU_Q_TOPOLOGY_CONTROL 0 0 0 0
16 CPU_Q_PROTO_SNOOPING 0 0 0 0
17 CPU_Q_DHCP_SNOOPING 0 0 0 0
18 CPU_Q_TRANSIT_TRAFFIC 0 0 0 0
19 CPU_Q_RPF_FAILED 0 0 0 0
20 CPU_Q_MCAST_END_STATION_SERVICE 0 0 0 0
21 CPU_Q_LOGGING 34960 0 0 0
22 CPU_Q_PUNT_WEBAUTH 0 0 0 0
23 CPU_Q_HIGH_RATE_APP 0 0 0 0
24 CPU_Q_EXCEPTION 0 0 0 0
25 CPU_Q_SYSTEM_CRITICAL 0 0 0 0
26 CPU_Q_NFL_SAMPLED_DATA 0 0 0 0
27 CPU_Q_LOW_LATENCY 0 0 0 0
28 CPU_Q_EGR_EXCEPTION 0 0 0 0
29 CPU_Q_FSS 0 0 0 0
30 CPU_Q_MCAST_DATA 0 0 0 0
31 CPU_Q_GOLD_PKT 0 0 0 0
-----------------------------------------------------------------------------
```

Meervoudige uitvoer in zeer korte intervallen verzamelen:

```
C9500-2#show platform software fed switch active punt rates interfaces 0x42 | in SW_FORWARDING
14 CPU_Q_SW_FORWARDING 2126315 1000 0 0
C9500-2#
C9500-2#show platform software fed switch active punt rates interfaces 0x42 | in SW_FORWARDING
14 CPU_Q_SW_FORWARDING 2128390 1000 0 0
C9500-2#
C9500-2#show platform software fed switch active punt rates interfaces 0x42 | in SW_FORWARDING
14 CPU_Q_SW_FORWARDING 2132295 1000 0 0
C9500-2#
```

Dit toont duidelijk aan dat de Sw-doorsturen wachtrij is verstikt.
ip tcp adjust-mss Zodra u de opdracht uit de Te1/0/37 verwijdert, of als u dit TCP-verkeer stopt, wordt de SSH-toegang van C9500-1 tot C9200 onmiddellijk opnieuw ingesteld.

Laten we eens kijken naar de SSH sessie na het afsluiten van C9500-2 Te1/0/37:

```
C9500-1#ssh -l admin 10.10.20.1
Password:
```

U kunt zien dat de toegang van SSH opnieuw wordt hersteld.
Daarom kunt u de TCP-traagheid hier (SSH-toegang geblokkeerd) correleren vanwege de grote hoeveelheid TCP-verkeer in het netwerk, met TCP MSS-aanpassing.

Belangrijke punten

1. Wanneer u TCP-traagheid in uw netwerk hebt, zoals traagheid bij bestandsoverdracht, toegankelijkheid voor TCP-gerelateerde toepassingen enzovoort, en u TCP MSS-aanpassing hebt geconfigureerd op een Catalyst Switch, zorg dan dat u de COPP Policer laat vallen om te controleren of er een grote hoeveelheid TCP-verkeer in het netwerk is of niet.
2. Als u TCP MSS-aanpassing hebt geconfigureerd op een Catalyst Switch, zorg er dan voor dat het TCP-verkeer in uw netwerk niet te veel abonneert op het COPP Policer-tarief, anders worden TCP-gerelateerde problemen (traagheid, pakketdalingen) in uw netwerk gezien.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.