Problemen met routers voor ondernemingsnetwerk oplossen

Inhoud

Inleiding

Dit document beschrijft hoe u latentieproblemen in ondernemingsnetwerken kunt identificeren, oplossen en oplossen met behulp van Cisco-routers.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden of vereisten voor dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke softwareversie en hardwaretype, maar opdrachten zijn van toepassing op Cisco IOS® XE-routers zoals ASR 1000, ISR 4000 en Catalyst 8000-families.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft een basisgids om algemene latentiekwesties te begrijpen, te isoleren en problemen op te lossen, geeft nuttige bevelen/debugs om de worteloorzaken en beste praktijken te ontdekken. Houd in gedachten dat niet alle mogelijke variabelen en scenario's kunnen worden overwogen en een diepere analyse hangt af van specifieke situaties.

Latency Definitie

In algemene termen, en het citeren van de strikte definitie voor opslag en voorwaartse apparaten (op RFC 1242), is de latentie het tijdinterval dat begint wanneer het laatste beetje van het inputkader de inputpoort bereikt en dat eindigt wanneer het eerste beetje van het uitvoerkader op de uitvoerpoort wordt gezien.

Netwerkvertraging kan eenvoudig verwijzen naar vertraging bij de gegevensoverdracht over het netwerk. Voor praktische kwesties is deze definitie slechts het beginpunt; je moet het latentieprobleem definiëren waar je het over hebt in elk specifiek geval, hoewel het voor de hand ligt, de eerste stap die nodig is om een probleem op te lossen, en dat echt belangrijk wordt, is het definiëren ervan.

Latency-gebruik

Veel toepassingen vereisen een lage latentie voor real-time communicatie en zakelijke activiteiten; met de hardware en software verbeteringen dagelijks, meer toepassingen zijn beschikbaar voor mission-critical computing, online vergaderapplicaties, streaming onder anderen; op dezelfde manier blijft netwerkverkeer groeien en neemt de behoefte aan geoptimaliseerde netwerkontwerpen en betere apparaatprestaties ook toe.

Naast het geven van betere gebruikerservaring en het vereiste minimum leveren voor latency-gevoelige toepassingen, effectief identificeren en verminderen latency kwesties op een netwerk kan veel tijd en middelen besparen hoogst waardevol op een netwerk.

Latency problemen aanpakken

Het moeilijke deel van dit soort kwesties is het aantal variabelen waarmee je rekening moet houden, plus er kan geen enkel punt van falen zijn. Vandaar, wordt de definitie van latentie een belangrijke sleutel om het op te lossen en sommige aspecten u moet in overweging nemen om een nuttige probleembeschrijving te hebben zijn de volgende.

1. Verwachtingen en opsporing

Het is belangrijk om een gewenste latentie, de verwachte of baseline werkende latentie en de huidige te onderscheiden. Afhankelijk van het ontwerp, de leveranciers of de apparaten op het netwerk, soms kunt u niet de gewenste latentie bereiken, is het een goede procedure om echte onder normale omstandigheden te meten maar u moet op meetmethodes consistent zijn om misleidende aantallen te vermijden; IP SLAs, en de hulpmiddelen van de netwerkanalyzer kunnen op dit punt helpen.

Een van de meest gebruikte en basistools om latentie door toepassingen of zelfs IP SLA te identificeren is via ICMP of ping:

<#root>

```
Router#
```

ping

```
 198.51.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
```

round-trip min/avg/max

```
 =
```

2/109/541 ms

Naast het controleren van bereikbaarheid, pingelt vertelt de Ronde Tijd van de Reis (RTT) van bron aan bestemming; het minimum (2), gemiddelde (109) en maximum (541) in milliseconden. Dit betekent, de duur van wanneer de router het verzoek verzendt naar wanneer het het antwoord van apparatenbestemming ontvangt. Het geeft echter niet aan hoeveel hop of diepere informatie, maar het is een makkelijke en snelle manier om een probleem op te sporen.

2. Isolatie

Hetzelfde als ping, traceroute kan worden gebruikt als startpunt voor isolatie, het ontdekt hop en RTT per hop:

<#root>

```
Router#
```

traceroute

```
 198.51.100.1
Type escape sequence to abort.
Tracing the route to 198.51.100.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.3.1 5 msec 6 msec 1 msec
  2 10.0.1.1 1 msec 1 msec 1 msec
  3 10.60.60.1 1 msec 1 msec 1 msec
  4 10.90.0.2
```

```
362 msec 362 msec 362 msec


<<<< you can see the RTT of the three probes only on both hops

  5 10.90.1.2
363 msec 363 msec 183 msec


  6 10.90.7.7 3 msec 2 msec 2 msec
```

Traceroute werkt door een pakket te verzenden met een TimeTo Live (TTL) van 1. Eerste hop stuurt een ICMP-foutbericht dat aangeeft dat het pakket niet kan worden doorgestuurd omdat de TTL is verlopen en RTT wordt gemeten, het tweede pakket wordt dan weergegeven met een TTL van 2, en de tweede hop retourneert de TTL verlopen. Dit proces gaat door tot de bestemming is bereikt.

In het voorbeeld, kunt u zich nu beperken tot twee specifieke gastheer en u kunt van daar beginnen op onze isolatie.

Ondanks deze zijn nuttige opdrachten die een probleem gemakkelijk kunnen identificeren, houden ze geen rekening met andere variabelen zoals protocollen, pakketmarkeringen en afmetingen (hoewel u ze als tweede stap kunt instellen), verschillende IP-bronnen, bestemmingen tussen meerdere factoren.

Latentie zeggen kan een zeer breed concept zijn en je ziet vaak alleen het symptoom op een toepassing, browsen, bellen of specifieke taken. Eén van de eerste dingen die we moeten beperken, is de impact te begrijpen en het probleem gedetailleerder te definiëren, de volgende vragen te beantwoorden en elementen kunnen helpen bij deze dimensionering:

- Heeft latency alleen invloed op specifieke soort verkeer of toepassing? Voorbeeld: alleen UDP, TCP, ICMP...
- Zo ja, heeft dit verkeer unieke identificatiecodes? Bijvoorbeeld: specifieke QoS-markering, alleen bepaalde pakketgroottes, IP-opties...
- Hoeveel gebruikers of sites worden getroffen? Voorbeeld: slechts één specifieke subnetverbinding, een of twee eindhosts, een hele site verbonden met een of meerdere apparaten...
- Zijn er specifieke tijdstempels geïdentificeerd? Voorbeeld: gebeurt dit alleen tijdens piekuren, enig tijdpatroon of volledig willekeurig...
- Ontwerpaspecten. Voorbeeld: verkeer dat door een specifiek apparaat gaat, misschien veel apparaten maar slechts met één leverancier verbindt, verkeer dat lastverdeling doet maar één weg beïnvloedde...

Er zijn veel andere overwegingen maar het doorkruisen van de verschillende antwoorden (en zelfs tests die kunnen worden gedaan om ze te beantwoorden) kan effectief de scope isoleren en beperken om door te gaan met het oplossen van problemen. Bij wijze van voorbeeld: slechts één toepassing (hetzelfde soort verkeer) is van invloed op alle filialen die via verschillende providers eindigen op hetzelfde datacenter tijdens piekuren. In dit geval, begint u niet alle access switches in

alle branches te controleren, in plaats daarvan richt u zich op het verzamelen van meer informatie over het datacenter en inspecteer verder aan die kant,

Bewakingstools en enige automatisering die u op het netwerk kunt hebben, helpt ook veel bij deze isolatie, hangt echt af van de middelen die u hebt en unieke situaties.

Probleemoplossing voor algemene oorzaken

Zodra u de omvang van de probleemoplossing beperkt, kunt u beginnen met het controleren van specifieke oorzaken, bijvoorbeeld, op het gegeven traceroute voorbeeld, kunt u isoleren tot twee verschillende hop en dan, versmallen tot mogelijke oorzaken.

Platformgerelateerd

Hoge CPU

Een van de meest voorkomende oorzaken kan een apparaat zijn met een hoge CPU die vertraging veroorzaakt bij het verwerken van alle pakketten. Voor routers, zijn het nuttigste en meest basisbevel om routers te controleren

Totale prestaties voor router:

<#root>

Router#

show platform resources

```
**State Acronym: H - Healthy, W - Warning, C - Critical
Resource                Usage                Max            Warning         Critical        State
-------------------------------------------------------------------------------------------------
RP0 (ok, active)                                                                              H

Control Processor       1.15%                100%           80%             90%             H



DRAM                    3631MB(23%)          15476MB        88%             93%             H

  bootflash             11729MB(46%)         25237MB        88%             93%             H
  harddisk              1121MB(0%)           225279MB       88%             93%             H
ESP0(ok, active)                                                                              H
 QFP                                                                                          H
  TCAM                  8cells(0%)           131072cells    65%             85%             H
  DRAM                  359563KB(1%)         20971520KB     85%             95%             H
  IRAM                  16597KB(12%)         131072KB       85%             95%             H

CPU Utilization         0.00%                100%           90%             95%             H
```

```
Crypto Utilization     0.00%                 100%            90%             95%             H

  Pkt Buf Mem (0)        1152KB(0%)            164864KB        85%             95%             H
  Pkt Buf CBlk (0)       14544KB(1%)           986112KB        85%             95%             H
```

Handig om geheugen en CPU-gebruik in één keer te zien, het is verdeeld op Control-vlak en Data-vlak (QFP) hetzelfde als drempels voor elke. Het geheugen zelf, leidt niet tot een latentieprobleem, echter, als er niet meer het geheugen van de BORREL voor controlevliegtuig is, Cisco Express Forwarding (CEF) is gehandicapt en induceert een hoog CPU-gebruik dat latentie kan veroorzaken, dat is waarom het belangrijk is om aantallen onder gezonde staat te houden. De basisgids voor het oplossen van geheugenproblemen is uit het werkingsgebied maar verwijst nuttige verbinding op Verwante informatiesectie.

Als een hoge CPU wordt gedetecteerd voor gebruik van Control Processor, QFP CPU of Crypto, kunt u de volgende opdrachten gebruiken:

Voor het bedieningsvlak:

proces cpu gesorteerd tonen

<#root>

```
Router#
show processes cpu sorted
CPU utilization for five seconds:
99%/0%
; one minute: 13%; five minutes: 3%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  65        1621         638       2540 89.48%  1.82%  0.41%  0 crypto sw pk pro
   9         273          61       4475  1.56%  0.25%  0.05%   0 Check heaps
  51         212          64       3312  0.72%  0.21%  0.05%   0 Exec
 133         128          16       8000  0.60%  0.08%  0.01%   0 DBAL EVENTS
 473          25          12       2083  0.48%  0.04%  0.00%   0 WSMAN Process
  84        1173         353       3322  0.36%  0.07%  0.02%   0 IOSD ipc task
  87          23          12       1916  0.24%  0.02%  0.00%   0 PuntInject Keepa
  78         533         341       1563  0.12%  0.29%  0.07%   0 SAMsgThread
 225          25        1275         19  0.12%  0.00%  0.00%   0 SSS Feature Time
 386           4           4       1000  0.12%  0.00%  0.00%   0 Crypto WUI
 127         204       18810         10  0.12%  0.02%  0.00%   0 L2 LISP Punt Pro
```

Als de control plane CPU hoog is (dit voorbeeld ligt op 99% vanwege processen), moet u het proces isoleren en, afhankelijk van het, verder gaan met isolatie (kan worden gepunte pakketten voor ons zoals ARP of control netwerk pakketten, kan elk routingprotocol, multicast, NAT, DNS, crypto-verkeer of elke service).

Afhankelijk van uw verkeersstroom, kan dit een probleem bij verdere verwerking veroorzaken, als het verkeer niet bestemd is voor de router kunt u zich op gegevensvlak concentreren:

Voor het gegevensvlak:

toon platform hardware qfp actief datapath gebruik [samenvatting]

<#root>

```
Router#
```

show platform hardware qfp active datapath utilization

```
  CPP 0: Subdev 0
```

5 secs

```
        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
            Total (pps)          231          192           68            6
                 (bps)       114616        95392        33920         3008
Output: Priority (pps)            0            0            0            0
                 (bps)            0            0            0            0
    Non-Priority (pps)            3            2            2            0
                 (bps)        14896         9048         8968         2368
```

Total (pps)

```
         3323         2352          892            0
```

(bps)

```
        14896         9048         8968         2368
```

Processing: Load (pct)

3

```
            3            3            3
```

```
Crypto/IO
```

Crypto: Load (pct)   0

```
            0            0            0
        RX: Load (pct)            0            0            0            0
        TX: Load (pct)            1            1            0            0
            Idle (pct)           99           99           99           99
```

Als het gegevensvlak hoog is (geïdentificeerd door het aantal van de Lading van de Verwerking dat 100% bereikt), behoefte om hoeveelheid verkeer te zien dat door de router (Totaal pakket per seconden en beetjes per seconden) overgaat en productieprestaties van het platform (u kunt een idee op specifiek gegevensblad hebben).

Om te bepalen of dit verkeer al dan niet wordt verwacht, kan Packet Capture (EPC) of een bewakingsfunctie zoals NetFlow voor verdere analyse worden gebruikt, worden de volgende controles uitgevoerd:

- Is het verkeer geldig en wordt verwacht deze router te passeren?
- Identificeer abnormale verkeersstromen of hogere tarieven.
- Als u een hoog pakket per seconde nummers hebt, zoekt u naar de grootte van de pakketten. Bepaal of dit wordt verwacht en of u een fragmentatiekwestie hebt.

Als al verkeer wordt verwacht, kunt u een platformbeperking bereiken, dan, zoek de eigenschappen die op uw router lopen als tweede deel voor analyse via tonen in werking stelt -in werking stellen-config, meestal op de interfaces, identificeer om het even welke onnodige eigenschappen en maak hen onbruikbaar of verkeers in evenwicht om de cycli van cpu vrij te geven.

Als er echter geen indicatie is van een platformlimiet, is een ander nuttig hulpmiddel om te bevestigen als de router vertraging op pakketten toevoegt het FIA-spoor, kunt u de exacte procestijd zien die voor elk pakket wordt doorgebracht en de functies die het grootste deel van de verwerking nemen. De volledige hoge CPU-probleemoplossing valt buiten het bereik van dit document, maar raadpleegt de koppelingen in het gedeelte Verwante informatie.

Verkeersgerelateerd

MTU en fragmentatie

Max. Transmissie-eenheid (MTU) is de maximale pakketlengte die kan worden verzonden en die afhangt van het aantal octetten dat fysieke links kunnen verzenden.Wanneer protocollen in de bovenste laag gegevens naar het onderliggende IP verzenden en de resulterende lengte van het IP-pakket groter is dan het pad MTU, wordt het pakket in fragmenten verdeeld. Deze lagere grootte op het netwerk veroorzaakt meer verwerking en verschillende behandeling in sommige gevallen en dat is waarom u moet voorkomen dat het mogelijk.

Voor sommige functies, zoals NAT of Zone Based Firewall, is virtuele hermontage vereist om "het hele pakket te hebben", past wat nodig is toe, stuurt de fragmenten door en vernietigt de opnieuw samengestelde kopie. Dit proces voegt CPU-cycli toe en is vatbaar voor fouten.

Sommige toepassingen baseren zich niet op fragmentatie, is één van de meest fundamentele test om MTU te controleren pingelen met een geen fragmentoptie en test verschillende pakketgrootte: pingelen ip-adres PDF-bit grootteaantal. Als ping niet succesvol is, repareer MTU over het pad als drop optreedt en veroorzaakt verdere problemen.

Functies, zoals op beleid gebaseerde routing en gelijke kosten multipath op een netwerk met gefragmenteerde pakketten kunnen vertragingsproblemen en meer fouten veroorzaken meestal op hoge gegevenssnelheden, het veroorzaken van hoge assemblagetijden, dubbele ID's en beschadigde pakketten, als een aantal van deze problemen worden geïdentificeerd, kijk dan om deze fragmentatie zo goed mogelijk op te lossen. Eén opdracht om te controleren of u fragmenten en eventuele mogelijke problemen hebt, is IP-verkeer tonen:

<#root>

```
Router#
```

show ip traffic

```
IP statistics:
  Rcvd:  9875429 total, 14340254 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other, 0 ignored
```

Frags:

150 reassembled

, 0

timeouts

,

0 could not reassemble

0

fragmented

, 600

fragments

, 0

could not fragment

```
         0 invalid hole
  Bcast: 31173 received, 6 sent
  Mcast: 0 received, 0 sent
  Sent:  15742903 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
<output omitted>
```

Van de output hierboven, verwijzen de gewaagde woorden op de sectie van Frags naar:

- Hergemonteerd: Aantal hergemonteerde pakketten.
- Time-outs: elke keer dat de tijd voor het opnieuw samenvoegen van een pakketfragment verloopt.
- Kan niet opnieuw samenstellen: aantal pakketten dat niet opnieuw kon worden gemonteerd.
- Gefragmenteerd: aantal pakketten dat MTU overschrijdt en onderwerp is voor fragmentatie.
- Fragmenten: Aantal stukken waarin de pakketten waren gefragmenteerd.

- Kon niet fragmenteren: Aantal pakketten die MTU overschrijden maar kon niet worden gefragmenteerd.

Als fragmentatie wordt gebruikt en u heeft onderbrekingen of kon niet tellers te reassembleren verhogen, is één manier om kwesties te bevestigen die door het platform worden veroorzaakt, via QFP dalingen, die het zelfde bevel gebruiken zoals later verklaard op dalingen sectie: toon platform hardware qfp actieve statistieken daling. Zoek naar fouten zoals: TCPbadfrag, IPFragErr, FragTailDrop, ReassDrop, ReassFragTooBig, ReassTooManyFrags, ReassTimeout of verwante fouten. Elke case kan verschillende oorzaken hebben, zoals het niet krijgen van alle fragmenten, gedupliceerd, CPU stremming onder anderen. Nogmaals, nuttige tools voor verdere analyse en mogelijke oplossing kan een FIA spoor en configuratie controle zijn.

TCP biedt Max Segment Size (MSS) mechanisme om dit probleem op te lossen maar het kan latentie veroorzaken als onjuist, niet MSS onderhandeld of verkeerde Path MTU ontdekt.

Aangezien UDP dit fragmentatiemechanisme niet heeft, kunt u vertrouwen op handmatige implementatie van PMTD of enige applicatie-laagoplossing, kunt u hen (indien van toepassing) in staat stellen om pakketten korter dan 576 bytes te verzenden, wat de kleinere effectieve MTU is voor het verzenden van nummer volgens RFC1122 in hulpmiddelen om fragmentatie te voorkomen.

Ontwerpgerelateerd

Meer dan een suggestie voor probleemoplossing, beschrijft deze sectie kort twee meer belangrijke componenten die kunnen toevoegen aan latentieproblemen en zij vereisen een uitgebreide bespreking en een analyse uit het werkingsgebied van dit document.

Suboptimale routing

Suboptimale routing in netwerken verwijst naar een situatie waarin gegevenspakketten niet door het efficiëntste of kortste pad worden geleid dat in een netwerk beschikbaar is. In plaats daarvan maken deze pakketten gebruik van een route die minder efficiënt is, wat mogelijk leidt tot meer latentie, stremming of waardoor de netwerkprestaties worden beïnvloed. IGP's kiezen altijd de beste paden, wat de lagere kosten betekent, maar het hoeft niet noodzakelijkerwijs de goedkoopste of de laagste vertragingstraject te zijn (het beste kan degene zijn met een hogere bandbreedte).

Suboptimale routing kan voorkomen bij problemen met routeringsprotocollen, ofwel configuratie of elke situatie zoals rasvoorwaarden, dynamische veranderingen (topologiewijzigingen of koppelingsfouten), geplande traffic engineering op basis van bedrijfsbeleid of kosten, redundanties of failovers (naar het back-uppad gaan onder bepaalde omstandigheden) en andere situaties.

Tools zoals traceroutes of monitoring-apparatuur kunnen helpen deze situatie voor specifieke stromen te identificeren, als dit het geval is, en afhankelijk zijn van veel andere factoren, voldoen aan de toepassingsvereisten en lagere latentie kan vereisen dat routering opnieuw wordt ontworpen of traffic engineering.

Quality-of-Service (QoS)

Door de Quality of Service (QoS) te configureren kunt u bepaalde typen verkeer een voorkeursbehandeling geven ten koste van andere typen verkeer. Zonder QoS biedt het apparaat biedt de best-inspanningsservice voor elk pakket, ongeacht de pakketinhoud of grootte. Het apparaat verzendt de pakketten zonder enige verzekering van betrouwbaarheid, vertragingsgrenzen, of productie.

Als QoS op zijn plaats is, wordt het echt belangrijk om te identificeren als de router markeert, hertekent of enkel de pakketten classificeert, de configuratie controleert en beleid-kaart toont [name_of_policy_map | zitting | interface_id] helpt om klassen te begrijpen die worden beïnvloed door hoge snelheden, dalingen of pakketten die onjuist zijn geclassificeerd.

Het implementeren van QoS is een zware taak die een serieuze analyse vereist en buiten het bereik van dit document valt, maar het wordt sterk aanbevolen om dit te overwegen om prioriteit te geven aan tijdgevoelige toepassingen en om veel latency en toepassingsproblemen op te lossen of te voorkomen.

Andere prestatieproblemen

Andere omstandigheden kunnen traagheid, sessie opnieuw verbinden of algemene slechte prestaties die u moet controleren, sommige zijn:

Drops

Een probleem dat direct te maken heeft met de verwerking op een apparaat is pakketdruppels, u moet de invoer en uitvoer kant controleren vanuit interfaceperspectief:

<#root>

```
Router#sh interfaces GigabitEthernet0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is vNIC, address is 0ce0.995d.0000 (bia 0ce0.995d.0000)
  Internet address is 10.10.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is Virtual
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:19, output 00:08:33, output hang never
  Last clearing of "show interface" counters never


 Input queue: 0/375/6788/0 (size/max/drops/flushes); Total output drops: 18263

  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 114000 bits/sec, 230 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     193099 packets input, 11978115 bytes, 0 no buffer
```

```
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles


1572 input errors

,

12 CRC

, 0 frame,

1560 overrun

, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     142 packets output, 11822 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     23 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

Aan de inkomende zijde heeft u:

- De rij van de input daalt: Elke interface bezit een inputrij (dit is een softwarebuffer die kan worden gewijzigd) die inkomende pakketten worden geplaatst om verwerking door de Routing Processor (RP) te wachten. als het tarief voor inkomende die pakketten op de inputrij worden geplaatst de snelheid overschrijdt waarmee de RP de pakketten kan verwerken kunt u laten vallen toename hebben. Houd er echter rekening mee dat alleen controlepakketten en "Voor ons" verkeer worden geplaatst, daarom, als latentie wordt gezien bij het passeren van het verkeer, zelfs als u sporadische druppels hebt, mag dit geen oorzaak zijn.

- Overschrijdingen: Dit gebeurt wanneer de ontvangerhardware de ontvangen pakketten niet aan een hardwarebuffer kan overhandigen omdat de inputsnelheid de capaciteit van de ontvanger overschrijdt om de gegevens te behandelen. Dit nummer kan een probleem aangeven met de snelheid en prestaties van de router, verkeer alleen voor deze interface opnemen en op zoek gaan naar verkeerspieken. Een gemeenschappelijke tijdelijke oplossing is debietcontrole toe te laten maar dit kan aan vertragingspakketten toevoegen. Dit kan ook een bewijs zijn voor knelpunten en overinschrijving.
- CRC's: treedt op vanwege fysieke problemen, controleer de bekabeling, poorten en SFP's op de juiste manier verbonden en goed functionerend.

Aan de uitvoerzijde hebt u:

- De rij van de output daalt: Elke interface bezit een outputrij waar uitgaande pakketten die op de interface moeten worden verzonden worden geplaatst zijn. Soms overschrijdt het tarief voor uitgaande pakketten die op de outputrij door RP worden geplaatst het tarief waarmee de interface de pakketten kan verzenden, Dit kan prestatieskwestie en latentieproblemen veroorzaken als er geen QoS op zijn plaats is, anders, kunt u dit aantal hebben dat wegens

bepaald toegepast beleid stijgt en adviseert te controleren of QoS configuratie om voorgenomen of kritisch verkeer te beschermen en te verzekeren uitvoert.

Tot slot, druppels op QFP is direct gerelateerd aan hoge verwerking die latentie kan veroorzaken, check via show platform hardware qfp actieve statistieken drop:

<#root>

```
Router#
show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                          Packets                  Octets
-------------------------------------------------------------------------
Disabled                                         2                     646
Ipv4NoAdj                                   108171                 6706602
Ipv6NoRoute                                     10                     560
```

Oorzaken hangen af van code, FIA-spoor helpt te bevestigen of weggooien als het verkeer dat wordt beïnvloed door latentie op dit punt wordt gelaten vallen.

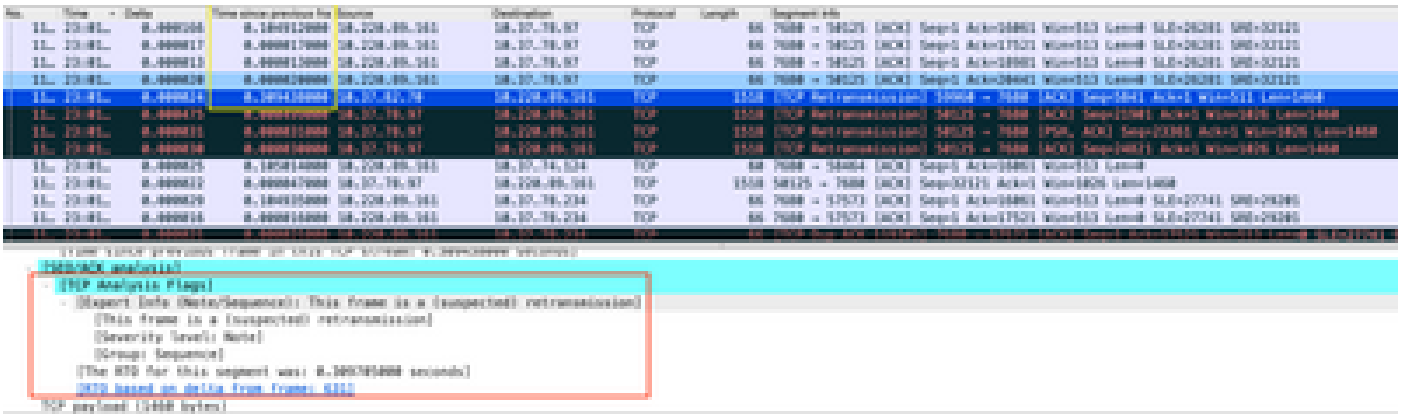
TCP-hertransmissie

TCP-doorgifte is een symptoom of kan een gevolg zijn van een onderliggend probleem zoals pakketverlies. Dit probleem kan leiden tot traagheid en slechte prestaties bij de toepassing.

Het Transmission Control Protocol (TCP) maakt gebruik van een hertransmissietimer om de levering van gegevens te garanderen bij afwezigheid van feedback van de externe gegevensontvanger. De duur van deze timer wordt aangeduid als RTO (doorlooptijd). Wanneer de wederuitzendingstimer verloopt, zendt de afzender het vroegste segment opnieuw uit dat niet door de TCP-ontvanger is bevestigd en wordt RTO verhoogd.

Sommige heruitzendingen kunnen niet volledig worden geëlimineerd, als zij minimaal zijn, kan het geen probleem weerspiegelen. Echter, zoals je kunt afleiden, meer hertransmissie gezien, meer latentie op de TCP sessie en moet worden aangepakt.

Packet Capture geanalyseerd in Wireshark kan het probleem als volgende voorbeeld bevestigen:



Opname van TCP-gesprek

Als er wederuitzendingen zijn, gebruik de zelfde opnamemethode op de router in- en uitgangsrichting om alle pakketten te controleren verzenden en ontvangen. Natuurlijk kan dit op elke hop een enorme inspanning vertegenwoordigen, zodat is de gedetailleerde analyse van opname nodig voor TCP, kijkend naar TTLs, tijden van vorige frames op dezelfde TCP stream om te begrijpen van welke richting (server of client) u deze vertraging of gebrek aan reactie hebt om uw probleemoplossing te sturen.

Overtekening en knelpunten

Overtekening gebeurt wanneer de vereiste bronnen (bandbreedte) groter zijn dan de werkelijk beschikbare bronnen. Opdrachten om te identificeren als u dit probleem op een router hebt, zijn al behandeld in de vorige sectie.

Als gevolg van deze situatie kunnen knelpunten ontstaan wanneer verkeersstromen worden vertraagd door onvoldoende bandbreedte of hardwarecapaciteit. Het is belangrijk om vast te stellen of dit in korte tijd gebeurt of dat het een langetermijnsituatie is om oplossingen toe te passen.

Er is geen specifiek advies om het op te lossen maar sommige opties zijn balanceren verkeer naar verschillende platform, segmenteren het netwerk of upgrade naar robuustere apparaten gebaseerd op huidige behoeften en toekomstige groeianalyse.

Gerelateerde informatie

- IP SLA's ICMP-echobewerkingen
- Geheugen - probleemoplossing
- Probleemoplossing met de functie Cisco IOS-XE Datapath Packet Trace
- Probleemoplossing voor Packet Drops op ASR 1000 Series servicerouterieën.
- QoS-gerelateerde informatie
- QoS-configuratie op routers
- Cisco Technical Support en downloads

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.