Risoluzione dei problemi dei router sulle reti aziendali

Sommario

Introduzione

Questo documento descrive come identificare, risolvere e risolvere i problemi di latenza nelle reti aziendali con router Cisco.

Prerequisiti

Requisiti

Non sono previsti prerequisiti o requisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o per tutti i tipi di hardware, ma i comandi sono validi per i router Cisco IOS® XE come ASR 1000, ISR 4000 e le famiglie Catalyst

8000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento descrive una guida di base per comprendere, isolare e risolvere i problemi di latenza generale, fornisce comandi e debug utili per rilevare le cause principali e le best practice. Tenete presente che non è possibile prendere in considerazione tutte le variabili e gli scenari possibili e che un'analisi più approfondita dipende da situazioni specifiche.

Definizione della latenza

In termini generali, e citando la definizione rigida per i dispositivi di archiviazione e inoltro (in RFC 1242), la latenza è l'intervallo di tempo che inizia quando l'ultimo bit del frame di input raggiunge la porta di input e termina quando il primo bit del frame di output viene visualizzato sulla porta di output.

La latenza di rete può semplicemente riferirsi a un ritardo nel trasferimento dei dati attraverso la rete. Per i problemi pratici, questa definizione è solo il punto di partenza; è necessario definire il problema di latenza di cui si sta parlando in ogni caso specifico, anche se sembra ovvio, il primo passo necessario per risolvere un problema, e diventa davvero importante, è quello di definirlo.

Utilizzo latenza

Molte applicazioni richiedono una bassa latenza per le comunicazioni e le operazioni aziendali in tempo reale; con i miglioramenti hardware e software che si verificano ogni giorno, sono disponibili più applicazioni per l'elaborazione mission-critical, le applicazioni per le riunioni online, lo streaming e altre ancora. Allo stesso modo, il traffico di rete continua a crescere e aumenta la necessità di progetti di rete ottimizzati e di migliori prestazioni dei dispositivi.

Oltre a offrire una migliore esperienza utente e a fornire il minimo necessario per le applicazioni sensibili alla latenza, identificare e ridurre efficacemente i problemi di latenza su una rete può far risparmiare molto tempo e risorse di grande valore su una rete.

Problemi relativi alla latenza

La parte difficile di questo tipo di problemi è il numero di variabili che è necessario prendere in considerazione e non può esserci un singolo punto di errore. Pertanto, la definizione di latenza diventa una chiave importante per risolverla e alcuni aspetti da prendere in considerazione per avere una descrizione utile del problema sono i prossimi.

1. Previsione e rilevamento

È importante differenziare la latenza desiderata, la latenza di lavoro prevista o di base e quella corrente. A seconda della progettazione, dei provider o dei dispositivi della rete, a volte non è possibile ottenere la latenza desiderata, è consigliabile misurare quella reale in condizioni normali, ma è necessario essere coerenti con i metodi di misurazione per evitare numeri fuorvianti. Gli SLA IP e gli strumenti di analisi della rete possono essere di aiuto in questo senso.

Uno degli strumenti più utilizzati e di base per identificare la latenza delle applicazioni o persino degli SLA IP è tramite ICMP o 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
```

Oltre a controllare la raggiungibilità, il comando ping indica il tempo di andata e ritorno (RTT) dall'origine alla destinazione; il valore minimo (2), la media (109) e il valore massimo (541) in millisecondi. Questo valore indica la durata da quando il router invia la richiesta a quando riceve la risposta dalla destinazione del dispositivo. Tuttavia, non mostra quanti hop o informazioni più approfondite, ma è un modo semplice e veloce per rilevare un problema.

2. Isolamento

Analogamente al ping, il comando traceroute può essere usato come punto di inizio per l'isolamento e permette di individuare gli hop e gli 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
```

Il comando traceroute invia un pacchetto con un valore TTL (TimeTo Live) di 1. Il primo hop invia un messaggio di errore ICMP che indica che il pacchetto non può essere inoltrato perché il valore TTL è scaduto e viene misurato l'RTT, il secondo pacchetto viene quindi inviato nuovamente con un valore TTL di 2 e il secondo hop restituisce il valore TTL scaduto. Questo processo continua finché non viene raggiunta la destinazione.

Sull'esempio, ora è possibile restringere la ricerca a due host specifici e iniziare da lì sul nostro isolamento.

Nonostante questi comandi siano utili per identificare facilmente un problema, non prendono in considerazione altre variabili, come i protocolli, i contrassegni dei pacchetti e le dimensioni (anche se è possibile impostarli come secondo passaggio), le diverse origini IP e le destinazioni tra più fattori.

Dire latenza può essere un concetto molto ampio e spesso si vede solo il sintomo su un'applicazione, esplorazione, chiamata o attività specifiche. Una delle prime cose da limitare è capire l'impatto e definire il problema in modo più dettagliato, rispondere alle domande successive e gli elementi possono aiutare per questa quotatura:

- La latenza influisce solo su un tipo specifico di traffico o applicazione? Esempio: solo UDP, TCP, ICMP...
- In caso affermativo, il traffico ha identificatori univoci? Esempio: marcatura QoS specifica, solo dimensioni del pacchetto determinate, opzioni IP...
- Quanti utenti o siti sono interessati? Esempio: solo una subnet specifica, uno o due host terminali, un intero sito connesso a uno o più dispositivi...
- Sono stati identificati timestamp specifici? Esempio: questo si verifica solo durante le ore di punta, qualsiasi modello di tempo o completo casuale...
- Aspetti di progettazione. Esempio: il traffico che attraversa un dispositivo specifico, forse molti dispositivi ma che si connettono a un solo provider, il traffico che esegue il bilanciamento del carico, ha interessato un solo percorso...

Ci sono molte altre considerazioni, ma attraversare le diverse risposte (e anche i test che possono essere eseguiti per rispondervi) può efficacemente isolare e limitare l'ambito per procedere con la risoluzione dei problemi. Ad esempio, solo un'applicazione (stesso tipo di traffico) ha influito su tutte le filiali che passano attraverso provider diversi e terminano nello stesso centro dati nelle ore di punta. In questo caso, non si inizia a controllare tutti gli switch di accesso in tutte le filiali, ma ci si concentra sulla raccolta di ulteriori informazioni sul centro dati e si ispeziona ulteriormente da quel lato,

Gli strumenti di monitoraggio e alcuni strumenti di automazione che è possibile avere sulla rete aiutano molto anche su questo isolamento, dipende davvero dalle risorse che avete e situazioni uniche.

Risoluzione dei problemi comuni

Dopo aver limitato l'ambito della risoluzione dei problemi, è possibile iniziare a controllare cause specifiche, ad esempio nell'esempio traceroute fornito, è possibile isolare due hop diversi e quindi limitare il numero alle possibili cause.

Correlato alla piattaforma

Elevato consumo della CPU

Una delle cause più comuni può essere un dispositivo con un elevato ritardo della CPU nell'elaborazione di tutti i pacchetti. Per i router, il comando più utile e di base per controllare i router è

Prestazioni complessive per il 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
```

Utile per vedere contemporaneamente l'utilizzo della memoria e della CPU, è diviso sul Control Plane e sul Data Plane (QFP) come soglie per ciascuna di esse. La memoria in sé non crea problemi di latenza. Tuttavia, se non è disponibile più memoria DRAM per il control plane, Cisco Express Forwarding (CEF) viene disabilitato e determina un elevato utilizzo della CPU che può produrre latenza. Per questo motivo è importante mantenere i numeri in uno stato integro. La guida di base per la risoluzione dei problemi relativi alla memoria non è inclusa nell'ambito, ma fare riferimento al collegamento Utile nella sezione Informazioni correlate.

Se viene rilevata una CPU elevata per l'utilizzo del processore di controllo, della CPU QFP o della crittografia, è possibile utilizzare i comandi seguenti:

Per il piano di controllo:

mostra cpu processo ordinata

<#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
```

Se la CPU del control plane è elevata (questo esempio è al 99% a causa dei processi), è necessario isolare il processo e, a seconda di esso, procedere con l'isolamento (possono essere pacchetti punted per noi come ARP o pacchetti di rete di controllo, possono essere qualsiasi protocollo di routing, multicast, NAT, DNS, traffico crypto o qualsiasi servizio).

A seconda del flusso del traffico, ciò può causare problemi di ulteriore elaborazione. Se il traffico non è destinato al router, è possibile concentrarsi sul data plane:

Per il piano dati:

visualizzare l'utilizzo del percorso dati attivo qfp hardware della piattaforma [riepilogo]

<#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
```

Se il data plane è alto (identificato dal numero di elaborazione del carico che raggiunge il 100%), è necessario verificare la quantità di traffico che attraversa il router (pacchetto totale per secondo e bit per secondo) e le prestazioni di throughput della piattaforma (un'idea può essere trovata su un data sheet specifico).

Per determinare se il traffico è previsto o meno, è possibile usare l'acquisizione dei pacchetti (EPC) o qualsiasi funzione di monitoraggio, ad esempio Netflow, per ulteriori analisi, effettuare i seguenti controlli:

- Il traffico è valido e dovrebbe passare questo router?
- Identificare i flussi di traffico anomali o le velocità più elevate.
- Se il numero di pacchetti al secondo è elevato, cercare le dimensioni dei pacchetti. Verificare se è previsto un problema di frammentazione o se si tratta di un problema previsto.

Se è previsto tutto il traffico, è possibile che si stia raggiungendo una limitazione della piattaforma, quindi cercare le funzionalità in esecuzione sul router come seconda parte per l'analisi tramite show running-config, principalmente sulle interfacce, identIfy tutte le funzionalità non necessarie e disabilitarle o bilanciare il traffico per rilasciare i cicli della CPU.

Tuttavia, se non c'è alcuna indicazione di un limite di piattaforma, un altro utile strumento per confermare se il router sta aggiungendo ritardo ai pacchetti è la traccia FIA, è possibile vedere l'esatto tempo di processo impiegato per ogni pacchetto e le funzionalità che richiedono la maggior parte dell'elaborazione. La risoluzione completa dei problemi relativi alla CPU elevata non è compresa nell'ambito di questo documento, ma fare riferimento ai collegamenti della sezione Informazioni correlate.

Traffico correlato

MTU e frammentazione

MTU (Maximum Transmission Unit) è la lunghezza massima del pacchetto da trasmettere che dipende dal numero di ottetti che i collegamenti fisici possono trasmettere.Quando i protocolli di livello superiore inviano i dati all'IP sottostante e la lunghezza del pacchetto IP risultante è superiore all'MTU del percorso, il pacchetto viene suddiviso in frammenti. Le dimensioni inferiori della rete causano una maggiore elaborazione e un trattamento diverso in alcuni casi. Per questo motivo è necessario evitarlo il più possibile.

Per alcune funzionalità come NAT o il firewall basato su zona, è necessario il riassemblaggio virtuale per "ottenere l'intero pacchetto", applica ciò che è necessario, inoltra i frammenti e elimina la copia riassemblata. Questo processo aggiunge cicli di CPU ed è soggetto a errori.

Alcune applicazioni non si basano sulla frammentazione; uno dei test più semplici per verificare l'MTU è un ping con l'opzione no fragment (nessun frammento) e testare diverse dimensioni del pacchetto: ping ip-address df-bit size number. Se il ping ha esito negativo, correggere l'MTU sul percorso quando il pacchetto viene scartato e si verificano altri problemi.

Caratteristiche quali il routing basato su criteri e la funzione multipath a costo uguale su una rete con pacchetti frammentati possono creare problemi di ritardo e più errori, soprattutto con velocità di trasferimento dati elevate, riducendo i tempi di assemblaggio, duplicando gli ID e danneggiando i pacchetti. Se vengono identificati alcuni di questi problemi, cercare di risolvere la frammentazione il più possibile. Per verificare la presenza di frammenti e i potenziali problemi, usare il comando show ip traffic:

<#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>
```

Nell'output precedente, le parole in grassetto nella sezione Frammenti fanno riferimento a:

- Riassemblati: numero di pacchetti riassemblati.
- Timeout: ogni volta che scade il tempo di riassemblaggio di un frammento di pacchetto.
- Impossibile ricomporre: numero di pacchetti che non è stato possibile ricomporre.
- Frammentato: numero di pacchetti che superano l'MTU e soggetti a frammentazione.
- Frammenti: numero di blocchi in cui i pacchetti sono stati frammentati.
- Impossibile frammentare. Numero di pacchetti che superano l'MTU ma non possono essere

frammentati.

Se si utilizza la frammentazione e si verificano timeout o non è stato possibile ricomporre i contatori, un modo per confermare i problemi causati dalla piattaforma è tramite i cali QFP, usando lo stesso comando come spiegato più avanti nella sezione dei cali: show platform hardware qfp active statistics drop. Cercare errori quali: TcpBadfrag, IpFragErr, FragTailDrop, ReassDrop, ReassFragTooBig, ReassTooManyFrags, ReassTimeout o errori correlati. Ciascun caso può avere cause diverse, ad esempio la mancata ricezione di tutti i frammenti, la duplicazione e la congestione della CPU. Anche in questo caso, gli strumenti utili per ulteriori analisi e potenziali correzioni possono essere una traccia FIA e un controllo della configurazione.

Per risolvere il problema, il TCP offre il meccanismo Maximum Segment Size (MSS), ma può indurre latenza se viene rilevata un'MTU del percorso errata, negoziata non MSS o rilevata una MTU del percorso errata.

Poiché UDP non dispone di questo meccanismo di frammentazione, è possibile fare affidamento sull'implementazione manuale della PMTD o di qualsiasi soluzione a livello di applicazione, è possibile consentire a UDP (quando applicabile) di inviare pacchetti di dimensioni inferiori a 576 byte, ossia la MTU più piccola per l'invio di numeri come da RFC1122, al fine di evitare la frammentazione.

Relativo alla progettazione

Anziché un suggerimento per la risoluzione dei problemi, questa sezione descrive brevemente altri due componenti chiave che possono aggiungere problemi di latenza e che richiedono un'ampia discussione e analisi al di fuori dell'ambito di questo documento.

Routing non ottimale

Il routing subottimale nella rete si riferisce a una situazione in cui i pacchetti di dati non vengono indirizzati attraverso il percorso più efficiente o più breve disponibile in una rete. Al contrario, questi pacchetti utilizzano un percorso meno efficiente che potrebbe causare un aumento della latenza, della congestione o un calo delle prestazioni della rete. Gli IGP scelgono sempre i percorsi migliori, il che significa il costo più basso, ma non è necessariamente quello più economico o il percorso di ritardo più basso (il migliore può essere quello con una larghezza di banda più alta).

Il routing non ottimale può verificarsi in caso di problemi con i protocolli di routing: configurazione o qualsiasi situazione, ad esempio condizioni di gara, modifiche dinamiche (modifiche della topologia o errori di collegamento), progettazione del traffico prevista basata sulle politiche o sui costi aziendali, ridondanze o failover (passaggio al percorso di backup in determinate condizioni), tra le altre situazioni.

Strumenti quali tracciati o dispositivi di monitoraggio possono aiutare a identificare questa situazione per flussi specifici e, in questo caso, dipendono da molti altri fattori, a soddisfare le richieste delle applicazioni. Una latenza inferiore può richiedere una riprogettazione del routing o della gestione del traffico.

QoS (Quality of Service)

Configurando la qualità del servizio (QoS), è possibile fornire un trattamento preferenziale a tipi di traffico specifici a scapito di altri tipi di traffico. Senza QoS, la sul dispositivo bootflash o slot0: offre la massima efficienza per ogni pacchetto, indipendentemente dal suo contenuto o dalle sue dimensioni. OSPF (Open Shortest Path First) sul dispositivo bootflash o slot0: invia i pacchetti senza alcuna garanzia di affidabilità, ritardi o velocità effettiva.

Se è presente la funzionalità QoS, è molto importante verificare se il router contrassegna, contrassegna nuovamente o semplicemente classifica i pacchetti, controllare la configurazione e visualizzare la mappa dei criteri [name_of_policy_map | sessione | interface [id_interfaccia] aiuta a comprendere le classi interessate da frequenze alte, cadute o pacchetti classificati in modo errato.

L'implementazione di QoS è un'attività complessa che richiede un'analisi approfondita e che esula dagli obiettivi del presente documento, ma si consiglia di tenere presente questa considerazione per dare priorità alle applicazioni più impegnative e risolvere o prevenire molti problemi di latenza e applicazioni.

Altri problemi di prestazioni

Altre condizioni possono aggiungere lentezza, riconnessione della sessione o prestazioni generali non ottimali da controllare, ad esempio:

Cadute

Un problema direttamente correlato all'elaborazione su un dispositivo è la perdita di pacchetti. È necessario controllare il lato di input e output dalla prospettiva dell'interfaccia:

<#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#
```

Sul lato dell'input sono presenti:

- Interruzioni coda di input: ogni interfaccia possiede una coda di input (un buffer software che può essere modificato) in cui i pacchetti in ingresso sono posizionati in attesa di elaborazione da parte del processore di routing (RP). se la velocità dei pacchetti in entrata inseriti nella coda di input supera la velocità alla quale l'RP è in grado di elaborare i pacchetti, è possibile che le perdite aumentino. Tenere presente, tuttavia, che solo i pacchetti di controllo e il traffico "For us" vengono posizionati, quindi, se si rileva una latenza nel traffico di passaggio, anche in caso di cadute sporadiche, questa non deve essere una causa.

- Sovraccarichi: questo si verifica quando l'hardware ricevente non è in grado di consegnare i pacchetti ricevuti a un buffer hardware perché la velocità di input supera la capacità del ricevente di gestire i dati. Questo numero può indicare un problema con la velocità e le prestazioni del router, acquisire il traffico solo per questa interfaccia e cercare i picchi di traffico. Una soluzione comune è abilitare il controllo del flusso, ma ciò può aumentare il ritardo dei pacchetti. Ciò può anche essere una prova di colli di bottiglia e di sottoscrizioni eccessive.
- CRC: si verifica a causa di problemi fisici, controllare il cablaggio, le porte e gli SFP correttamente collegati e funzionanti.

Sul lato dell'output sono presenti:

- Perdite coda di output: ogni interfaccia è proprietaria di una coda di output in cui vengono inseriti i pacchetti in uscita da inviare all'interfaccia. A volte la frequenza dei pacchetti in uscita inseriti dalla coda di output dall'RP supera la velocità alla quale l'interfaccia può inviare i pacchetti. Ciò può causare problemi di prestazioni e latenza se non è presente

alcuna funzionalità QoS. In caso contrario, è possibile aumentare questo numero a causa di alcuni criteri applicati e consigliare di controllare o implementare la configurazione QoS per proteggere e garantire il traffico previsto o critico.

Infine, le cadute su QFP sono direttamente correlate a un'elevata elaborazione che può causare latenza, controllare tramite show platform hardware qfp active statistics 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
```

Le cause dipendono dal codice, la traccia FIA consente di confermare o ignorare se il traffico interessato dalla latenza viene interrotto in questo punto.

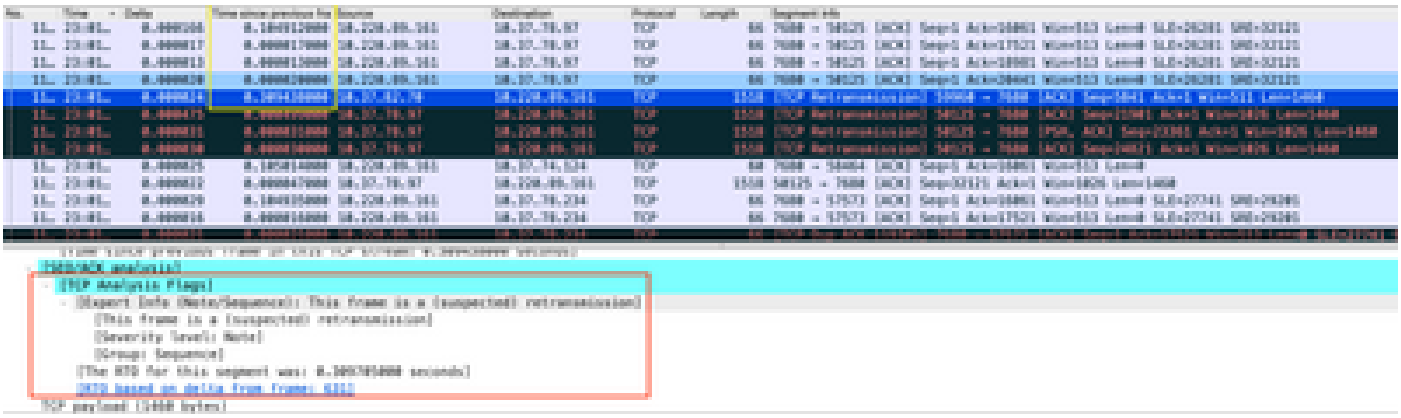
Ritrasmissione TCP

La ritrasmissione TCP è un sintomo o può essere una conseguenza di un problema di underlay, come la perdita di pacchetti. Questo problema può causare rallentamenti e cattive prestazioni dell'applicazione.

Il protocollo TCP (Transmission Control Protocol) utilizza un timer di ritrasmissione per garantire la consegna dei dati in assenza di feedback da parte del ricevitore remoto. La durata di questo timer è indicata come RTO (retransmission timeout). Alla scadenza del timer di ritrasmissione, il mittente trasmette nuovamente il segmento più vecchio che non è stato riconosciuto dal ricevitore TCP e l'RTO aumenta.

Alcune ritrasmissioni non possono essere eliminate completamente, se sono minime, non può riflettere un problema. Tuttavia, come si può dedurre, più ritrasmissione visto, più latenza sulla sessione TCP e deve essere affrontato.

L'acquisizione dei pacchetti analizzata in Wireshark può corroborare il problema, come nell'esempio seguente:



Acquisizione conversazione TCP

In caso di ritrasmissioni, usare lo stesso metodo di acquisizione sul router in entrata e in uscita per controllare tutti i pacchetti inviati e ricevuti. Naturalmente, eseguire questa operazione su ogni hop può rappresentare uno sforzo enorme, quindi è necessaria un'analisi dettagliata sull'acquisizione per il TCP, considerando i TTL, i tempi dei frame precedenti sullo stesso flusso TCP per capire da quale direzione (server o client) si ha questo ritardo o mancanza di risposta per indirizzare la risoluzione dei problemi.

Sottoscrizione in eccesso e colli di bottiglia

La sottoscrizione in eccesso si verifica quando le risorse richieste (larghezza di banda) sono maggiori di quelle effettivamente disponibili. I comandi per individuare la presenza del problema su un router sono già stati illustrati nella sezione precedente.

Di conseguenza, si possono verificare colli di bottiglia quando i flussi di traffico sono rallentati a causa di larghezza di banda insufficiente o capacità hardware insufficiente. È importante stabilire se ciò avviene in un breve periodo di tempo o se è una situazione a lungo termine applicare le soluzioni.

Non sono disponibili suggerimenti specifici per risolverlo, ma alcune opzioni sono bilanciare il traffico verso piattaforme diverse, segmentare la rete o eseguire l'aggiornamento a dispositivi più solidi in base alle esigenze attuali e all'analisi della crescita futura.

Informazioni correlate

- Operazioni echo ICMP sugli SLA IP
- Risoluzione dei problemi relativi alla memoria
- Risoluzione dei problemi con la funzionalità Cisco IOS-XE Datapath Packet Trace
- Risoluzione dei problemi di perdita di pacchetti sui router di servizio ASR serie 1000.
- Informazioni correlate al Qos
- Configurazione QoS sui router
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).