Dépannage des problèmes de routeur sur le réseau d'entreprise

Table des matières

Introduction

Ce document décrit comment identifier, dépanner et résoudre les problèmes de latence dans les réseaux d'entreprise à l'aide de routeurs Cisco.

Conditions préalables

Exigences

Il n'y a pas de prérequis ni de conditions spécifiques pour ce document.

Composants utilisés

Ce document n'est pas limité à une version logicielle et un type de matériel spécifiques, mais les commandes sont applicables aux routeurs Cisco IOS® XE tels que les gammes ASR 1000, ISR

4000 et Catalyst 8000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document décrit un guide de base pour comprendre, isoler et dépanner les problèmes généraux de latence. Il fournit des commandes/débogages utiles pour détecter les causes premières et les meilleures pratiques. Gardez à l'esprit que toutes les variables et tous les scénarios possibles ne peuvent pas être pris en compte et une analyse plus approfondie dépend de situations spécifiques.

Définition de la latence

En termes généraux, et en citant la définition stricte pour les périphériques de stockage et de transfert (sur RFC 1242), la latence est l'intervalle de temps commençant lorsque le dernier bit de la trame d'entrée atteint le port d'entrée et se terminant lorsque le premier bit de la trame de sortie est vu sur le port de sortie.

La latence du réseau peut simplement se référer au délai de transfert des données sur le réseau. Pour les questions pratiques, cette définition n'est que le point de départ ; vous devez définir le problème de latence dont vous parlez sur chaque cas spécifique, bien qu'il semble évident, la première étape nécessaire pour résoudre un problème, et qui devient vraiment importante, est de le définir.

Utilisation de la latence

De nombreuses applications nécessitent une faible latence pour les communications en temps réel et les opérations commerciales. Avec les améliorations matérielles et logicielles quotidiennes, davantage d'applications sont disponibles pour le calcul stratégique, les applications de réunion en ligne, la diffusion en continu, entre autres. De même, le trafic réseau continue de croître et le besoin de conceptions réseau optimisées et de meilleures performances des périphériques augmente également.

En plus d'améliorer l'expérience utilisateur et de fournir le minimum requis pour les applications sensibles à la latence, l'identification et la réduction efficaces des problèmes de latence sur un réseau peuvent permettre d'économiser beaucoup de temps et de ressources sur un réseau extrêmement précieux.

Problèmes de latence imminents

La partie difficile de ce type de problèmes est le nombre de variables que vous devez avoir en considération plus il ne peut pas y avoir un seul point de défaillance. Par conséquent, la définition

de la latence devient une clé importante pour la résoudre et certains aspects que vous devez prendre en considération pour avoir une description utile du problème sont les suivants.

1. Attentes et détection

Il est important de différencier la latence souhaitée, la latence de travail prévue ou de référence et la latence actuelle. En fonction de la conception, des fournisseurs ou des périphériques du réseau, il est parfois impossible d'obtenir la latence souhaitée. Il s'agit d'une bonne procédure pour mesurer la latence réelle dans des conditions normales, mais vous devez être cohérent sur les méthodes de mesure afin d'éviter les nombres trompeurs. Les SLA IP et les outils d'analyse du réseau peuvent vous aider à cet égard.

L'un des outils les plus utilisés et les plus basiques pour identifier la latence par les applications ou même IP SLA est via ICMP ou 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
```

Outre la vérification de l'accessibilité, la commande ping indique le temps de parcours aller-retour (RTT) de la source à la destination ; le minimum (2), la moyenne (109) et le maximum (541) en millisecondes. Cela signifie la durée entre le moment où le routeur envoie la requête et celui où il reçoit la réponse du périphérique de destination. Cependant, il ne montre pas le nombre de sauts ou d'informations plus détaillées, mais il s'agit d'un moyen facile et rapide de détecter un problème.

2. Isolement

Comme pour la commande ping, la commande traceroute peut être utilisée comme point de départ pour l'isolation. Elle détecte les sauts et le temps de transmission par saut :

<#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 fonctionne en envoyant un paquet avec une durée de vie (TTL) de 1. Le premier saut renvoie un message d'erreur ICMP indiquant que le paquet n'a pas pu être transféré car la durée de vie a expiré et que la durée de vie utile est mesurée. Le second paquet est alors renvoyé avec une durée de vie utile de 2 et le second saut renvoie la durée de vie utile expirée. Ce processus se poursuit jusqu'à ce que la destination soit atteinte.

Dans l'exemple, vous pouvez maintenant vous limiter à deux hôtes spécifiques et vous pouvez commencer à partir de là sur notre isolement.

Malgré ces commandes utiles qui peuvent facilement identifier un problème, elles ne prennent pas en considération d'autres variables telles que les protocoles, les marquages et les tailles de paquets (bien que vous puissiez les définir comme deuxième étape), les différentes sources IP, les destinations parmi plusieurs facteurs.

Dire que la latence peut être un concept très large et que vous ne voyez souvent que le symptôme sur une application, la navigation, l'appel ou des tâches spécifiques. L'une des premières choses à limiter est de comprendre l'impact et de définir le problème plus en détail, répondre aux questions suivantes et les éléments peuvent aider pour ce dimensionnement :

- La latence affecte-t-elle uniquement un type spécifique de trafic ou d'application ? Exemple : Uniquement UDP, TCP, ICMP...
- Si oui, ce trafic possède-t-il des identificateurs uniques ? Exemple : marquage QoS spécifique, tailles de paquets déterminées uniquement, options IP...
- Combien d'utilisateurs ou de sites sont concernés ? Exemple : Un seul sous-réseau spécifique, un ou deux hôtes finaux, un site entier connecté à un ou plusieurs périphériques...
- Des horodatages spécifiques ont-ils été identifiés ? Exemple : cela se produit-il seulement pendant les heures de pointe, n'importe quel modèle de temps ou aléatoire complète...
- Aspects de conception. Exemple : le trafic transitant par un périphérique spécifique, peut-être plusieurs périphériques mais se connectant à un seul fournisseur, le trafic équilibrant la charge mais affectant un chemin...

Bien d’autres considérations existent, mais le fait de croiser les différentes réponses (et même les tests qui peuvent être effectués pour y répondre) peut isoler et limiter efficacement la portée de la procédure de dépannage. À titre d'exemple, une seule application (trafic de même type) a affecté toutes les filiales passant par différents fournisseurs et se terminant sur le même data center aux heures de pointe. Dans ce cas, vous ne commencez pas à vérifier tous les commutateurs d'accès dans toutes les filiales, mais vous vous concentrez plutôt sur la collecte d'informations supplémentaires sur le data center et sur l'inspection de ce côté,

Les outils de surveillance et l'automatisation que vous pouvez avoir sur le réseau contribuent également beaucoup à cet isolement, qui dépend vraiment des ressources dont vous disposez et des situations uniques.

Dépanner les causes courantes

Une fois que vous avez limité la portée du dépannage, vous pouvez commencer à vérifier des causes spécifiques, par exemple, dans l’exemple de traceroute fourni, vous pouvez isoler deux sauts différents, puis vous limiter aux causes possibles.

Lié à la plateforme

CPU élevé

Une des causes courantes peut être un périphérique avec un CPU élevé qui retarde le traitement de tous les paquets. Pour les routeurs, la commande la plus utile et la plus simple à vérifier est

Performances globales du routeur :

<#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 pour voir l'utilisation de la mémoire et du processeur à la fois, il est divisé sur le plan de contrôle et le plan de données (QFP) de la même manière que les seuils pour chacun. La mémoire elle-même ne crée pas de problème de latence. Cependant, s'il n'y a plus de mémoire DRAM pour le plan de contrôle, Cisco Express Forwarding (CEF) est désactivé et induit une utilisation élevée du CPU qui peut produire une latence, c'est pourquoi il est important de maintenir les nombres dans un état sain. Le guide de base pour le dépannage de la mémoire n'est pas inclus, mais reportez-vous au lien utile de la section Informations connexes.

Si une utilisation CPU élevée est détectée pour Control Processor, QFP CPU ou Crypto, vous pouvez utiliser les commandes suivantes :

Pour le plan de contrôle :

show process cpu sorted

<#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
```

Si le CPU du plan de contrôle est élevé (cet exemple est à 99% en raison des processus), besoin

d'isoler le processus et, en fonction de lui, procéder à l'isolation (peut être pointé paquets pour nous comme ARP ou des paquets de réseau de contrôle, peut être tout protocole de routage, multidiffusion, NAT, DNS, trafic de chiffrement ou tout service).

Selon votre flux de trafic, cela peut entraîner un problème lors du traitement ultérieur. Si le trafic n'est pas destiné au routeur, vous pouvez vous concentrer sur le plan de données :

Pour le plan de données :

show platform hardware qfp active datapath utilisation [summary]

<#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
```

Si le plan de données est élevé (identifié par un nombre de charges de traitement atteignant 100 %), vous devez voir la quantité de trafic passant par le routeur (nombre total de paquets par seconde et de bits par seconde) et les performances de débit de la plate-forme (vous pouvez vous faire une idée sur une fiche technique spécifique).

Afin de déterminer si ce trafic est attendu ou non, la capture de paquets (EPC) ou toute fonctionnalité de surveillance telle que Netflow peuvent être utilisées pour une analyse plus approfondie, certaines vérifications sont :

- Le trafic est-il valide et doit-il passer par ce routeur ?
- Identifiez les flux de trafic anormaux ou les débits supérieurs.
- Si vous avez des nombres élevés de paquets par seconde, recherchez la taille des paquets. Déterminez si cela est attendu ou si vous rencontrez un problème de fragmentation.

Si tout le trafic est attendu, vous pouvez atteindre une limite de plate-forme, puis, rechercher les fonctionnalités exécutées sur votre routeur comme une deuxième partie pour l'analyse via show running-config, principalement sur les interfaces, identIfy toutes les fonctionnalités inutiles et les désactiver ou équilibrer le trafic pour libérer des cycles CPU.

Cependant, s'il n'y a aucune indication d'une limite de plate-forme, un autre outil utile pour corroborer si le routeur ajoute un délai sur les paquets est la trace FIA, vous pouvez voir le temps de traitement exact passé pour chaque paquet et les fonctionnalités prenant la plupart du traitement. Le dépannage complet de l'UC élevée n'est pas traité dans ce document, mais reportez-vous aux liens de la section Informations connexes.

Lié au trafic

MTU et fragmentation

L'unité de transmission maximale (MTU) est la longueur maximale de paquet à transmettre, qui dépend du nombre d'octets que les liaisons physiques peuvent transporter.Lorsque les protocoles de couche supérieure envoient des données à l’adresse IP sous-jacente et que la longueur résultante du paquet IP est supérieure à la MTU du chemin, le paquet est divisé en fragments. Cette taille plus faible sur le réseau entraîne plus de traitement et un traitement différent dans certains cas et c'est pourquoi vous devez l'éviter autant que possible.

Pour certaines fonctionnalités telles que NAT ou le pare-feu basé sur les zones, le réassemblage virtuel est nécessaire pour « avoir le paquet entier », applique ce qui est nécessaire, transfère ses fragments et rejette la copie réassemblée. Ce processus ajoute des cycles CPU et il est sujet à des erreurs.

Certaines applications ne dépendent pas de la fragmentation, l'un des tests les plus basiques pour vérifier la MTU est une requête ping avec une option no fragment et tester différentes tailles de paquets : ping ip-address df-bit size number. Si la requête ping échoue, corrigez la MTU sur le chemin lorsque la suppression se produit et provoque d'autres problèmes.

Des fonctionnalités, telles que le routage basé sur des politiques et le multichemin à coût égal sur un réseau avec des paquets fragmentés peuvent créer des problèmes de délai et plus d'erreurs,

principalement sur des débits de données élevés, ce qui entraîne des temps d'assemblage élevés, des ID en double et des paquets endommagés. Si certains de ces problèmes sont identifiés, essayez de résoudre cette fragmentation autant que possible. Une commande pour vérifier si vous avez des fragments et des problèmes potentiels est 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>
```

À partir du résultat ci-dessus, les mots en gras de la section Frags se réfèrent à :

- Reassemblé : nombre de paquets réassemblés.
- Timeouts : chaque fois que le temps de réassemblage d'un fragment de paquet expire.
- Impossible de réassembler : nombre de paquets qui n'ont pas pu être réassemblés.
- Fragmented : nombre de paquets dépassant le MTU et objet de la fragmentation.
- Fragments : nombre de segments dans lesquels les paquets ont été fragmentés.
- Impossible de fragmenter : nombre de paquets dépassant MTU mais n'ayant pas pu être fragmentés.

Si la fragmentation est utilisée et que vous avez des délais d'attente ou que vous n'avez pas pu réassembler les compteurs augmentent, une façon de corroborer les problèmes causés par la plate-forme, est via les abandons QFP, en utilisant la même commande que expliquée plus loin sur la section abandons : show platform hardware qfp active statistics drop. Recherchez des erreurs telles que : TcpBadfrag, IpFragErr, FragTailDrop, ReassDrop, ReassFragTooBig, ReassTooManyFrags, ReassTimeout ou des erreurs connexes. Chaque cas peut avoir différentes causes comme ne pas obtenir tous les fragments, dupliqué, congestion CPU entre autres. Là encore, des outils utiles pour une analyse plus approfondie et une correction potentielle peuvent être un suivi FIA et une vérification de la configuration.

TCP offre un mécanisme de taille de segment maximale (MSS) pour résoudre ce problème, mais il peut induire une latence si le MTU du chemin découvert est incorrect, non négocié par MSS ou incorrect.

Comme le protocole UDP ne dispose pas de ce mécanisme de fragmentation, vous pouvez compter sur l'implémentation manuelle de PMTD ou de toute solution de couche application. Vous pouvez les activer (le cas échéant) pour envoyer des paquets de moins de 576 octets, ce qui correspond à la MTU effective la plus petite pour l'envoi du numéro conformément à la RFC1122, afin d'éviter la fragmentation.

Lié à la conception

Plus qu'une suggestion de dépannage, cette section décrit brièvement deux autres composants clés qui peuvent ajouter des problèmes de latence et qui nécessitent une discussion et une analyse approfondies hors du cadre de ce document.

Routage non optimal

Le routage sous-optimal dans un réseau fait référence à une situation dans laquelle les paquets de données ne sont pas acheminés par le chemin le plus efficace ou le plus court disponible sur un réseau. Au lieu de cela, ces paquets empruntent une route moins efficace, ce qui peut augmenter la latence, l'encombrement ou affecter les performances du réseau. Les protocoles IGP choisissent toujours les meilleurs chemins, ce qui signifie un coût plus faible, mais ce n'est pas nécessairement le chemin le moins cher ou le plus lent (le meilleur peut être celui avec une bande passante plus élevée).

Un routage non optimal peut survenir pour des problèmes liés aux protocoles de routage ; configuration ou toute situation telle que les conditions de concurrence, les modifications dynamiques (modifications de topologie ou défaillances de liaison), l’ingénierie du trafic prévue en

fonction des politiques ou des coûts de l'entreprise, les redondances ou les basculements (passage sur le chemin de secours dans certaines conditions), entre autres situations.

Des outils tels que traceroutes ou l'appliance de surveillance peuvent aider à identifier cette situation pour des flux spécifiques, si c'est le cas, et dépend de nombreux autres facteurs, satisfaire les demandes des applications et une latence plus faible peut nécessiter une nouvelle conception du routage ou une ingénierie du trafic.

Qualité de service (QoS)

En configurant la qualité de service (QoS), vous pouvez accorder un traitement préférentiel à des types de trafic spécifiques au détriment d'autres types de trafic. Sans QoS, le périphérique offre un service au mieux pour chaque paquet, quelle que soit sa taille ou son contenu.
Les périphérique envoie les paquets sans aucune garantie de fiabilité, de limites de délai ou de débit.

Si la QoS est en place, il devient vraiment important d'identifier si le routeur marque, marque à nouveau ou classifie simplement les paquets, vérifiez la configuration et show policy-map [nom_de_policy_map | session | interface interface_id] aide à comprendre les classes affectées par des débits élevés, des abandons ou des paquets mal classés.

La mise en oeuvre de la qualité de service est une tâche lourde qui nécessite une analyse sérieuse et sort du cadre de ce document, mais il est fortement recommandé d'en tenir compte pour hiérarchiser les applications urgentes et résoudre ou prévenir de nombreux problèmes de latence et d'applications.

Autres problèmes de performances

D'autres conditions peuvent ajouter de la lenteur, une reconnexion de session ou de mauvaises performances générales que vous devez vérifier, parmi lesquelles :

Gouttes

Un problème directement lié au traitement sur un périphérique est les abandons de paquets, vous devez vérifier le côté entrée et sortie du point de vue de l'interface :

<#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#
```

Côté entrée, vous avez :

- Abandons de la file d'attente d'entrée : chaque interface possède une file d'attente d'entrée (il s'agit d'un tampon logiciel qui peut être modifié) dans laquelle les paquets entrants sont placés en attente de traitement par le processeur de routage (RP). si le taux de paquets entrants placés sur la file d'attente d'entrée dépasse le taux auquel le RP peut traiter les paquets, vous pouvez avoir un incrément de abandons. Cependant, sachez que seuls les paquets de contrôle et le trafic « Pour nous » sont placés, par conséquent, si la latence est visible lors du passage du trafic, même si vous avez des pertes sporadiques, cela ne doit pas être une cause.

- Dépassements de capacité : cela se produit lorsque le matériel du récepteur ne peut pas remettre les paquets reçus à une mémoire tampon matérielle parce que le débit d'entrée dépasse la capacité du récepteur à traiter les données. Ce nombre peut indiquer un problème de débit et de performances du routeur, capturer le trafic uniquement pour cette interface et rechercher les pics de trafic. Une solution de contournement courante consiste à activer le contrôle de flux, mais cela peut augmenter le délai des paquets. Cela peut également être une preuve de goulots d'étranglement et de sursouscription.
- CRC : se produit en raison de problèmes physiques, vérifier le câblage, les ports et les SFP correctement connectés et le bon fonctionnement.

Côté sortie, vous avez :

- Extinction de la file d'attente de sortie : chaque interface possède une file d'attente de sortie dans laquelle sont placés les paquets sortants à envoyer sur l'interface. Parfois, le débit des paquets sortants placés sur la file d'attente de sortie par le RP dépasse le débit auquel l'interface peut envoyer les paquets. Cela peut causer des problèmes de performances et de latence s'il n'y a pas de QoS en place, sinon, vous pouvez avoir ce nombre croissant en raison de certaines politiques appliquées et conseiller de vérifier ou d'implémenter la configuration de QoS pour protéger et assurer le trafic prévu ou critique.

Enfin, les abandons sur QFP sont directement liés à un traitement élevé qui peut provoquer une latence, vérifiez via 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
```

Les causes dépendent du code, FIA trace aide à corroborer ou à rejeter si le trafic affecté par la latence est abandonné à ce stade.

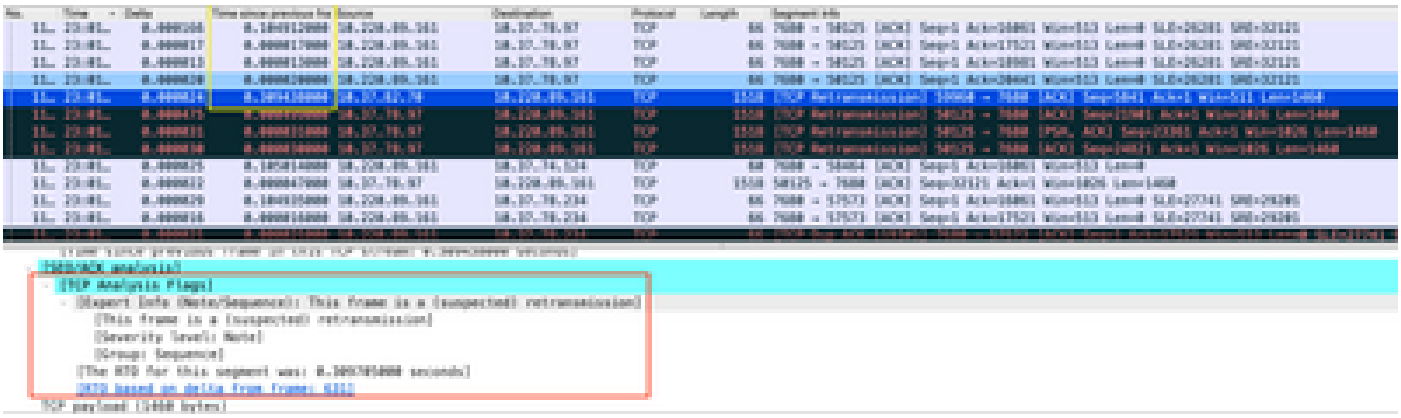
Retransmission TCP

La retransmission TCP est un symptôme ou peut être une conséquence due à un problème sous-jacent tel que la perte de paquets. Ce problème peut entraîner des problèmes de lenteur et de mauvaises performances sur l'application.

Le protocole de contrôle de transmission (TCP) utilise un temporisateur de retransmission pour assurer la livraison des données en l'absence de rétroaction de la part du récepteur de données distant. La durée de ce temporisateur est appelée RTO (Retransmission Timeout). Lorsque le délai de retransmission expire, l’émetteur retransmet le segment le plus ancien qui n’a pas été accusé de réception par le récepteur TCP et le RTO est augmenté.

Certaines retransmissions ne peuvent pas être éliminées complètement, si elles sont minimales, il ne peut pas refléter un problème. Cependant, comme vous pouvez le déduire, plus de retransmissions sont observées, plus la session TCP est en latence et doit être traitée.

La capture de paquets analysée dans Wireshark peut corroborer le problème comme exemple suivant :



Capture de conversation TCP

En cas de retransmissions, utilisez la même méthode de capture sur les directions d'entrée et de sortie du routeur pour vérifier tous les paquets envoyés et reçus. Bien sûr, cette opération peut représenter un effort considérable. Il est donc nécessaire d'effectuer une analyse détaillée de la capture pour TCP, en examinant les TTL, les temps des trames précédentes sur le même flux TCP afin de comprendre dans quelle direction (serveur ou client) vous avez ce retard ou ce manque de réponse pour diriger votre dépannage.

Surabonnement et goulots d'étranglement

Un surabonnement se produit lorsque les ressources requises (bande passante) sont supérieures aux ressources réellement disponibles. Les commandes permettant d'identifier si vous rencontrez ce problème sur un routeur ont déjà été traitées dans la section précédente.

Par conséquent, des goulots d'étranglement peuvent se produire lorsque les flux de trafic sont ralentis en raison d'une bande passante ou d'une capacité matérielle insuffisante. Il est important d'identifier si cela se produit dans un court laps de temps ou s'il s'agit d'une situation à long terme pour appliquer des solutions.

Il n'y a pas de conseil spécifique pour le résoudre, mais certaines options sont l'équilibrage du trafic vers différentes plates-formes, le segment du réseau ou la mise à niveau vers des périphériques plus robustes en fonction des besoins actuels et de l'analyse de la croissance future.

Informations connexes

- IP SLA Opérations d'écho ICMP
- Dépannage de la mémoire
- Dépannage avec la fonctionnalité de suivi des paquets de chemin de données Cisco IOS-XE
- Dépannez les pertes de paquets sur les routeurs de service de la gamme ASR 1000.
- Informations relatives à Qos
- Configuration QoS sur les routeurs
- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.