Fehlerbehebung bei Routerproblemen im Unternehmensnetzwerk

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Latenzprobleme in Enterprise Networks mithilfe von Cisco Routern identifizieren, beheben und beheben.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen oder Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Softwareversionen und Hardwaretypen beschränkt. Die Befehle gelten jedoch für Cisco IOS® XE-Router wie die ASR 1000-, ISR 4000- und Catalyst

8000-Produktfamilien.

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

Hintergrundinformationen

In diesem Dokument wird ein grundlegender Leitfaden für das Verständnis, die Isolierung und die Fehlerbehebung bei allgemeinen Latenzproblemen beschrieben. Darüber hinaus enthält es nützliche Befehle/Debugging-Anweisungen zum Erkennen der Ursachen und Best Practices. Beachten Sie, dass nicht alle möglichen Variablen und Szenarien berücksichtigt werden können und eine tiefere Analyse von bestimmten Situationen abhängt.

Latenzdefinition

Generell und unter Bezugnahme auf die strenge Definition für Speicher- und Weiterleitungsgeräte (auf RFC 1242) ist Latenz das Zeitintervall, das beginnt, wenn das letzte Bit des Eingangsrahmens den Eingangsport erreicht, und endet, wenn das erste Bit des Ausgangsrahmens auf dem Ausgangsport zu sehen ist.

Netzwerklatenz kann sich einfach auf Verzögerungen bei der Datenübertragung im Netzwerk beziehen. Für praktische Fragen ist diese Definition nur der Ausgangspunkt; Sie müssen das Latenzproblem definieren, über das Sie in jedem einzelnen Fall sprechen, obwohl es offensichtlich scheint, ist der erste Schritt, der notwendig ist, um ein Problem zu lösen, und wirklich wichtig wird, es zu definieren.

Latenznutzung

Viele Anwendungen benötigen eine niedrige Latenz für Kommunikation in Echtzeit und für Geschäftsabläufe. Aufgrund der Verbesserungen an Hardware und Software, die jeden Tag vorgenommen werden, stehen mehr Anwendungen für geschäftskritische Berechnungen, Online-Meeting-Anwendungen und Streaming zur Verfügung. Auf die gleiche Weise nimmt der Netzwerkverkehr weiter zu und der Bedarf an optimierten Netzwerkdesigns und einer höheren Geräteleistung steigt.

Neben einer besseren Benutzererfahrung und der Bereitstellung des Mindestbedarfs für latenzempfindliche Anwendungen kann die effektive Erkennung und Verringerung von Latenzproblemen in einem Netzwerk viel Zeit und Ressourcen einsparen, die in einem Netzwerk besonders wertvoll sind.

Probleme mit Latenzzeiten

Der schwierige Teil dieser Art von Problemen ist die Anzahl der Variablen, die Sie in Betracht

ziehen müssen, und es kann keinen einzigen Fehlerpunkt geben. Daher wird die Definition von Latenz zu einem wichtigen Schlüssel, um es zu lösen, und einige Aspekte, die Sie berücksichtigen müssen, um eine nützliche Problembeschreibung haben, sind die nächsten.

1. Erwartungen und Erkennung

Es ist wichtig, zwischen einer gewünschten Latenz, der erwarteten oder Basisarbeitslatenz und der aktuellen zu unterscheiden. Je nach Design, Anbieter oder Geräte im Netzwerk, manchmal können Sie nicht die gewünschte Latenz zu erreichen, ist es ein gutes Verfahren, um die reale unter normalen Bedingungen zu messen, aber Sie müssen konsistente Messmethoden zu vermeiden irreführende Zahlen; IP SLAs und Netzwerk-Analyse-Tools können in dieser Hinsicht helfen.

Eines der am häufigsten verwendeten und grundlegenden Tools zum Identifizieren von Latenzen nach Anwendungen oder sogar IP SLA ist ICMP oder 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
```

Abgesehen von der Überprüfung der Erreichbarkeit teilt ping die Round Trip Time (RTT) von der Quelle bis zum Ziel mit; das Minimum (2), den Durchschnitt (109) und das Maximum (541) in Millisekunden. Das bedeutet, die Dauer, ab der der Router die Anforderung sendet, bis er die Antwort vom Geräteziel erhält. Allerdings zeigt es nicht, wie viele Hops oder tiefere Informationen, aber es ist eine einfache und schnelle Möglichkeit, ein Problem zu erkennen.

2. Isolierung

Wie beim Ping kann die Traceroute als Ausgangspunkt für die Isolierung verwendet werden. Dabei werden Hops und RTT pro Hop erkannt:

<#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 sendet ein Paket mit einer TimeTo Live (TTL) von 1. Der erste Hop sendet eine ICMP-Fehlermeldung zurück, die besagt, dass das Paket nicht weitergeleitet werden konnte, da die TTL abgelaufen und RTT gemessen wurde. Das zweite Paket wird dann mit einer TTL von 2 erneut gesendet, und der zweite Hop gibt die abgelaufene TTL zurück. Dieser Prozess wird fortgesetzt, bis das Ziel erreicht ist.

In diesem Beispiel können Sie sich jetzt auf zwei spezifische Hosts einschränken und von dort aus mit unserer Isolation beginnen.

Obwohl es sich hierbei um nützliche Befehle handelt, die ein Problem leicht identifizieren können, berücksichtigen sie keine anderen Variablen wie Protokolle, Paketmarkierungen und -größen (obwohl Sie diese als zweiten Schritt festlegen können), verschiedene IP-Quellen und Ziele unter mehreren Faktoren.

Latenz kann ein sehr weit gefasstes Konzept sein, und Sie sehen häufig nur das Symptom einer Anwendung, eines Surfens, eines Anrufs oder bestimmter Aufgaben. Zunächst gilt es, die Auswirkungen zu verstehen und das Problem genauer zu definieren. Die nächsten Fragen und Elemente können bei der Dimensionierung hilfreich sein:

- Betrifft die Latenz nur bestimmte Arten von Datenverkehr oder Anwendungen? Beispiel: Nur UDP, TCP, ICMP...
- Wenn ja, verfügt dieser Datenverkehr über eindeutige Bezeichner? Beispiel: Spezifische QoS-Markierung, nur bestimmte Paketgrößen, IP-Optionen...
- Wie viele Benutzer oder Standorte sind betroffen? Beispiel: Nur ein bestimmtes Subnetz, ein oder zwei End-Hosts, ein ganzer Standort verbunden mit einem oder mehreren Geräten...
- Gibt es bestimmte Zeitstempel? Beispiel: tritt dies nur während Spitzenzeiten, jedes Zeitmuster oder vollständig zufällig...
- Design-Aspekte. Beispiel: Datenverkehr, der ein bestimmtes Gerät durchläuft, z. B. viele Geräte, aber nur mit einem Anbieter verbunden ist, wobei der Datenverkehr die Last ausgleicht, aber einen Pfad beeinflusst...

Es gibt noch viele weitere Überlegungen, aber das Überkreuzen der verschiedenen Antworten (und sogar Tests, die durchgeführt werden können, um sie zu beantworten) kann den Umfang für die Fehlerbehebung effektiv isolieren und einschränken. Beispielsweise ist nur eine Anwendung (Datenverkehr derselben Art) in allen Zweigstellen betroffen, die über verschiedene Anbieter geleitet werden und zu Spitzenzeiten im selben Rechenzentrum enden. In diesem Fall überprüfen Sie nicht alle Access Switches in allen Zweigstellen, sondern konzentrieren sich auf das Sammeln von weiteren Informationen zum Rechenzentrum und führen weitere Prüfungen auf dieser Seite durch.

Überwachungstools und einige Automatisierungsfunktionen im Netzwerk tragen ebenfalls wesentlich zu dieser Isolierung bei und sind abhängig von den vorhandenen Ressourcen und den jeweiligen Situationen.

Fehlerbehebung häufiger Ursachen

Sobald Sie den Umfang der Fehlerbehebung eingeschränkt haben, können Sie mit der Prüfung bestimmter Ursachen beginnen, z. B. bei dem angegebenen Beispiel für die Traceroute. Sie können zwei verschiedene Hops isolieren und dann auf mögliche Ursachen eingrenzen.

Plattformbezogen

Hohe CPU-Auslastung

Eine der häufigsten Ursachen kann ein Gerät mit hoher CPU sein, das Verzögerungen bei der Verarbeitung aller Pakete verursacht. Bei Routern sind der nützlichste und einfachste Befehl zum Überprüfen von Routern

Gesamtleistung des Routers:

<#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
```

Die Auslastung von Arbeitsspeicher und CPU kann sofort angezeigt werden. Sie ist auf der Kontroll- und Datenebene (QFP) aufgeteilt und entspricht den Schwellenwerten für die einzelnen Ebenen. Der Speicher selbst verursacht kein Latenzproblem. Wenn jedoch kein DRAM-Speicher mehr für die Steuerungsebene vorhanden ist, wird Cisco Express Forwarding (CEF) deaktiviert, und es wird eine hohe CPU-Auslastung ausgelöst, die zu Latenz führen kann. Aus diesem Grund ist es wichtig, die Zahlen auf einem gesunden Zustand zu halten. Grundlegende Anleitungen zur Speicherfehlerbehebung sind nicht im Umfang enthalten. Weitere Informationen finden Sie unter dem entsprechenden Link im Abschnitt .

Wenn eine hohe CPU-Auslastung bei der Verwendung von Control Processor, QFP-CPU oder Crypto erkannt wird, können Sie die folgenden Befehle verwenden:

Für Kontrollebene:

Prozess-CPU sortiert anzeigen

<#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
```

Wenn die Kontrollebenen-CPU hoch ist (dieses Beispiel liegt wegen der Prozesse bei 99 %), müssen Sie den Prozess isolieren und, abhängig davon, mit der Isolierung fortfahren (kann für uns Pakete wie ARP oder Kontrollnetzwerkpakete gestoppt werden, kann jedes Routing-Protokoll, Multicast, NAT, DNS, Krypto-Verkehr oder irgendein Dienst sein).

Je nach Datenverkehrsfluss kann dies zu Problemen bei der weiteren Verarbeitung führen. Wenn der Datenverkehr nicht an den Router gerichtet ist, können Sie sich auf die Datenebene konzentrieren:

Für Datenebene:

show platform hardware qfp active datapath usage [Zusammenfassung]

<#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
```

Wenn die Datenebene hoch ist (durch die Anzahl der Verarbeitungslasten, die 100 % erreicht), müssen Sie die Menge des über den Router geleiteten Datenverkehrs (Gesamtpaket pro Sekunde und Bits pro Sekunde) und die Durchsatzleistung der Plattform sehen (Sie können eine Idee auf einem bestimmten Datenblatt haben).

Um festzustellen, ob dieser Datenverkehr erwartet wird oder nicht, können die Paketerfassung (Packet Capture, EPC) oder Überwachungsfunktionen wie Netflow für weitere Analysen verwendet werden. Hierbei werden folgende Prüfungen durchgeführt:

- Ist der Datenverkehr gültig und wird dieser Router voraussichtlich passieren?
- Erkennen Sie ungewöhnliche Datenverkehrsflüsse oder höhere Geschwindigkeiten.
- Wenn Sie hohe Paketraten pro Sekunde haben, achten Sie auf die Größe der Pakete. Stellen Sie fest, ob dies angezeigt wird oder ob ein Fragmentierungsproblem vorliegt.

Wenn der gesamte Datenverkehr erwartet wird, erreichen Sie möglicherweise eine Plattformbeschränkung. Suchen Sie dann im zweiten Teil nach den Funktionen, die auf Ihrem Router ausgeführt werden, und analysieren Sie sie mithilfe von show running-config, hauptsächlich auf den Schnittstellen, identIfy alle unnötigen Funktionen, und deaktivieren Sie sie, oder gleichen Sie den Datenverkehr aus, um CPU-Zyklen freizugeben.

Wenn es jedoch keinen Hinweis auf eine Plattformgrenze gibt, kann ein weiteres nützliches Tool zur Bestätigung, ob der Router Verzögerungen bei Paketen hinzufügt, die FIA-Verfolgung sein. Sie können die genaue Prozesszeit für jedes Paket und die Funktionen, die den größten Teil der Verarbeitung ausmachen, sehen. Die vollständige CPU-Fehlerbehebung wird in diesem Dokument nicht behandelt. Weitere Informationen finden Sie unter den Links im Abschnitt "Verwandte Informationen".

Datenverkehrsbezogen

MTU und Fragmentierung

Maximum Transmission Unit (MTU) (Maximale Übertragungseinheit): Die maximale Paketlänge, die übertragen wird, hängt von der Anzahl der Oktetts ab, die physische Verbindungen übertragen können.Wenn Protokolle höherer Layer Daten an die zugrunde liegende IP-Adresse senden und die resultierende Länge des IP-Pakets größer ist als die MTU des Pfads, wird das Paket in Fragmente unterteilt. Diese geringeren Netzwerkgrößen führen in einigen Fällen zu mehr Verarbeitung und unterschiedlichen Behandlungen, und deshalb müssen Sie sie so weit wie möglich vermeiden.

Bei einigen Funktionen wie NAT oder Zone Based Firewall ist eine virtuelle Reassemblierung erforderlich, um das gesamte Paket zu erhalten. Dabei werden die erforderlichen Komponenten angewendet, die Fragmente weitergeleitet und die reassemblierte Kopie verworfen. Dieser Prozess verlängert die CPU-Zyklen und ist anfällig für Fehler.

Einige Anwendungen basieren nicht auf Fragmentierung. Einer der einfachsten Tests zur Prüfung der MTU ist ein Ping ohne Fragmentoption, mit dem verschiedene Paketgrößen getestet werden: Ping IP-Adresse DF-Bitgröße. Wenn Ping nicht erfolgreich ist, reparieren Sie die MTU über den Pfad, während das Drop auftritt und weitere Probleme verursacht.

Funktionen wie richtlinienbasiertes Routing und Multipath mit gleichen Kosten in einem Netzwerk mit fragmentierten Paketen können Verzögerungsprobleme und mehr Fehler verursachen, vor allem bei hohen Datenraten, was zu hohen Assemblierungszeiten, doppelten IDs und beschädigten Paketen führt. Wenn einige dieser Probleme erkannt werden, achten Sie darauf, diese Fragmentierung so weit wie möglich zu beheben. Mit dem folgenden Befehl können Sie überprüfen, ob Fragmente vorhanden sind und mögliche Probleme auftreten: 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>
```

Aus der obigen Ausgabe beziehen sich fette Wörter auf den Abschnitt Frags auf:

- Reassembliert: Anzahl der reassemblierten Pakete
- Timeouts: Jedes Mal, wenn die Reassemblierungszeit für ein Paketfragment abläuft.
- Konnte nicht wieder zusammengesetzt werden: Anzahl der Pakete, die nicht wieder zusammengesetzt werden konnten
- Fragmentiert: Anzahl der Pakete, die MTU überschreiten und fragmentiert werden müssen.
- Fragmente: Anzahl der Blöcke, in die Pakete fragmentiert wurden
- Konnte nicht fragmentiert werden: Anzahl der Pakete, die MTU überschreiten, konnte aber nicht fragmentiert werden.

Wenn die Fragmentierung verwendet wird und Sie Zeitüberschreitungen haben oder die Zähler nicht wieder zusammensetzen konnten, erhöhen sich die durch die Plattform verursachten Probleme durch QFP-Drops. Verwenden Sie dazu den gleichen Befehl wie weiter unten im Abschnitt "Drops" erläutert: show platform hardware qfp active statistics drop. Suchen Sie nach Fehlern wie: TcpBadfrag, IpFragErr, FragTailDrop, ReassDrop, ReassFragTooBig, ReassTooManyFrags, ReassTimeout oder ähnlichen. Jeder Fall kann unterschiedliche Ursachen haben, wie z. B. nicht alle Fragmente zu erhalten, dupliziert, CPU-Überlastung unter anderem. Auch hier können nützliche Tools für weitere Analysen und mögliche Korrekturen eine FIA-Ablaufverfolgungs- und Konfigurationsprüfung sein.

TCP bietet einen MSS-Mechanismus (Maximum Segment Size), um dieses Problem zu beheben. Es kann jedoch zu einer Latenz führen, wenn eine falsche, nicht von MSS ausgehandelte oder falsche Pfad-MTU erkannt wird.

Da UDP nicht über diesen Fragmentierungsmechanismus verfügt, können Sie sich auf die manuelle Implementierung von PMTD oder einer Lösung auf Anwendungsebene verlassen. Sie können diese (falls zutreffend) aktivieren, um Pakete mit einer Größe von weniger als 576 Byte zu senden. Dies ist die kleinere effektive MTU für die Sendeanzahl gemäß RFC1122, um eine Fragmentierung zu vermeiden.

Design-bezogen

In diesem Abschnitt werden nicht nur Vorschläge zur Fehlerbehebung gemacht, sondern auch zwei weitere Schlüsselkomponenten beschrieben, die zu Latenzproblemen führen können. Diese Komponenten erfordern eine ausführliche Erörterung und Analyse außerhalb des Rahmens dieses Dokuments.

Suboptimales Routing

Suboptimales Routing im Netzwerk bezeichnet eine Situation, in der Datenpakete nicht über den effizientesten oder kürzesten verfügbaren Pfad in einem Netzwerk geleitet werden. Stattdessen werden diese Pakete auf einer weniger effizienten Route übertragen, was zu einer höheren

Latenz, Überlastung oder einer Beeinträchtigung der Netzwerkleistung führen kann. IGPs wählen immer die besten Pfade aus, d. h. die geringeren Kosten, sind aber nicht unbedingt der billigste oder der niedrigste Verzögerungspfad (am besten geeignet für Pfade mit höherer Bandbreite).

Bei Problemen mit Routing-Protokollen kann es zu suboptimalem Routing kommen. Entweder bei der Konfiguration oder in Situationen wie Rennbedingungen, dynamischen Änderungen (Topologieänderungen oder Verbindungsausfälle), bei beabsichtigten Traffic-Engineering auf Basis von Unternehmensrichtlinien oder Kosten, Redundanzen oder Failovers (unter bestimmten Bedingungen Weiterleitung an den Backup-Pfad).

Tools wie Traceroutes oder Monitoring-Appliances können dabei helfen, diese Situation für bestimmte Datenflüsse zu identifizieren. Wenn dies der Fall ist, hängt dies von vielen anderen Faktoren ab, erfüllen die Anwendungsanforderungen, und eine geringere Latenz kann eine Umgestaltung des Routings oder ein Traffic Engineering erfordern.

Quality of Service (QoS)

Durch die Konfiguration der Quality of Service (QoS) können Sie bestimmte Datenverkehrstypen auf Kosten anderer Datenverkehrstypen bevorzugt behandeln. Ohne QoS "slot0:" bietet bestmöglichen Service für jedes Paket, unabhängig vom Paketinhalt oder der Größe. Die Fehlermeldung "slot0:" sendet die Pakete ohne Gewähr für Zuverlässigkeit, Verzögerungsgrenzen oder Durchsatz.

Wenn QoS vorhanden ist, ist es sehr wichtig, zu erkennen, ob Router die Pakete markiert, neu kennzeichnet oder nur klassifiziert, die Konfiguration zu überprüfen und die Richtlinienzuordnung anzuzeigen [name_of_policy_map | Sitzung | interface_id] hilft, Klassen zu verstehen, die von hohen Raten, Verwerfungen oder falsch klassifizierten Paketen betroffen sind.

Die Implementierung von QoS ist eine anspruchsvolle Aufgabe, die eine ernsthafte Analyse erfordert und nicht im Rahmen dieses Dokuments behandelt wird. Es wird jedoch dringend empfohlen, diese Aufgabe zu berücksichtigen, um zeitkritische Anwendungen zu priorisieren und viele Latenz- und Anwendungsprobleme zu beheben oder zu vermeiden.

Andere Leistungsprobleme

Andere Bedingungen können Langsamkeit, Sitzungswiederherstellung oder allgemein schlechte Leistung, die Sie überprüfen müssen, hinzufügen, einige von ihnen sind:

Herunterfallen

Ein Problem, das direkt mit der Verarbeitung auf einem Gerät in Zusammenhang steht, sind Paketverluste. Sie müssen die Eingangs- und Ausgangsseite aus Schnittstellensicht überprüfen:

<#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#
```

Auf der Eingabeseite haben Sie:

- Verwerfungen der Eingabewarteschlange: Jede Schnittstelle verfügt über eine Eingabewarteschlange (dies ist ein Softwarepuffer, der geändert werden kann), in der die eingehenden Pakete auf die Verarbeitung durch den Routing-Prozessor (RP) warten. Wenn die Rate der eingehenden Pakete in der Eingangswarteschlange die Rate überschreitet, mit der der RP die Pakete verarbeiten kann, für die ein Drop-Inkrement möglich ist. Beachten Sie jedoch, dass nur Steuerungspakete und Datenverkehr "für uns" platziert werden. Wenn also beim Passieren von Datenverkehr eine Latenz auftritt, selbst wenn es zu sporadischen Verlusten kommt, darf dies keine Ursache sein.
- Überläufe: Dies tritt auf, wenn die Empfängerhardware die empfangenen Pakete nicht an einen Hardwarepuffer übergeben kann, weil die Eingaberate die Fähigkeit des Empfängers,

die Daten zu verarbeiten, übersteigt. Diese Zahl kann auf ein Problem mit der Geschwindigkeit und Leistung des Routers hinweisen, den Datenverkehr nur für diese Schnittstelle erfassen und nach Datenverkehrsspitzen suchen. Eine gängige Problemumgehung besteht in der Aktivierung der Flusskontrolle. Dies kann jedoch zu Verzögerungen bei Paketen führen. Dies kann auch ein Beweis für Engpässe und Überbelegung sein.
- CRCs: Tritt aufgrund von physischen Problemen auf, überprüfen Sie die Verkabelung, die richtig verbundenen Ports und SFPs und die ordnungsgemäße Funktion.

Auf der Ausgabeseite haben Sie:

- Ausgabewarteschlangenverluste: Jede Schnittstelle verfügt über eine Ausgabewarteschlange, in der die ausgehenden Pakete platziert werden, die über die Schnittstelle gesendet werden sollen. Manchmal übersteigt die Rate für ausgehende Pakete, die vom RP in die Ausgabewarteschlange gestellt werden, die Rate, mit der die Schnittstelle die Pakete senden kann. Dies kann Leistungsprobleme und Latenzprobleme verursachen, wenn kein QoS vorhanden ist. Andernfalls können Sie diese Anzahl aufgrund bestimmter angewendeter Richtlinien erhöhen und empfehlen, die QoS-Konfiguration zu überprüfen oder zu implementieren, um beabsichtigten oder kritischen Datenverkehr zu schützen und sicherzustellen.

Und schließlich, Drops auf QFP ist direkt auf hohe Verarbeitung, die Latenz verursachen können, Prüfung über 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
```

Ursachen hängen vom Code ab. FIA-Ablaufverfolgung unterstützt die Bestätigung oder das Verwerfen, wenn der von der Latenz betroffene Datenverkehr an dieser Stelle verworfen wird.

TCP-Neuübertragung

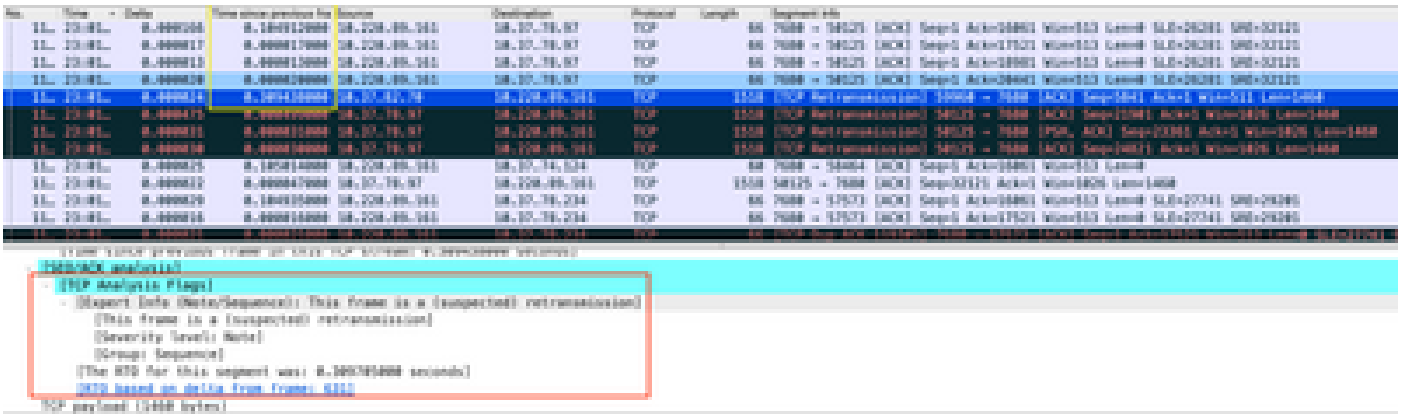
Die TCP-Neuübertragung ist ein Symptom oder kann aufgrund eines zugrunde liegenden Problems (z. B. Paketverlust) die Folge sein. Dieses Problem kann zu Langsamkeit und schlechter Leistung bei der Anwendung führen.

Das Transmission Control Protocol (TCP) verwendet einen Timer für die erneute Übertragung, um

die Datenübermittlung sicherzustellen, wenn der Remote-Datenempfänger keine Rückmeldung sendet. Die Dauer dieses Timers wird als RTO (Retransmission Timeout) bezeichnet. Wenn der Timer für die erneute Übertragung abläuft, sendet der Sender das früheste Segment, das vom TCP-Empfänger nicht bestätigt wurde, erneut, und die RTO wird erhöht.

Einige Neuübertragungen können nicht vollständig eliminiert werden, wenn sie minimal sind, kann es kein Problem widerspiegeln. Wie Sie jedoch daraus schließen können, ist eine höhere Weiterleitung zu beobachten, und die Latenz bei der TCP-Sitzung ist zu erhöhen.

Die in Wireshark analysierte Paketerfassung kann das Problem als nächstes Beispiel bestätigen:



TCP-Gesprächserfassung

Wenn es zu erneuten Übertragungen kommt, verwenden Sie die gleiche Erfassungsmethode für die Eingangs- und Ausgangsrichtung des Routers, um alle gesendeten und empfangenen Pakete zu überprüfen. Natürlich kann dies auf jedem Hop eine enorme Anstrengung darstellen, sodass eine detaillierte Analyse der Erfassung für TCP erforderlich ist, wobei TTLs, Zeiten aus früheren Frames im selben TCP-Stream betrachtet werden müssen, um zu verstehen, aus welcher Richtung (Server oder Client) Sie diese Verzögerung oder fehlende Antwort haben, um Ihre Fehlerbehebung zu leiten.

Überbelegung und Engpässe

Eine Überbelegung tritt auf, wenn die erforderlichen Ressourcen (Bandbreite) größer als die tatsächlich verfügbaren sind. Die Befehle zum Identifizieren, ob bei einem Router dieses Problem auftritt, wurden bereits im vorherigen Abschnitt behandelt.

In einer solchen Situation kann es zu Engpässen kommen, wenn der Datenverkehr aufgrund unzureichender Bandbreite oder Hardwarekapazität verlangsamt wird. Es ist wichtig festzustellen, ob dies in kurzer Zeit geschieht oder ob es eine langfristige Situation ist, um Lösungen anzuwenden.

Es gibt keine spezifischen Empfehlungen für eine Lösung, aber einige der Optionen sind die Verteilung des Datenverkehrs auf eine andere Plattform, die Segmentierung des Netzwerks oder das Upgrade auf robustere Geräte, basierend auf aktuellen Anforderungen und zukünftigen Wachstumsanalysen.

Zugehörige Informationen

- IP SLA ICMP-Echo-Vorgänge
- Speicherfehlerbehebung
- Fehlerbehebung mit der Paketverfolgungsfunktion Cisco IOS-XE Datapath
- Fehlerbehebung bei Paketverlusten auf Service-Routern der Serie ASR 1000
- QoS-bezogene Informationen
- QoS-Konfiguration auf Routern
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

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