企業ネットワークでのルータ問題のトラブルシューティング

内容

概要

このドキュメントでは、Ciscoルータを使用してエンタープライズネットワークの遅延の問題を特定、トラブルシューティング、および解決する方法について説明します。

前提条件

要件

このドキュメントに関する特定の前提条件や要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアバージョンやハードウェアタイプに限定されるものではありませんが、コマンドはASR 1000、ISR 4000、Catalyst 8000ファミリなどのCisco IOS®

XEルータに適用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、一般的な遅延の問題を理解し、切り分け、トラブルシューティングするための基本的なガイドについて説明し、根本原因とベストプラクティスを検出するための便利なコマンドとデバッグを提供します。すべての可能な変数とシナリオを考慮することはできず、詳細な分析は特定の状況によって異なることに注意してください。

遅延の定義

一般的に、ストアアンドフォワードデバイスの厳密な定義(RFC 1242)を引用すると、遅延は、入力フレームの最後のビットが入力ポートに到達した時点から、出力フレームの最初のビットが出力ポートに現れた時点までの時間間隔です。

ネットワーク遅延とは、ネットワーク上でのデータ転送の遅延を指すだけです。実際の問題の場合、この定義は出発点に過ぎません。どの特定のケースについても、ここで説明している遅延の問題を定義する必要があります。問題を解決するために必要な最初のステップは、その問題を定義することであることは明白ですが、非常に重要です。

遅延の使用状況

多くのアプリケーションでは、リアルタイムの通信とビジネス運用に低遅延が必要です。日常的に使用されるハードウェアとソフトウェアの改善により、ミッションクリティカルなコンピューティング、オンライン会議アプリケーション、ストリーミングなどに使用できるアプリケーションが増加します。同様に、ネットワークトラフィックは増加し続け、最適化されたネットワーク設計とデバイスのパフォーマンス向上のニーズも高まっています。

優れたユーザエクスペリエンスを提供し、遅延の影響を受けやすいアプリケーションに必要な最低限の要件を満たすだけでなく、ネットワークの遅延の問題を効果的に特定して削減することで、ネットワーク上で非常に価値の高い時間とリソースを大幅に節約できます。

遅延の問題に近づく

このような問題の難しい部分は、考慮する必要がある変数の数と、シングルポイント障害が発生する可能性がないことです。したがって、遅延の定義は解決の重要な鍵となり、有用な問題の説明を得るために考慮する必要がある側面は次のとおりです。

1.期待と発見

望ましい遅延、予測される動作遅延またはベースラインの動作遅延、および現在の動作遅延を区

別することが重要です。ネットワーク上の設計、プロバイダー、またはデバイスによっては、必要な遅延を達成できないことがあります。通常の条件下で実際の遅延を測定することは適切な手順ですが、紛らわしい数値を回避するには、測定方法に一貫性がある必要があります。IP SLAおよびネットワークアナライザツールがこの点で役立ちます。

アプリケーションまたはIP SLAによって遅延を特定するために最も使用される基本的なツールの1つは、ICMPまたはpingを使用することです。

<#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

到達可能性のチェックに加えて、pingは発信元から宛先までのラウンドトリップ時間(RTT)をミリ秒単位で通知します。最小(2)、平均(109)、および最大(541)です。つまり、ルータが要求を送信してから、デバイスの宛先から応答を受信するまでの時間です。ただし、ホップ数や深い情報は表示されませんが、問題を検出するための簡単で迅速な方法です。

2.隔離

pingと同様に、tracerouteは分離の開始点として使用でき、ホップとホップごとのRTTを検出します。

<#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は、TimeTo Live（TTL；存続可能時間）が1のパケットを送信することで動作します。第1ホップが、TTLが期限切れになりRTTが測定されたためパケットを転送できなかったことを示すICMPエラーメッセージを返信し、次にTTLが2のパケットを再送信し、第2ホップがTTLが期限切れになったことを返します。このプロセスは、宛先に到達するまで続きます。

この例では、2つの特定のホストに絞り込むことができ、そこから切り離して開始できます。

これらのコマンドは問題を簡単に特定できる便利なコマンドですが、プロトコル、パケットマーキング、サイズ（2番目のステップとして設定できますが）、異なるIP送信元、複数の要因の宛先など、他の変数は考慮されません。

レイテンシは非常に広い概念であり、アプリケーション、ブラウジング、コール、または特定のタスクの症状のみを見ることがよくあります。最初に制限する必要があるのは、影響を理解し、問題をより詳細に定義し、次の質問に答えて、この寸法記入に役立つ要素を定義することです。

- 遅延は特定の種類のトラフィックまたはアプリケーションにのみ影響しますか。例：UDP、TCP、ICMPのみ…
- 存在する場合、このトラフィックには一意のIDがありますか。例：特定のQoSマーキング、決定されたパケットサイズのみ、IPオプション…
- 影響を受けるユーザまたはサイトの数はいくつですか。例：1つの特定のサブネット、1つまたは2つのエンドホスト、1つまたは複数のデバイスに接続されたサイト全体…
- 特定のタイムスタンプが確認されているか。例：これは、ピーク時、時間パターン、または完全にランダムな時間帯にのみ発生しますか。
- 設計の側面。例：特定のデバイスを通過するトラフィック（多くのデバイスを通過する可能性があるが、1つのプロバイダーにのみ接続するトラフィック、ロードバランシングを行うトラフィックだが、1つのパスに影響を与えるトラフィック）

その他にも多くの考慮事項がありますが、異なる解答（および解答に対して実行可能なテスト）をクロスすることで、効果的に切り分けてトラブルシューティングを進める範囲を制限できます。たとえば、ピーク時に同じデータセンターを経由して異なるプロバイダーを通過するすべてのブランチで、1つのアプリケーション（同種のトラフィック）のみが影響を受けます。この場合、すべてのブランチのすべてのアクセススイッチのチェックを開始するのではなく、データセンターに関する詳細な情報の収集に重点を置き、その側をさらに調査します。

ネットワーク上でモニタリングツールや自動化を行うことで、この分離に大きく役立ちます。これは、実際に使用するリソースや固有の状況によって異なります。

一般的な原因のトラブルシューティング

トラブルシューティングの範囲を制限したら、特定の原因のチェックを開始できます。たとえば

、提供されているtracerouteの例では、2つの異なるホップに切り分けて、考えられる原因に絞り込むことができます。

プラットフォーム関連

CPU の使用率が高い

一般的な原因の1つは、すべてのパケットを処理する際にCPUの遅延が大きいデバイスが原因である可能性があります。ルータで確認する最も便利で基本的なコマンドは次のとおりです

ルータ全体のパフォーマンス：

<#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
```

メモリとCPUの使用率を一度に確認する場合に便利です。コントロールプレーン(CP)とデータプレーン(QFP)で、それぞれのしきい値と同じ値に分割されます。メモリ自体は遅延の問題を引き起こしませんが、コントロールプレーン用のDRAMメモリがこれ以上ない場合、Cisco Express

Forwarding(CEF)がディセーブルにされ、CPUの高使用率が引き起こされて遅延が発生する可能性があります。そのため、番号を正常な状態に保つことが重要です。メモリのトラブルシューティングに関する基本的なガイドは範囲外ですが、「関連情報」の項にある役立つリンクを参照してください。

Control Processor、QFP CPU、またはCrypto使用率で高CPU使用率が検出された場合は、次のコマンドを使用できます。

コントロールプレーン：

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
```

コントロールプレーンのCPU使用率が高い場合（この例ではプロセスが原因で99 %）、プロセスを分離する必要があり、それに依存して分離に進みます（ARPまたは制御ネットワークパケットなどのパントされたパケットであり、任意のルーティングプロトコル、マルチキャスト、NAT、DNS、暗号化トラフィック、または任意のサービスです）。

トラフィックフローによっては、トラフィックの宛先がルータでない場合は、以降の処理で問題が発生する可能性があります。データプレーンに焦点を当てることができます。

データプレーン：

show platform hardware qfp active datapath utilization [サマリー]

<#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
```

データプレーンの使用率が高い（処理負荷の数が100 %に達することで識別される）場合は、ルータを通過するトラフィックの量（秒あたりの総パケット数と秒あたりのビット数）とプラットフォームのスループットパフォーマンスを確認する必要があります（具体的なデータシートでアイデアを得ることができます）。

このトラフィックが予想されているかどうかを判断するには、パケットキャプチャ(EPC)またはNetflowなどのモニタリング機能を使用してさらに分析します。いくつかのチェックは次のとおりです。

- トラフィックは有効で、このルータを通過することが予想されますか。
- 異常なトラフィックフローまたはより高いレートを特定する。
- 1秒あたりのパケット数が多い場合は、パケットサイズを調べます。これが発生すると予想されるか、またはフラグメンテーションの問題が発生するかを判断します。

すべてのトラフィックが予想される場合は、プラットフォームの制限に達している可能性があり

ます。その場合は、show running-configを使用して分析するため2番目の部分としてルータで実行されている機能を探します（主にインターフェイス）。不要な機能を特定して無効にするか、トラフィックのバランスを取ってCPUサイクルを解放します。

ただし、プラットフォームの制限が示されない場合、ルータがパケットに遅延を追加している場合に裏付けるもう1つの便利なツールはFIAトレースです。各パケットに費やされた正確な処理時間と、処理の大部分を占める機能を確認できます。CPU使用率が高くなる問題の完全なトラブルシューティングについては、このドキュメントの対象外ですが、「関連情報のリンク」の項を参照してください。

トラフィック関連

MTUとフラグメンテーション

最大伝送ユニット(MTU)は、物理リンクが伝送できるオクテットの数に応じて伝送される最大パケット長です。上位層プロトコルが基盤となるIPにデータを送信し、その結果IPパケットの長さがパスMTUを超えると、パケットはフラグメントに分割されます。ネットワークのサイズが小さいほど、処理が多くなり、処理が異なる場合があるため、できるだけ避ける必要があります。

NATやゾーンベースファイアウォールなどの一部の機能では、仮想リアセンブリは「パケット全体を持つ」ために必要であり、必要な内容を適用してフラグメントを転送し、リアセンブルされたコピーを破棄します。このプロセスによってCPUサイクルが増え、エラーが発生しやすくなります。

一部のアプリケーションはフラグメンテーションに依存しません。MTUを確認する最も基本的なテストの1つは、フラグメントなしオプションを使用してpingを実行し、さまざまなパケットサイズ(ping ip-address df-bit size number)をテストすることです。 pingが失敗した場合は、廃棄が発生したときにパス上のMTUを修正し、さらに問題を引き起こします。

断片化されたパケットを含むネットワーク上のポリシーベースルーティング(PBR)や等コストマルチパスなどの機能は、遅延の問題や、主に高いデータレートでの エラーを引き起こし、高いアセンブリ時間、重複したID、破損したパケットを誘発する可能性があります。この問題の一部が特定された場合は、この断片化を可能な限り解決してください。フラグメントが存在するかどうか、および潜在的な問題があるかどうかを確認する1つのコマンドは、show ip trafficです。

<#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>
```

上記の出力から、Fragsセクションの太字の単語は次を参照しています。

- リアセンブル：リアセンブルされたパケットの数。
- Timeouts:パケットフラグメントのリアセンブル時間が満了するたびに送信されます。
- Could not reassembly：再構成できなかったパケットの数。
- フラグメント化：MTUを超え、フラグメント化の対象となるパケットの数。
- フラグメント：パケットがフラグメント化されたチャンクの数。
- Could not fragment:MTUを超えているものの、フラグメント化できなかったパケットの数。

フラグメンテーションが使用されていて、タイムアウトが発生しているか、またはカウンタを再構成できない場合は、プラットフォームによって引き起こされる問題を裏付ける1つの方法として、QFPドロップを使用します。この場合は、後の「ドロップ」セクションで説明するshow platform hardware qfp active statistics dropと同じコマンドを使用します。TcpBadfrag、IpFragErr、FragTailDrop、ReassDrop、ReassFragTooBig、ReassTooManyFrags、ReassTimeout、または関連するエラーを探します。それぞれのケースには、すべてのフラグメントが取得されない、重複する、CPUの輻輳など、さまざまな原因が考えられます。繰り返しますが、さらなる分析と潜在的な修正のための便利なツールは、FIAトレースと設定チェックです。

TCPは、この問題を解決するために最大セグメントサイズ(MSS)メカニズムを提供しますが、誤った、非MSSネゴシエーション、または誤ったパスMTUが検出された場合に遅延を引き起こす可

能性があります。

UDPにはこのフラグメンテーションメカニズムがないため、PMTDの手動実装や任意のアプリケーション層ソリューションに依存できます。また、576バイトよりも短いパケット（該当する場合）を送信するように有効にできます。これは、フラグメンテーションを回避するために、RFC1122に従って、送信番号の有効なMTUよりも小さくなります。

設計関連

このセクションでは、トラブルシューティングの提案に加え、遅延の問題を引き起こす可能性のあるさらに2つの主要なコンポーネントについて簡単に説明します。これらのコンポーネントについては、このドキュメントの範囲外で詳しく説明し、分析する必要があります。

最適でないルーティング

ネットワーク内の最適でないルーティングとは、ネットワーク内で最も効率的または最短のパスを通じてデータパケットが転送されない状況を指します。その代わり、これらのパケットは効率の低いルートを通っているため、遅延や輻輳が増加したり、ネットワークパフォーマンスに影響を与える可能性があります。IGPは常にベストパスを選択します。これは低コストを意味しますが、必ずしも最も安価なパスや最も低い遅延パスとは限りません（より高い帯域幅を持つパスが最適なパスになる場合もあります）。

設定または競合状態、動的な変更（トポロジの変更またはリンクの障害）、会社のポリシーまたはコストに基づく意図したトラフィックエンジニアリング、冗長性またはフェールオーバー（特定の条件下でバックアップパスに向かう）などの状況など、ルーティングプロトコルの問題に対して最適でないルーティングが発生する可能性があります。

tracerouteやモニタリングアプライアンスなどのツールは、この状況が該当する場合、特定のフローについてこの状況を識別するのに役立ちます。また、他の多くの要因によってアプリケーションの要求が満たされ、遅延が短い場合は、ルーティングの再設計またはトラフィックエンジニアリングが必要になることがあります。

Quality of Service（QoS）

Quality of Service(QoS)を設定すると、他のトラフィックタイプを犠牲にして、特定のトラフィックタイプを優先的に処理できます。QoSを使用しない場合、 デバイス パケットの内容やサイズに関係なく、パケットごとにベストエフォート型のサービスを提供します。「 デバイス 信頼性、遅延範囲、またはスループットを保証せずにパケットを送信します。

QoSが設定されている場合、ルータがパケットをマーク、再マーク、または単に分類するかどうかを特定し、設定を確認してshow policy-map [name_of_policy_map | session | interface interface_id]は、高レート、廃棄、または誤って分類されたパケットの影響を受けるクラスを理解するのに役立ちます。

QoSの実装は、深刻な分析を必要とするヘビーデューティなタスクであり、このドキュメントの適用範囲外です。ただし、時間に影響を受けやすいアプリケーションに優先順位を付け、多くの遅延やアプリケーションの問題を解決または防止するために、このタスクを検討することを強く

お勧めします。

その他のパフォーマンスの問題

その他の状況では、速度低下、セッションの再接続、または全体的なパフォーマンスの低下が発生する可能性があり、確認が必要です。その状況には次のようなものがあります。

ドロップ

デバイスでの処理に直接関連する問題はパケットドロップです。インターフェイスの観点から入力側と出力側を確認する必要があります。

<#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#
```

入力側には次の要素があります。

- 入力キュードロップ：各インターフェイスは、ルーティングプロセッサ(RP)による処理を待機するために着信パケットが配置される入力キュー（変更可能なソフトウェアバッファ）を所有します。 入力キューに配置された着信パケットのレートが、RPがパケットを処理できるレートを超えると、ドロップが増加する可能性があります。ただし、制御パケットと「For us」トラフィックだけが配置されるので、トラフィックの通過に遅延が発生した場合は、散発的にドロップが発生しても、これが原因ではないことに注意してください。

- オーバーラン：これは、入力レートがレシーバのデータ処理能力を超えているために、レシーバのハードウェアが受信パケットをハードウェアバッファに渡すことができない場合に発生します。この数は、ルータのレートとパフォーマンスに問題があることを示している可能性があります。このインターフェイスのトラフィックだけをキャプチャして、トラフィックの急上昇を探します。一般的な回避策は、フロー制御を有効にすることです。ただし、遅延パケットが増える可能性があります。これは、ボトルネックとオーバーサブスクリプションの証拠にもなります。
- CRC：物理的な問題が原因で発生し、ケーブル配線、ポート、およびSFPが正しく接続され、正しく機能していることを確認します。

出力側には次のものがあります。

- 出力キュードロップ：各インターフェイスは、インターフェイス上で送信される発信パケットが配置される出力キューを所有します。RPによって出力キューに配置された発信パケットのレートが、インターフェイスがパケットを送信できるレートを超える場合があります。QoSが適用されていない場合、パフォーマンスの問題や遅延の問題が発生する可能性があります。それ以外の場合は、特定のポリシーが適用されているために、この数値が増加する可能性があります。また、目的のトラフィックまたは重要なトラフィックを保護および保証するために、Qo設定を確認することを提案します。

最後に、QFPでのドロップは、遅延を引き起こす可能性がある高い処理に直接関係しています。show platform hardware qfp active statistics dropで確認してください。

<#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
```

原因はコードによって異なります。FIAトレースは、遅延の影響を受けるトラフィックがこの時点でドロップされた場合に、裏付けまたは廃棄するのに役立ちます。

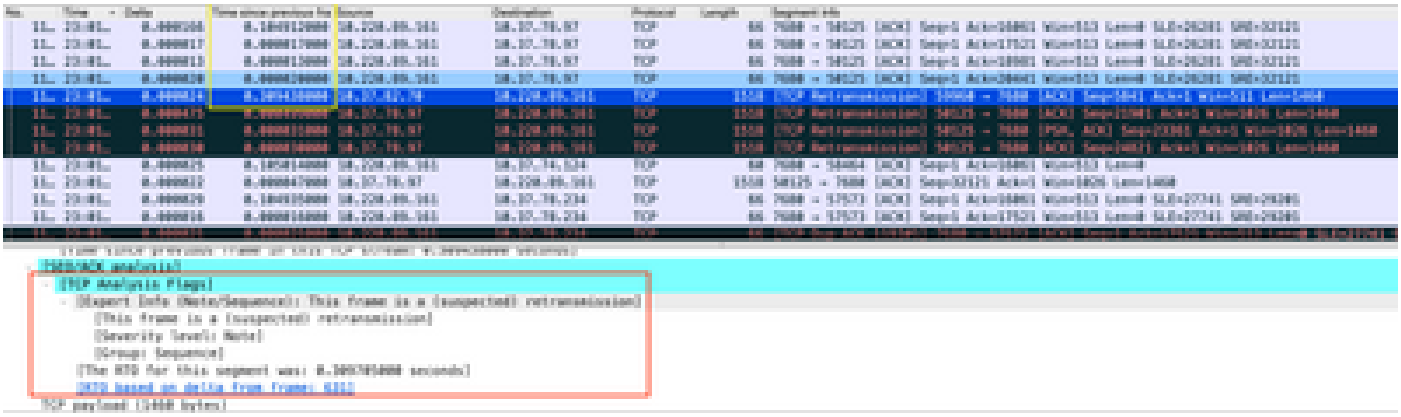
TCP再送信

TCPの再送信は、症状の1つであるか、パケット損失などのアンダーレイの問題による結果である可能性があります。この問題は、アプリケーションの速度低下やパフォーマンスの低下を引き起こす可能性があります。

Transmission Control Protocol（TCP；伝送制御プロトコル）は、再送信タイマーを使用して、リモートデータ受信者からのフィードバックがない状態でのデータ配信を保証します。このタイマーの持続時間は、RTO（再送信タイムアウト）と呼ばれます。再送信タイマーが期限切れになると、送信側はTCP受信側によって確認応答されていない最も古いセグメントを再送信し、RTOが増加します。

一部の再送信は完全に排除することはできません。最小限の場合は、問題を反映することはできません。ただし、推測できるように、再送信が増え、TCPセッションの遅延が増えるため、対処する必要があります。

Wiresharkで分析されたパケットキャプチャは、次の例のように問題を裏付けることができます。



TCPカンバセーションキャプチャ

再送信がある場合は、ルータの入力方向と出力方向で同じキャプチャ方式を使用して、送受信されたすべてのパケットを確認します。もちろん、すべてのホップでこれを行うことは非常に大きな労力を伴う可能性があるため、TCPのキャプチャに関する詳細な分析が必要になります。つまり、同じTCPストリーム上の以前のフレームからのTTLと時間を調べて、トラブルシューティングを指示する際に遅延または応答の欠如が発生している方向（サーバまたはクライアント）を理解する必要があります。

オーバーサブスクリプションとボトルネック

オーバーサブスクリプションは、必要なリソース（帯域幅）が実際に使用可能なリソースよりも大きい場合に発生します。ルータでこの問題が発生しているかどうかを確認するコマンドについては、前のセクションですでに説明しています。

この状況の結果、帯域幅またはハードウェア容量が不十分であるためにトラフィックフローが遅

くなると、ボトルネックが発生する可能性があります。ソリューションを適用する際には、これが短期間で発生するのか、長期的な状況で発生するのかを特定することが重要です。

この問題を解決するための具体的なアドバイスはありませんが、一部のオプションは、異なるプラットフォームへのトラフィックのバランス調整、ネットワークのセグメント化、または現在のニーズと将来の拡張分析に基づくより堅牢なデバイスへのアップグレードです。

関連情報

- IP SLAのICMPエコー動作
- メモリのトラブルシューティング
- Cisco IOS XEデータパスパケットトレース機能を使用したトラブルシューティング
- ASR 1000シリーズサービスルータでのパケットドロップのトラブルシューティング
- Qos関連情報
- ルータでのQoSの設定
- シスコテクニカルサポートおよびダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。