Catalyst 9000スイッチのネットワーク遅延とパケットドロップのトラブルシューティング

はじめに

このドキュメントでは、Cisco Catalyst 9000シリーズスイッチでのネットワーク遅延とパケット損失の問題のトラブルシューティングに関する詳細な方法論について説明します。

前提条件

要 件

TCP/IP、VLAN、スパニングツリープロトコル(STP)などのネットワーキングの概念に関する基本的な知識があることが推奨されます。 Cisco Catalyst 9000シリーズスイッチとCisco IOS® XE CLIに関する知識は不可欠です。ネットワーク監視ツールに精通していること、および設定と診断のためのアクセス権限も必要です。

使用するコンポーネント

このドキュメントの情報は、すべてのバージョンのCisco Catalyst 9000スイッチに基づくものです。このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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たものです。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。

バックグラウンド情報

このドキュメントは、ネットワーク管理者とエンジニアを対象としており、企業ネットワーク環境内でこれらの問題を効率的に特定、分離、および解決するためのガイダンスを提供します。ネットワークの遅延とパケットのドロップは、エンタープライズ環境のパフォーマンスと信頼性に悪影響を及ぼす可能性があります。これらの問題は、多くの場合、ネットワークの輻輳、設定ミ

ス、または環境要因によって発生します。Cisco Catalyst 9000シリーズスイッチは、高いパフォーマンスと復元力を実現するように設計されています。このドキュメントでは、ネットワークプロフェッショナルがこれらのスイッチを使用して遅延とパケットドロップの問題を特定および解決する際に役立つ、焦点を絞ったトラブルシューティングの手順について説明します。

ネットワーク遅延とパケットドロップについて

ネットワーク遅延

ネットワーク遅延は、データが送信元から宛先までネットワークを通過する際に発生する遅延の測定値です。遅延は、ラウンドトリップ時間(RTT)として表現されることが最も多く、パケットが送信元から宛先に往復するのに要する時間です。

遅延は通常、ミリ秒(ms)単位で測定されます。

影響：遅延が大きいと、特にTCPなどのプロトコルでは、データを効率的に送信するためにタイムリーな確認応答に依存するため、アプリケーションパフォーマンスが低下する可能性があります。

パケットドロップ

パケットドロップは、ネットワークデバイスが目的の宛先にパケットを転送できないときに発生します。これは、輻輳、バッファオーバーフロー、設定ミス、またはハードウェアの障害が原因で発生することが多くあります。パケットドロップは通常、特定の間隔で失われたパケットの割合として測定されます。

影響：パケットドロップはスループットを低下させ、再送信を引き起こし、アプリケーションの信頼性を中断させる可能性があります。

予想される遅延ベンチマーク

ネットワーク タイプ	一般的なRTT
同じVLAN（アクセスレイヤ）	1ミリ秒未満
キャンパスコアトラバーサル	1 ～ 5ミリ秒

メトロWAN	5 ~ 30ミリ秒
インターネット/WAN	30 ~ 150ミリ秒

注:ネットワークホップ間の地理的な距離により、RTTが増加し、遅延の増大の一因となる可能性があります。

ネットワーク遅延の測定

最初に、ネットワークとそのトポロジを十分に理解します。ネットワークが決定論的な変数を使用し、予測不可能性を最小限に抑えて設計されている場合は、遅延とパケット廃棄の問題を特定して解決するプロセスが非常に簡単になります。

通常、ネットワーク遅延の測定には2つの主要なツールが使用されます。

ping

パケット損失とRTTに関する統計情報とともに、宛先が到達可能かどうかを出力として返します。問題のあるホップを特定したら、それらの間で直接pingを実行し、問題を見つけるためにデバイスをチェックインできます。

<#root>

Switch#ping 8.8.8.8

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!.!!.
```

Success rate is 60 percent (3/5),

round-trip min/avg/max = 12/

15

/22 ms

<===== 2 dropped out of 5 packets, Average RTT 15 ms

トレースルート

tracerouteは、送信元から宛先までのルーティングパスにあるすべてのホップと、各ホップのRTT結果を表示します。たとえば、tracerouteを使用すると、ネットワーク内のどこで（ルーティングパス内のどのホップで）遅延が発生しているか、または発生し始めたかを表示できます。このような例を次のtraceroute出力に示します。

<#root>

Switch#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

1 2 ms 2 ms 2 ms [10.10.10.10]
2 2 ms 1 ms 1 ms [20.20.20.20]

3 7 ms 45 ms 40 ms [30.30.30.30]

<===== High latency at this hop

4 7 ms 3 ms 1 ms [40.40.40.40]

Note: The IP addresses shown for each hop are provided for demonstration purposes only.

この出力は、ホップ2とホップ3の間のRTTが大幅に増加していることからわかるように、ホップ3での遅延の可能性を示しています。ホップ3とホップ4の時間差が比較的小さいことは、問題が20.20.20.20と30.30.30.30の間のセグメントに限定されていることを示しています。

遅延およびパケットドロップの一般的な原因

第1層（物理層）の問題

第1層の問題は、ネットワーク遅延とパケットドロップの一般的な原因です。物理層で次の側面を確認することが重要です。

- デュプレックスと速度の設定がすべてのインターフェイスで正しく設定されていることを確認します。
- インターフェイスでCRCおよび入力エラーをチェックします。これらは物理層の問題を示している可能性があります。
- ネットワークケーブル、ファイバ接続、SFPモジュール、またはスイッチポートの障害によっても、パケットの遅延やドロップが発生する可能性があります。

<#root>

Switch#show interface gi1/0/1

GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,

Full-duplex, 1000Mb/s,

 media type is 10/100/1000BaseTX
  ...
  5 minute input rate 2000 bits/sec, 5 packets/sec
  5 minute output rate 3000 bits/sec, 8 packets/sec
     250000 packets input, 22000000 bytes, 0 no buffer
     Received 300 broadcasts (200 multicasts)
     0 runts, 0 giants, 0 throttles

85 input errors, 85 CRC,

 0 frame, 0 overrun, 0 ignored

<===== Input errors and CRC

     0 watchdog, 0 multicast, 0 pause input
  ...
     260000 packets output, 23000000 bytes, 0 underruns
     5 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output

Switch# show interfaces counters errors

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize	OutDiscards
Gi1/0/1	**0**	**0**	**0**	**0**	**0**	**0**

```
Gi1/0/2     0           0           0         0         0           0
...
```

出力ドロップ

出力ドロップは、スイッチインターフェイスの送信キューがいっぱいになり、追加のパケットを転送できない場合に発生します。これは、パケットがキューで待機する際の遅延の増加につながり、キューがオーバーフローするとパケットのドロップが発生して、アプリケーションのパフォーマンスとネットワークの信頼性に影響を与える可能性があります。

<#root>

```
Switch#show interface gi1/0/1


GigabitEthernet1/0/1 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 70b3.171d.c101
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
...
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 2d00h
  Input queue: 0/2000/0/0 (size/max/drops/flushes)

; Total output drops: 4216760900


  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 389946000 bits/sec, 84175 packets/sec
  5 minute output rate 694899000 bits/sec, 106507 packets/sec
     7885666654 packets input, 4677291827948 bytes, 0 no buffer
...
```

Total output dropsカウンタは、多数のドロップされたパケットを示しており、このインターフェイスでの輻輳またはキューオーバーフローを示しています。これにより、遅延とパケット損失が増加し、ネットワークとアプリケーションのパフォーマンスに影響が及ぶ可能性があります。

STPの安定性

STPの不安定性は、ネットワーク遅延やパケットドロップの原因となる可能性があります。安定したネットワークでは、トポロジの変更を最小限に抑える必要があります。頻繁なトポロジ変更

は、根本的な問題を示している可能性があり、通常の転送動作を中断させる可能性があります。

STP関連の遅延を最小限に抑えるための主な考慮事項：

トポロジ変更(TCN):STPトポロジの変更が多すぎると、スイッチ(CAM)テーブルのMACアドレスが頻繁にフラッシュされ、テーブルが再生成されるまでスイッチによって不明なユニキャストパケットがフラッディングされるため、ブロードキャストトラフィックと遅延が増加する可能性があります。

エッジポートの設定：すべてのエッジポートにPortFastが設定されていることを確認します。PortFastを有効にすると、クライアントまたはサーバの接続または切断時にSTPトポロジ変更通知(TCN)が生成されなくなります。これにより、不要なCAMテーブルのエージングが削減され、安定性が向上します。

ルートブリッジの計画：STPルートブリッジとプライオリティを手動で計画および割り当てて、予測可能なネットワークトポロジを維持し、不必要なトポロジ変更を最小限にします。

トポロジの変更が発生すると（ポートの状態が遷移するなど）、スイッチはルートブリッジに向けてTCN　BPDUを送信します。ルートブリッジはすべてのスイッチにTCN　BPDUを伝搬し、MACアドレスのエージングタイムをデフォルト（300秒）から転送遅延値（通常は15秒）に短縮するよう促します。 これにより、最近のアイドルエントリがフラッシュされ、より多くの未知のユニキャストが発生し、ネットワーク全体でのフラッディングが増加します。

<#root>

Switch#show spanning-tree detail | include ieee|from|occur|is exec

VLAN0705 is executing the ieee compatible Spanning Tree protocol

Number of topology changes 6233

last change occurred 00:00:03 ago

<===== Topology Changes

from GigabitEthernet1/0/25 <===== From Gi1/0/25

MACフラッピング/レイヤ2ループ

MACフラッピング/レイヤ2ループは、異なるポート上の同じ送信元MACを使用してMACアドレステーブルを継続的に更新することにより、ネットワーク遅延とパケットドロップを引き起こします。この絶え間ない変更によってトラフィック転送が中断され、中断やパケット損失が発生します。レイヤ2ループは、ブロードキャストパケットをエンドレスに循環させ、より多くのMACフラッピングを引き起こし、ネットワークパフォーマンスをさらに低下させることで、問題を悪化させます。STPなどのループ防止プロトコルの実装は、ネットワークの安定した動作を維持し、これらの問題を回避するために不可欠です。

MAC移動通知を設定するには、グローバルコンフィギュレーションモードで、コマンドmac address-table notification mac-moveを使用します。

<#root>

Mac Flapping logs:

```
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po2 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host 8c45.0021.0b17 in vlan 152 is flapping between port Po1 and port Po
%MAC_MOVE-SW1-4-NOTIF: Host b0f1.ec27.69ea in vlan 154 is flapping between port Po9 and port Po
```

フロー制御

フロー制御が有効で、スイッチポートの受信バッファが容量に近づくと、スイッチは一時停止フレームを送信して着信トラフィックを一時的に停止します。このプロセスでは、データ伝送が断続的に一時停止されるため、遅延が増加する可能性があります。逆に、フロー制御が有効でない場合、またはアップストリームデバイスがポーズフレームを許可しない場合、着信トラフィックがバッファ容量を超え、その結果バッファオーバーランとパケット廃棄が発生する可能性があります。

フロー制御は、トラフィックパス内のすべてのデバイスの機能を考慮しながら、慎重に設定する必要があります。不適切な使用や設定ミスは、遅延の増加やパケットのドロップにつながり、アプリケーションのパフォーマンスに悪影響を及ぼす可能性があります。

<#root>

Switch#show interfaces gigabitEthernet 1/0/1

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
□
```

input flow-control is on,

output flow-control is unsupported

<===== Input Flow Control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 6530
5 minute input rate 8000 bits/sec, 8 packets/sec□
5 minute output rate 0 bits/sec, 0 packets/s
0 watchdog, 5014620 multicast,

1989 pause input

<===== Pause Input

0 unknown protocol drops□0 babbles, 0 late collision,
0 deferred□0 lost carrier, 0 no carrier, 0 pause output

Switch#show controllers ethernet-controller gigabitEthernet 1/0/1

Transmit GigabitEthernet1/0/1 Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

1878 Pause frames <===== Pause frames in RX

CPU Utilization

CPU使用率が高いと、ネットワーク遅延の増加やパケットのドロップが発生する可能性があります。CPUの負荷が高いと、スイッチはコントロールプレーントラフィック、ルーティングアップデート、または管理機能を効率的に処理できません。これにより、パケット転送が遅延し、ARPやスパニングツリーなどのプロトコルでタイムアウトが発生し、特にCPUの介入を必要とするトラフィックでパケットがドロップされる可能性があります。

<#root>

Switch#show processes cpu sorted

CPU utilization for five seconds:

95%/8%;

one minute: 92%; five minutes: 90%

<===== CPU utilization 93%

PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process

```
 439     3560284      554004       6426 54.81% 55.37% 48.39%   0 SISF Main Thread


 438     2325444      675817       3440 22.67% 28.17% 27.15%   0


SISF Switcher Th

 104      548861       84846       6468 10.76%  8.17%  7.51%   0 Crimson flush tr
 119      104155      671081        155  1.21%  1.27%  1.26%   0 IOSXE-RP Punt Se
```

メモリ使用率

メモリの使用量が高いと、CPUおよびコントロールプレーンプロセスに過負荷が発生し、遅延やパケットのドロップが発生する可能性があります。この過負荷により、ルーティングアップデート、QoSポリシー、およびバッファ管理の処理が遅延し、パケット処理パイプラインで輻輳が発生します。その結果、パケットが廃棄されたり、遅延が発生したりする可能性があります。したがって、メモリ使用率が高いと、トラフィックの管理におけるスイッチの効率が低下し、ネットワークパフォーマンスに影響します。

<#root>

```
Switch#show platform resources


Resource                  Usage                    Max             Warning         Critical
-------------------------------------------------------------------------------------------
Control Processor       25.00%                     100%            90%             95%
  DRAM


3656MB(94%)


           866MB          90%             95%             W


High memory logs:


%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
%PLATFORM-4-ELEMENT_WARNING:Switch 2 R0/0: smand:  1/RP/0: Used Memory value 94% exceeds warning
```

ICMPリダイレクトおよび到達不能メッセージ

パケットがレイヤ3インターフェイスに到着し、同じインターフェイスからルーティングされると、スイッチでは、同じサブネット上のより効率的なネクストホップを送信元に通知するために、ICMPリダイレクトメッセージが生成されます。これにより、元のパケットはvLANを2回通過することになり、帯域幅の使用量が増加します。また、ICMPリダイレクトパケット自体が帯域幅を消費するため、CPU処理が必要になり、これがCPU割り込みと遅延の増加につながる可能性があります。このようなリダイレクトが多数発生すると（特に大量のトラフィックが流れている間）、CPUの負荷が著しく上昇し、パケットがドロップされる可能性があります。

ICMP到達不能メッセージを頻繁に生成して処理すると、CPU使用率が増加し、ネットワークパフォーマンスに影響を与えることがあります。大量のICMP到達不能トラフィックによってCPUリソースが消費され、遅延やパケットのドロップが発生する可能性があります。

これらの影響を緩和するには、no ip unreachablesコマンドとno ip redirectsコマンドを使用して、ICMP到達不能メッセージとICMPリダイレクトをスイッチ仮想インターフェイス(SVI)とレイヤ3インターフェイスで無効にすることを推奨します。このベストプラクティスにより、CPUの負荷が軽減され、ネットワークの安定性が向上します。

<#root>

Switch#show ip traffic | in unreachable

```
...
  Rcvd: 194943 format errors, 369707 checksum errors,
```

3130 redirects,

734412 unreachable

```
  Sent: 29265 redirects, 14015958 unreachable, 196823 echo, 786959149 echo reply
...
```

Switch#show platform hardware fed active qos queue stats internal cpu policer

```
           CPU Queue Statistics
============================================================================================
                                              (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                Enabled   Rate     Rate      Drop(Bytes)  Drop(Frames)
--------------------------------------------------------------------------------------------
0    11     DOT1X Auth                  Yes     1000      1000     0            0
```

```
1    1      L2 Control                Yes     2000      2000      0             0
2    14     Forus traffic             Yes     4000      4000      3296567       2336
3    0      ICMP GEN                  Yes     750       750       0             0
4    2      Routing Control           Yes     5500      5500      1085196       12919
5    14     Forus Address resolution  Yes     4000      4000      51723336      760639


6    0      ICMP Redirect             Yes     750       750       8444220485535  6978564145


...
```

トラフィックストーム

トラフィックストームは、過剰なブロードキャスト、マルチキャスト、またはユニキャストパケットがLANをフラッディングし、スイッチのリソースが不足して、ネットワークパフォーマンスが低下した場合に発生します。

スイッチのストーム制御は、物理インターフェイス上のブロードキャスト、マルチキャスト、およびユニキャストトラフィックを監視し、設定されたしきい値と比較します。トラフィックがこれらの制限を超えると、スイッチはネットワークの劣化を防ぐために、過剰なトラフィックを一時的にブロックします。これにより、スイッチリソースが保護され、ネットワーク全体の安定性とパフォーマンスが維持されます。

<#root>

Switch#show interfaces counters

```
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts

Gi1/0/1        125487955     550123004     250123555      105234788


Gi1/0/2          500123        100123          5123           1024
Gi1/0/3          250123         50123          1024            512


Switch#show platform hardware fed switch active qos queue stats internal cpu policer
```

```
                        CPU Queue Statistics
============================================================================================
                                                 (default) (set)     Queue         Queue
QId PlcIdx  Queue Name                Enabled    Rate      Rate      Drop(Bytes)   Drop(Frames)
--------------------------------------------------------------------------------------------
11   13     L2 LVX Data Pack           Yes       1000      1000      0             0

12   0      BROADCAST                  Yes       750       750       32529067      186363

13   10     Openflow                   Yes       250       250       0             0

14   13     Sw forwarding              Yes       1000      1000      48317658492   245507344

15   8      Topology Control           Yes       13000     16000     0             0
```

CAMとARPのエージングタイム

CAM（MACアドレステーブル）のエージングタイムとAddress Resolution Protocol(ARP)のエージングタイムも、ネットワーク遅延とパケットドロップの原因となる可能性があります。これは、MACアドレスからポートへのマッピングを格納するCAMテーブルでは、通常、IPアドレスからMACアドレスへのマッピングを格納するARPテーブル（デフォルトは4時間）よりもエントリのエージングアウトが高速であるためです（デフォルトは5分程度）。 MACアドレスがCAMテーブルからエージングアウトしてもARPテーブルにまだ存在している場合、スイッチはそのMACアドレスのユニキャストトラフィックを転送する特定のポートを認識しなくなります。その結果、スイッチはユニキャストトラフィックをVLAN内のすべてのポートにフラッディングし、ネットワークの輻輳とパケット損失を引き起こします。

CAMとARPのエージングタイムの比較による遅延とパケットドロップの原因

- CAMテーブルエントリがARPエントリよりも古くなると、スイッチはMACとポートのマッピングがないため、ユニキャストパケットをフラッディングします。
- このフラッディングによってCPUの負荷が増加し、帯域幅が不必要に消費されるため、ネットワークの遅延やパケットのドロップが発生します。
- このミスマッチは、非効率な転送やコントロールプレーン処理の増加の原因となる可能性もあります。

<#root>

Switch#show mac address-table aging-time

Global Aging Time:

300 <===== MAC aging

Vlan Aging Time
---- ----------

Switch#show ip arp

Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.95.1

124

Incomplete ARPA

<===== Arp age

...

Switch#show interface vlan1

Vlan1 is up, line protocol is up , Autostate Enabled
Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
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 not supported
ARP type: ARPA,

ARP Timeout 04:00:00

Last input never, output never, output hang never

Configuring MAC Aging and ARP Timeout:

Switch#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#mac-address-table aging-time ?

```
  <0-0>         Enter 0 to disable aging
  <10-1000000>  Aging time in seconds
```

Switch(config)#mac-address-table aging-time 14400 ?

```
  routed-mac  Set RM Aging interval
  vlan        VLAN Keyword
```

Switch(config)#interface vlan 1

```
Switch(config-if)#arp timeout 300

Switch(config-if)#do show interface vlan 1

Vlan1 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is 10b3.d6f0.1347 (bia 10b3.d6f0.1347)
  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 not supported
  ARP type: ARPA,
```

ARP Timeout 00:05:00

```
  Last input never, output never, output hang never
```

monitor session

複数の送信元ポートと宛先ポートを持つスイッチでアクティブモニタ(SPAN)セッションを設定すると、ネットワーク遅延とパケットドロップの原因になる可能性があります。

<#root>

Example:

Session 1

Type : Local Session

Source Ports :

Both : Po101,Po105,Po109,Po125,Po161,Po170 <===== Multiple source ports

Destination Ports : Te9/8

Egress SPAN Replication State:
Operational mode : Centralized
Configured mode : Centralized (default)

Session 2

Type : Local Session

Source Ports :

Both : Po161,Po170

Destination Ports : Te9/1

Egress SPAN Replication State:
Operational mode : Centralized

```
Configured mode         : Centralized (default)
```

SPANの動作の仕組み

SPAN (Switched Port Analyzer ; スイッチドポートアナライザ) は、CPUルックアップを行わずに送信元ポートから宛先ポートへのトラフィックをミラーリングするハードウェアアシストの機能です。スーパーバイザモジュール上の複製ASICがパケットのミラーリングを処理し、転送エンジンがミラーリングされたパケットを宛先ポートにリダイレクトします。ミラーリングされたパケットは、通常のトラフィックと同じタイミングでスイッチングされます。

複数の送信元ポートと宛先ポートの影響：

前述の例では、スイッチはすべての送信元インターフェイスから宛先インターフェイスにトラフィックを複製する必要があります。たとえば、インターフェイスPo170のトラフィックはミラーリングされ、2つの異なる宛先に2回転送されます。この複製によってフォワーディングエンジンの負荷が増大し、スイッチバックプレーンで輻輳が発生する可能性があります。

- ポートチャネルで3 GBPSのトラフィックを伝送する場合、このトラフィックを複数の宛先に複製すると、ミラーリングされたトラフィックが15 GBPSを超える可能性があります。
- 複製ASICの負荷は、発信元インターフェイスのトラフィックレートに比例して増加します。
- トラフィックレートが低い場合、遅延の影響は最小限ですが、トラフィックが増加するにつれて、遅延と輻輳が大きくなる可能性があります。

ASICレベルの例外

インターフェイスからASICへのマッピングを確認するには、次のコマンドを使用します。マッピングは、インターフェイスが存在するASICインスタンスを示します。

<#root>

```
Switch#show platform software fed switch active ifm mappings

Interface                IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type Active

GigabitEthernet2/0/12    0x13

 1     0    1

     11     0      20    17   12   108  NIF   Y
```

```
<===== ASIC Instance 1 (Asic 0/Core 1)
```

ASICインスタンスが特定されたら、次のコマンドを実行して、そのASICの転送ASICドロップ例外を表示します。

<#root>

```
Switch#show platform hardware fed switch active fwd-asic drops exceptions asic
```

```
Example output snippet for ASIC instance 1:

****EXCEPTION STATS ASIC INSTANCE 1 (asic/core 0/1)****
=================================================================================
 Asic/core |                NAME                    |   prev       |  current  |  delta

=================================================================================
0       1  NO_EXCEPTION                             2027072618   2028843223    1770605
0       1  ROUTED_AND_IP_OPTIONS_EXCEPTION          735          735           0
0       1  PKT_DROP_COUNT                           14556203    14556203       0
0       1  BLOCK_FORWARD                           14556171    14556171       0
0       1  IGR_EXCEPTION_L5_ERROR                   1            1             0
...
```

ソフトウェア バグ

ソフトウェアのバグによって、意図しない動作や予期しない動作が直接的または間接的に引き起こされる場合があります。これらのバグにより、ネットワーク遅延、パケットドロップ、その他のパフォーマンス低下などの問題が発生する可能性があります。これらの問題に対処するには、一般的な最初のステップとしてスイッチのリロードを行います。これにより、一時的な障害がクリアされ、通常の動作に戻ることができます。さらに、最新のファームウェアとソフトウェアのアップデートを定期的に適用して、デバイスを最新の状態に保つことが重要です。これらのアップデートには、既知のバグに対する修正や、デバイスの安定性とパフォーマンスを向上させる改良が含まれていることが多く、ソフトウェアの不具合に関連する問題の防止に役立ちます。

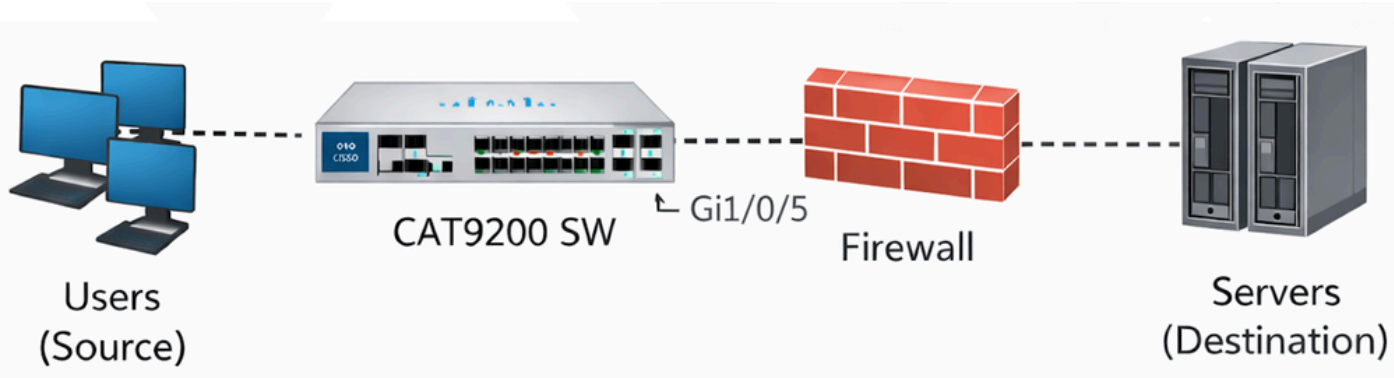
Cisco Bug Searchツール

ケース スタディ

問題の詳細

大容量ファイルの転送中など、vLAN経由で大量のデータを転送しようとすると、ネットワーク接続が断続的に失われる。これらの中断は、複数回の試行が成功したにもかかわらず、データ伝送の散発的な障害として現れ、ネットワークの信頼性とアプリケーションのパフォーマンスに大きな影響を与えます。この問題は、スイッチをリロードすることで一時的に解決されます。

トポロジ



観測された症状

- ソースと宛先の間のファイル転送は、数回成功した後に失敗することがあります。
- 障害発生時にスイッチからファイアウォールへの接続が失われる。
- 802.1X認証は、インシデント全体を通じて引き続き動作します。
- スイッチは、インシデントの間、コンソールを介して応答し続けます。
- ファイアウォールの接続ポートでは、障害発生中はブロードキャストトラフィックのみが示されます。
- 診断テスト(DiagGoldPktTest)がインターフェイスGi1/0/5で継続的に失敗し、データパスの問題があることを示しています。

実施したトラブルシューティング

- インターフェイスカウンタとプラットフォームレベルのバッファ統計情報が確認されます。
- スイッチインターフェイスGi1/0/5は、ファイアウォールから受信した非常に大量の802.3xポーズフレームを示しています。
- 出力ドロップとポーズフレームの統計情報は詳細に監視されます。
- プラットフォームソフトウェアのフォワーディングエンジンキューの統計情報は、バッファの動作を特定するために検査されます。
- スイッチインターフェイスのフロー制御設定がチェックされます。

関連するインターフェイス統計情報

<#root>

Switch#show interfaces GigabitEthernet 1/0/5

GigabitEthernet1/0/5 is up, line protocol is up (connected)
□

input flow-control is on,

output flow-control is unsupported

<===== Input Flow-control is ON

Input queue: 0/2000/0/0 (size/max/drops/flushes);

Total output drops: 78444

5 minute input rate 8000 bits/sec, 8 packets/sec□

5 minute output rate 0 bits/sec, 0 packets/s **<===== Output rate**

0 watchdog, 5014620 multicast,

1989 pause input

0 unknown protocol drops□0 babbles, 0 late collision,
...

Switch#show controllers ethernet-controller GigabitEthernet 1/0/5

Transmit GigabitEthernet1/0/5. Receive
0 MacUnderrun frames 0 MacOverrun frames
0 Pause frames

1878 Pause frames

<===== Pause Frames In RX

...

Switch#diagnostic start switch 1 test DiagGoldPktTest port 5

Switch#show diagnostic result switch 1 test DiagGoldPktTest detail

□Test results: (. = Pass, F = Fail, U = Untested)
_____
1) DiagGoldPktTest:
 Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24□
      U U U U

F

 U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U.

<===== DiagGoldPktTest Failed For Port 5

Port 25 26 27 28□----------------□U U U U

Switch#show flowcontrol interface GigabitEthernet 1/0/

Port Send FlowControl   Receive FlowControl RxPause TxPause
        admin   oper   admin Oper
------------ -------- -------- -------- -------- ------- -------
Gi1/0/5 Unsupp. Unsupp.   on   on.

13256

          0

<===== Pause Frames In RX

Switch#show platform hardware fed switch active qos queue stats interface GigabitEthernet 1/0/5

Asic:0 Core:0 DATA Port:8 Hardware Drop Counters□

Q   Drop-TH0   Drop-TH1   Drop-TH2   SBufDrop   QebDrop
□   (Bytes)   (Bytes)   (Bytes)   (Bytes)   (Bytes)□
----
0   0   0

18106020

0 0

根本原因の特定

根本的な原因は、ファイアウォールからスイッチインターフェイスに過剰な802.3xポーズフレームが送信されたことによるバッファロックアップであると特定されました。イーサネットのポーズフレームは、受信側デバイスが輻輳から回復できるようにするため、スイッチに送信を停止するように指示します。ただし、一時停止フレームが繰り返し送信される場合、または長い期間にわたって送信される場合：

- インターフェイスのスイッチバッファの出力キューが完全に飽和した状態になります。
- スイッチは、一時停止したインターフェイス宛ての着信パケットを引き続き受け入れます。このパケットは出力キューに蓄積されます。
- キューの飽和により、出力ドロップとトラフィックのブラックホールが発生します。
- この場合、バッファはロックされ、ポーズフレームレートが低下した後も転送は再開しませんでした。
- ロックされたバッファ状態をクリアするには、スイッチのリロードが必要でした。

この動作はCisco Bug CSCwm14612に記載されており、圧倒的なポーズフレームによってインターフェイスでバッファが正しく保持されず、出力廃棄が発生する仕組みが説明されています。

解決策

次のコマンドを使用して、影響を受けるスイッチインターフェイスで入力フロー制御を無効にしました。

<#root>

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 1/0/5
Switch(config-if)#
```

flowcontrol receive off

結論

Cisco C9200Lスイッチとファイアウォールの間で断続的に発生するネットワーク接続障害やパケットドロップは、802.3xポーズフレームの過剰なボリュームによって引き起こされるソフトウェアキューのロックアップが原因です。スイッチインターフェイスの入力フロー制御を無効にすることで、キューが飽和してロックされるのを防ぎ、問題を解決しました。

関連情報

- Catalyst 9000 スイッチでの出力ドロップのトラブルシュート
- Catalyst スイッチでの STP の問題のトラブルシューティング
- Cisco CatalystスイッチのMACフラップ/ループのトラブルシューティング
- シスコのテクニカルサポートとダウンロード

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。