FAQ:Cisco Catalyst 9000シリーズスイッチでの出力廃棄

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出力廃棄に関してよく寄せられる質問(FAQ)に回答しています。

前提条件

要 件

インターフェイスバッファリングやQuality of Service(QoS)の設定など、スイッチ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。

使用するコンポーネント

このドキュメントは、すべてのCisco Catalyst 9000シリーズスイッチに適用され、特定のハードウェアやソフト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

出力ドロップは、インターフェイスの出力バッファが使い果たされると発生し、パケット損失とネットワークパフォーマンスの低下を引き起こします。一般的な原因には、ネットワークの輻輳、トラフィックのマイクロバースト、設定の誤り、ハードウェアの制限などがあります。このFAQドキュメントでは、Cisco Catalyst 9000シリーズスイッチでの出力ドロップに関する一般的なお問い合せを取り上げています。ネットワークの効率性と信頼性を回復するための根本原因の特定、トラブルシューティング手法、および推奨プラクティスに関するガイダンスを提供します。

Q.出力ドロップとは何ですか。

A. Cisco Catalyst 9000スイッチでの出力ドロップ数とは、パケットがデバイスで処理されているにもかかわらず、インターフェイスから送出されずに廃棄されるパケットの数のことです。これは、インターフェイスの出力キューがいっぱいになると発生します。スイッチインターフェイスには、パケットがポートから送信または転送される前に一時的に保存するハードウェアバッファがあります。発信トラフィックのレートが、ハードウェアで送信できるレートを超えると、バッファがいっぱいになり、キューに到着した追加のパケットはすべて廃棄されます。

Q.出力ドロップの確認に使用できるコマンドはどれですか。

A.コマンドshow interfaces <interface>を使用して、total output dropsカウンタを探します。このカウンタは、そのインターフェイスの出力キューでドロップされたパケットの数を示しています。

例：

<#root>

```
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Input queue: 0/2000/0/0 (size/max/drops/flushes);

Total output drops: 3089


  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

Q.出力廃棄の一般的な原因は何ですか。

A. Catalyst 9000スイッチでの出力ドロップは通常、さまざまな輻輳や設定の問題が原因で、パケットが送信前に廃棄された場合に発生します。一般的な原因には次のものがあります。

- トラフィックのマイクロバースト：数ミリ秒にわたって発生する、突然の高強度のトラフィックのスパイク。通常、標準的なネットワーク監視ツール（SNMPなど）は1分または5分間隔でポーリングを行うため、これらのバーストは管理ソフトウェアからは見えないことが多いものの、ハードウェアの出力バッファを使い果たすには十分です。
- オーバーサブスクリプション：着信トラフィックの集約帯域幅が発信インターフェイスのキャパシティを大幅に超えると、輻輳は回避できません。これは、複数の高速ポート（10Gなど）が単一の低速ポート（1Gなど）にトラフィックを送信するシナリオで一般的です。

- バッファの制約：各インターフェイスのハードウェアバッファ領域の量は限られています。継続的な輻輳が原因で出力キューが最大容量に達すると、スイッチは「テールドロップ」を実行します。後続の着信パケットは、スペースが利用可能になるまで廃棄されます。
- Quality of Service(QoS)の設定ミス：誤って設定されたQoSポリシー（特にアグレッシブポリシングや制限シェーピング）により、ドロップが発生する可能性があります。ポリシーが実際のリンク容量を下回るトラフィックを制限するように設定されている場合、物理リンクが輻輳していなくても、そのしきい値を超えるパケットはドロップされます。
- 速度とデュプレックスのミスマッチ：最近のオートネゴシエーションではあまり一般的ではありませんが、スイッチポートと接続されたデバイス間のミスマッチにより、非効率な送信、（半二重での）コリジョンの増加、およびその後のキューの飽和が発生する可能性があります。
- フロー制御(IEEE 802.3x)：フロー制御が有効な場合、受信側デバイスによる送信を一時停止するようにスイッチに指示できます。ポーズフレームが頻繁に発生すると、スイッチの出力バッファがいっぱいになり、スイッチが伝送の再開を待機する間にドロップが発生する可能性があります。
- ポートチャネルの不均衡：EtherChannel/ポートチャネルのトラフィックがメンバーリンクに均等に分散されないと、1つのインターフェイスが輻輳し、他のインターフェイスが十分に活用されない可能性があります。

Q.マイクロバーストとは何ですか。

A.マイクロバーストは、マイクロ秒またはミリ秒にわたって発生する高強度で短時間のトラフィックスパイクです。Catalyst 9000スイッチの出力ハードウェアバッファがすぐに使い果たされて、出力ドロップが発生します。標準的なモニタリングツールでは、より長い間隔でトラフィックを平均化するため、これらのバーストは頻繁に見えなくなります。その結果、インターフェイスの平均使用率がキャパシティの範囲内に収まっていると思われる場合でも、パケット損失が発生します。したがって、これらの一時的なスパイクは、高速ネットワーク環境における輻輳の主な原因です。

Q.出力ドロップは常に問題になりますか。

A.いいえ、健全なネットワークであっても、短いトラフィックバーストの間は出力廃棄が発生する可能性があります。最近のスイッチではバッファベースのキューイングが使用されており、アプリケーションに影響を与えずに、時折廃棄が発生する可能性があります。 通常、ドロップは次の場合に問題になります。

- 廃棄が継続的に増加する
- アプリケーションで遅延やパケット損失が発生する
- TCP再送信数の増加
- リアルタイムアプリケーション（VoIP/ビデオ）が該当

Q.インターフェイスが完全に使用されていないときでも、出力ドロップが発生するのはなぜですか。

A.出力廃棄は、インターフェイスの使用率がリンクの最大帯域幅（ギガビットインターフェイスで1000 MBPSを大幅に下回る場合など）を大幅に下回る場合でも発生する可能性があります。これは、ネットワークトラフィックが完全にスムーズで連続的なフローで送信されないために発生します。理想的なシナリオでは、すべてのビットがリンク全体に均等に送信され、すべてのデバイスが正確に同期された間隔でトラフィックを送信します。ただし、実際のネットワークでは、デバイスは必要に応じていつでもトラフィックを送信します。その結果、複数のパケットが同時にスイッチに到着することがあり、同じ発信インターフェイスを介して送信される必要があります。この状況に対処するために、スイッチは各インターフェイスでハードウェアバッファを使用します。これらのバッファは、同時に着信したパケットを一時的に保存し、リンク上で順次送信できるようにします。ある時点でインターフェイスに到達するパケットの量が使用可能なバッファ容量を超えると、スイッチではすべてのパケットを保存できなくなります。これが発生すると、超過パケットは廃棄され、その結果、出力廃棄が発生します。

そのため、平均帯域幅使用率が比較的低い（たとえば、1 GBPSインターフェイスで300 MBPS）場合でも、出力の廃棄を観察することができます。 平均使用率は低く見えますが、トラフィックの短いバーストは、インターフェイスのパケット送信能力を一時的に超えたり、使用可能なバッファ容量を超えたりすることがあります。

また、SNMP監視ツールまたはshow interfaceコマンドを使用して表示されるインターフェイス使用率の値は、30秒や5分などの間隔で測定された平均トラフィックに基づいていることにも注意することが重要です。これらの平均は、ミリ秒以内に発生する可能性のある非常に短いトラフィックのスパイクを反映していません。

Q.リンク速度を上げずに出力ドロップを制御するにはどうすればよいのですか。

A.物理的なリンク速度をアップグレードすることなく、Catalyst 9000スイッチでの出力の廃棄を、いくつかの手法で管理および削減できます。

- SoftMax乗数の増加（簡易緩和）：キューが共有バッファプールから要求できるバッファの数を増加させるには、グローバル設定コマンドqos queue-softmax-multiplier <100-1200>を使用して、SoftMaxしきい値を調整できます。デフォルト値は 100 です。この値を1200に設定すると、キューがマイクロバーストを吸収する能力が、デフォルト設定と比較して12倍向上します。

  このコマンドは、ポートキューのしきい値を増やします。これにより、キューは必要に応じて共有バッファプールから追加のバッファユニットを消費できるようになります。これは通常、トラフィックバーストによる出力廃棄を減らす迅速な緩和策として使用されます。 た

だし、バッファは共有リソースであるため、この設定では、すべてのポートでマイクロバーストが同時に発生することはないと想定されています。

キュー単位のバッファの変更（QoSポリシーチューニング）:SoftMax乗数が不十分な場合、QoSポリシーマップを使用してバッファ割り当てをキューレベルで調整できます。これにより、管理者は特定のトラフィッククラスにより多くのバッファスペースを割り当て、キューバッファ比率を変更し、重要なトラフィックのプライオリティキューを設定できます。このアプローチは、特定のトラフィックタイプで専用のバッファリソースが必要な場合や、トラフィックプロファイルが大幅に異なる場合に便利です。

例：

```
policy-map QOS-POLICY
 class VOICE
  priority level 1
  queue-buffers ratio 50
 class class-default
  queue-buffers ratio 50
```

- Quality of Service(QoS)の実装：輻輳時に重要なネットワークトラフィックに優先順位を付けることにより、パケットドロップの制御を支援します。これにより、ネットワークでは、音声やビデオなど遅延の影響を受けやすいトラフィックの優先順位付け、コントロールプレーントラフィックの保護、優先度の低いトラフィックよりも重要なデータの送信を確実に行うことができます。一般的なQoSメカニズムには、トラフィックの分類、キューの優先順位付け、キューバッファの割り当て、輻輳管理などがあります。これらの手法を適用することで、ネットワークは重要度の低いトラフィックを最初に確実に廃棄し、ビジネスクリティカルなアプリケーションを保護して、ネットワーク全体のパフォーマンスを維持できます。

- トラフィックシェーピング：インターフェイスに出力シェーピングを設定して、トラフィックバーストを平滑化します。伝送レートを物理回線レートよりも少し低く制限することで、トラフィックをバッファに強制的に格納し、予測可能な一定のレートで送信できます。これにより、突然の高速マイクロバーストによるテールドロップの動作が防止されます。

例：

```
policy-map SHAPE-POLICY
 class class-default
  shape average
```

- 負荷分散の最適化（ポートチャネルバランシング）:EtherChannelまたはポートチャネルの構成で不均等なハッシュを使用すると、特定のメンバーリンクが輻輳し、その他のリンクが十分に活用されない可能性があります。ロードバランシングアルゴリズムを最適化することで、トラフィックがすべてのメンバーリンクに均等に分散され、個々のインターフェイスでの輻輳が防止され、出力ドロップが軽減されます。

例：

```
port-channel load-balance src-dst-ip
```

Q.出力ドロップの最終的なソリューションは何ですか。

A.出力ドロップを排除する最も効果的なソリューションは、次のとおりです。

- インターフェイスの回線速度を上げる：インターフェイスの速度を上げて、出力帯域幅を大きくし、オーバーサブスクリプションを減らします。たとえば、スイッチで使用可能な場合は、1Gインターフェイスから10Gインターフェイスに移動します。
- ポートバンドリングの使用(EtherChannel)：ポートバンドリングを使用して、複数の物理リンクを1つの論理リンクに集約します（接続デバイスがこの機能をサポートしている場合）。これにより、全体の帯域幅が増加し、トラフィック負荷の分散が促進されます。
- 必要に応じてハードウェアをアップグレード：スイッチで高速インターフェイスを使用できず、接続されたデバイスでポートバンドリングがサポートされない場合は、ハードウェアプラットフォームをより大容量または大容量のバッファを備えたプラットフォームにアップグレードすることを検討してください。

Q.インターフェイスでキューの統計情報をチェックするには、どうすればよいのですか。

A. Catalyst 9000スイッチの場合、show platform hardware fed active qos queue stats interface <port>コマンドを使用して、ハードウェアキューの詳細な統計情報をチェックできます。このコマンドは、指定したインターフェイスでのバッファ使用率、エンキュー数、キューごとのドロップ・カウンタなどの詳細な統計情報を提供し、キューのパフォーマンスを監視して、輻輳またはパケット・ドロップを識別するのに役立ちます。

例：

<#root>

show platform hardware fed switch active qos queue stats interface Gig 1/0/1

```
DATA Port:0 Enqueue Counters
-------------------------------------------------------------------------------------------
Q Buffers          Enqueue-TH0          Enqueue-TH1          Enqueue-TH2             Qpolicer
  (Count)              (Bytes)              (Bytes)              (Bytes)              (Bytes)
- ------- -------------------- -------------------- -------------------- --------------------
0       0                    0                    0

384251797

                  0
1       0                    0                    0

488393930284

                  0
...
DATA Port:0 Drop Counters
-------------------------------------------------------------------------------------------
Q             Drop-TH0             Drop-TH1             Drop-TH2             SBufDrop
                (Bytes)              (Bytes)              (Bytes)              (Bytes)
- -------------------- -------------------- -------------------- -------------------- ----------
0                     0                    0                    0                    0
1                     0                    0

192308101

                  0                    0                    0
...
```

Q. QoSによって出力ドロップが発生しているかどうかを確認するには、どうすればよいのですか。

A. QoSが出力廃棄の原因であるかどうかを確認するには、show policy-map interface <interface>コマンドとキューカウンタを使用して、QoSポリシー統計情報を確認します。 特定のQoSクラスでドロップカウンタが増加している場合は、QoSキュー制限またはポリシングが原因でドロップが発生している可能性があります。 可能であれば、メンテナンスの時間帯に、コマンドno service-policy output <policy-name>を使用してインターフェイスからQoSポリシーを一時的に削除し、出力のドロップが続くかどうかを監視します。ポリシーを削除した後にドロップが停止した場合は、QoS設定がドロップの原因になっている可能性があります。

例：

<#root>

sh policy-map interface gigabitEthernet 1/0/1

```
GigabitEthernet1/0/1
Service-policy output: TEST
Class-map: class-default (match-any)
0 packets
Match: any
Queueing
(total drops) 587230

(bytes output) 834545
...
```

Q.出力廃棄は10Gや40Gなどの高速インターフェイスで発生しますか。

A.はい。10Gや40Gのような高速インターフェイスでも、複数の高速フローが1つのポートに集中している場合に出力廃棄が発生し、インターフェイスバッファがいっぱいになる原因になります。さらに、マイクロバースト（インターフェイスの帯域幅を超えるトラフィックの短いバースト）によって、ポートバッファがすぐに使い果たされてパケットドロップが発生する可能性があります。

Q.出力廃棄はハードウェア障害によって発生する可能性がありますか。

A.出力ドロップは通常、ハードウェア障害が原因ではありません。通常は、トラフィックレートの増加やマイクロバーストによってインターフェイスバッファが過負荷になるトラフィック輻輳が原因で発生します。ハードウェア関連のドロップは発生する可能性がありますが、通常は特定のエラー状態に関連しており、輻輳関連のドロップと比較するとまれです。そのため、出力廃棄は、ハードウェア障害ではなく、主にネットワークトラフィックの状態に関連しています。FCS/CRCエラーなどのインターフェイスエラーの監視は、ハードウェアの問題がある場合の識別に役立ちますが、これらは輻輳によって発生した出力ドロップとは異なります。

Q.ソフトウェアのバグによって出力ドロップが発生する可能性はありますか。

A.ソフトウェアの不具合による出力ドロップは非常にまれで、ほとんどが表面的なものであり、トラフィックに大きな影響を与えることはありません。ほとんどの出力廃棄は、主にトラフィックの輻輳とバッファの枯渇によって発生します。

Q. ECMPまたはロードバランシングによって輻輳を軽減できますか。

A.はい。Equal-Cost Multi-Path(ECMP)ルーティングおよびロードバランシングは、宛先への複数の等コストパス全体にトラフィックを均等に分散させることによって、輻輳を軽減します。このアプローチにより、帯域幅の使用率が向上し、1つのパスがボトルネックになるのを防ぐことができます。

Q.出力廃棄は、TCPとは異なる方法でUDPトラフィックに影響を与えますか。

A.はい。出力ドロップは、TCPとは異なる方法でUDPトラフィックに影響を与えます。これは、UDPは失われたパケットを再送信しないコネクションレス型プロトコルなので、パケット損失が発生すると、適時配信に依存する音声やビデオなどのアプリケーションに直接影響を与えるためです。一方、TCPには、損失したパケットの回復を試みる再送信メカニズムがあり、ドロップの影響が軽減されます。そのため、出力ドロップは、UDPベースのリアルタイムアプリケーションでより顕著な劣化を引き起こす可能性があります。これは、損失したパケットが回復されず、品質問題につながる可能性があるためです。

Q.入力廃棄と出力廃棄の違いは何ですか。

A.インターフェイスでの入力廃棄は通常、入力キューがいっぱいになり、パケットを十分な速度で処理できなくなった場合に発生し、キューイングアルゴリズムに基づいて選択的にパケットが廃棄されます。出力ドロップは、出力キューの輻輳またはバッファの枯渇が原因で、インターフェイスから送信されるパケットがドロップされると発生します。入力廃棄は入力処理の制限に関連しますが、出力廃棄は主に出力輻輳とバッファオーバーフローによって発生します。これらのドロップは、トラフィックバースト、プラットフォームの制限、輻輳やバッファ割り当てを管理するQuality of Service(QoS)設定などの要因の影響を受ける可能性があります。

Q.大きなバックアップジョブによって出力廃棄が発生する可能性はありますか。

A.はい。データバックアップ、レプリケーション、バルク転送などの大規模なバックアップジョブでは、多くの場合、バーストトラフィックが生成され、インターフェイスバッファに過大な負荷がかかり、出力廃棄の原因になります。これらのバーストは、特に発信帯域幅が着信トラフィックレートよりも低い場合や、複数の高速フローが1つのポートに収束する場合、出力インターフェイスで一時的な輻輳を引き起こす可能性があります。

Q.トラフィックバーストによって出力廃棄が発生しているかどうかを判別するには、どうすればよいのですか。

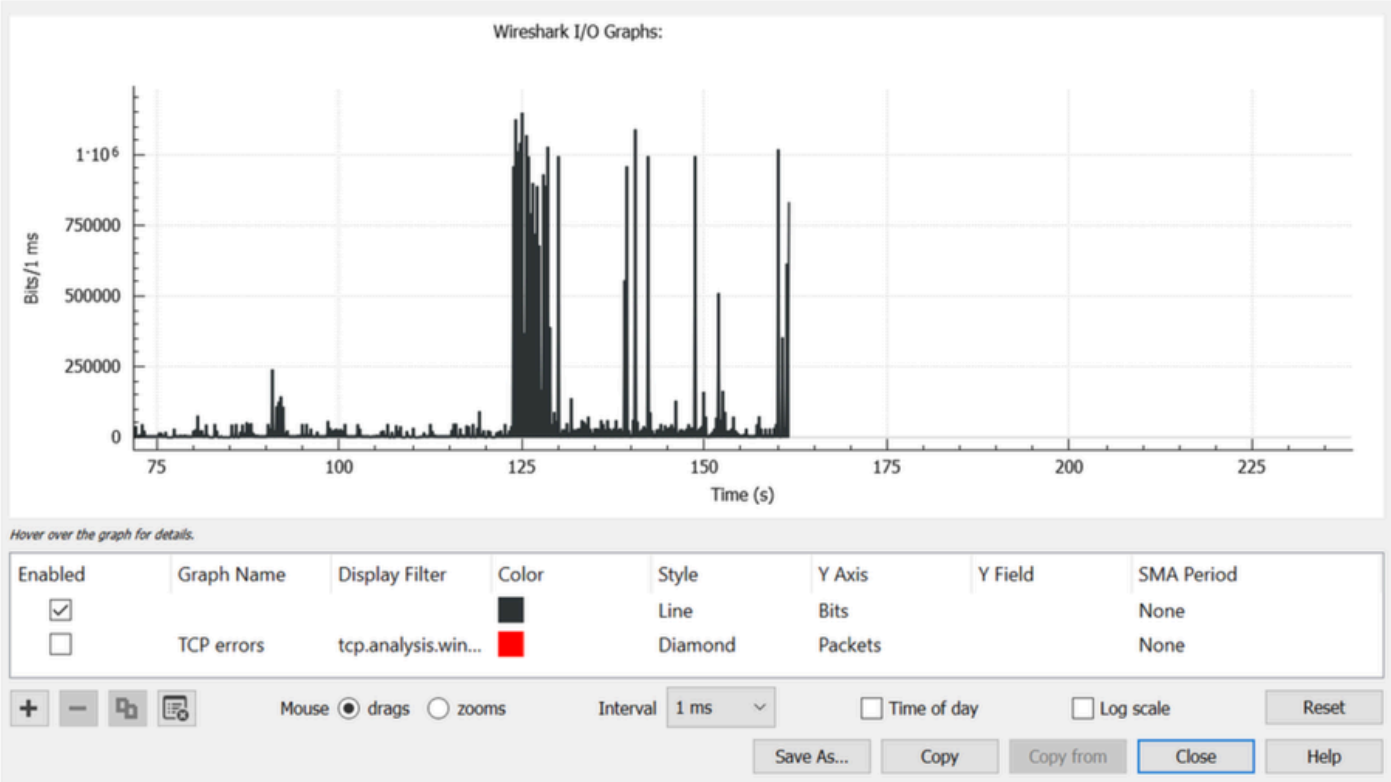
A.トラフィックバーストによる出力ドロップを確認するには、SPANセッションをWiresharkと組み合わせて使用し、出力ドロップが発生している間に、影響を受けるインターフェイスで出力トラフィックをキャプチャして分析します。トラフィックバーストによってトリガーされる出力ドロップを確認するには、次の手順を実行します。

- スイッチの未使用ポートにWiresharkがインストールされているラップトップを接続します。
- スイッチにSPANを設定し、ラップトップが接続されているポートへの出力廃棄が発生しているインターフェイスの出力トラフィックをミラーリングします。

```
monitor session 1 source interface

      Tx

monitor session 1 destination interface

Replace

      with the interface where output drops are seen for the source.

Replace

      with the interface connected to the laptop for the destination.
```

- 関連するトラフィックがキャプチャされるように、出力ドロップがアクティブに増加している間にスイッチでSPANキャプチャを開始します。
- Wiresharkでキャプチャファイルを開き、統計情報> I/Oグラフに移動します。
- [間隔]をデフォルトの1秒から1ミリ秒（1ミリ秒）に変更します。
- グラフを新しい間隔で更新するには、Resetをクリックします。
- グラフには、ビット/ミリ秒単位でトラフィックが表示されます。

ミリ秒スケールでインターフェイスの転送速度を超えるトラフィックの急増を探します（たとえば、1 GBPSインターフェイスでは1,000,000ビット/ミリ秒）。 トラフィックがこの転送速度を超えると、スイッチはパケットをバッファに入れるため、輻輳や出力のドロップが発生する可能性があります。トラフィックの急増（マイクロバースト）を特定するには、急増した後にトラフィックが少ない時間帯や少ない時間帯を観察します。Wiresharkでは、スパイクをクリックすると対応するパケットが選択され、ドロップをトリガーしたトラフィックをさらに分析できます。次の図は、出力廃棄が発生したインターフェイスの更新されたI/Oグラフを示しています。



重要な考慮事項

- 追加のドロップが発生するのを避けるために、SPAN送信元ポートと宛先ポートの速度が同じであるか、または互換性があることを確認します。
- 関連するバーストをキャプチャするために出力廃棄がアクティブに増加している間にトラフィックをキャプチャします。
- Embedded Packet Capture(EPC)は、キャプチャレートを制限し、バーストを見逃す可能性があるため、この目的には推奨されません。

出力ドロップに関する一般的な誤解

誤解：出力のドロップは、ネットワークが正常に機能していないことを意味します。

現実：高速ネットワークでは、マイクロバーストや短いトラフィックのスパイクにより、少数の出力廃棄は正常です。

誤解：インターフェイスの使用率が低い場合、廃棄は発生しません。

現実：使用率は時間の経過に伴う平均として測定されます。マイクロバーストは一時的にインターフェイスの帯域幅を超えることがあり、平均使用率が低い場合でもドロップが発生します。

誤解：出力ドロップは、スイッチのハードウェアに障害があることを意味します。

現実：出力廃棄は通常、ハードウェアの問題ではなく、トラフィックの輻輳またはバーストトラフィックによって発生します。

誤解：バッファ割り当てを増やすと、すべてのドロップが防止されます。

現実：バッファは一時的なバーストだけを吸収します。輻輳が続くと、パケットのドロップが発生します。

誤解：出力ドロップが発生するのは1Gインターフェイスだけです。

現実：トラフィックバーストが使用可能な帯域幅またはバッファ容量を超えると、10G、25G、40G、またはより高速なインターフェイスでドロップが発生する可能性があります。

誤解：QoSでは、すべてのドロップを排除し、パケット損失を防止する必要があります。

現実：QoSは重要なトラフィックに優先順位を付けますが、輻輳時には意図的に優先順位の低いトラフィックをドロップできます。

誤解：出力のドロップはユーザに影響を与えます。

現実：多くのアプリケーションはTCP再送信を使用します。これは、目立った影響を与えることなく、散発的なパケットドロップから回復できます。

誤解：廃棄が発生するのは、インターフェイスの使用率が100 %に達した場合だけです。

現実：ドロップは、平均使用率が低いままであっても、トラフィックの短いバースト中に発生する可能性があります。

誤解：QoS設定は常にドロップの原因になります。

現実：ほとんどのドロップは、QoSポリシーではなく、トラフィックパターンやオーバーサブスクリプションによって発生します。

誤解：正常なネットワークでは出力廃棄が起こらないようにする必要があります。

現実：高性能のスイッチング環境では、ときどきドロップが発生することが予想されますが、これは正常な動作です。

トラブルシューティングガイド

- Catalyst 9000 スイッチでの出力ドロップのトラブルシュート
- Catalyst 9000スイッチのキューバッファ割り当ての理解
- 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。