目次

関連情報

概要

このドキュメントでは、Cisco Catalyst 6500/6000 シリーズ スイッチおよび Virtual Switching System（VSS）1440 ベースのシステムで CPU 使用率が高くなる原因について説明しています。Cisco ルータと同様に、スイッチでは、スイッチのスーパーバイザ エンジン プロセッサの CPU 使用率を表示するのに **show processes cpu** コマンドが使用されます。 ただし、Cisco ルータと Cisco スイッチではアーキテクチャおよび転送メカニズムが異なるため、**show processes cpu** コマンドの一般的な出力も大幅に異なります。 出力の意味は同様に異なります。 この資料はこれらの相違点を明白にし、スイッチの CPU稼働率をおよび **show processes cpu コマンド**出力を理解する方法を記述したものです。

注このドキュメントでは、「スイッチ」という用語は Catalyst 6500/6000 スイッチを指しています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Catalyst 6500/6000 スイッチおよび Virtual Switching System（VSS）1440 ベースのシステムのソフトウェアとハードウェアのバージョンに基づくものです。

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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

注Virtual Switching System（VSS）1440 ベースのシステムにサポートされるソフトウェアは、Cisco IOS® ソフトウェア リリース 12.2(33)SXH1 以降です。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

CatOS と Cisco IOS システム ソフトウェアの違い

スーパーバイザ エンジンで Catalyst OS（CatOS）を使用し、マルチレイヤ スイッチ フィーチャ カード（MSFC）で Cisco IOS® を使用する場合（ハイブリッド）： Catalyst 6500/6000 スイッチでスーパーバイザ エンジンを稼働させるシステム ソフトウェアとして CatOS イメージを使用できます。 オプションの MSFC が取り付けられている場合、MSFC を稼働させるために、別途、Cisco IOS ソフトウェア イメージを使用します。

スーパーバイザ エンジンおよび MSFC 上の Cisco IOS ソフトウェア（ネイティブ）: Catalyst

6500/6000 スイッチでスーパーバイザ エンジンと MSFC の両方を稼働させるシステム ソフトウェアとして単一の Cisco IOS ソフトウェア イメージを使用できます。

注詳細は、『Cisco Catalyst 6500 シリーズ スイッチのための Cisco Catalyst オペレーティング システムと Cisco IOS オペレーティング システムの比較』を参照してください。

Catalyst 6500/6000 スイッチの CPU 使用率について

Cisco のソフトウェアベースのルータでは、パケットの処理とルーティングをソフトウェアで処理しています。 ルータによるパケットの処理とルーティングが多くなると、ルータの CPU 使用率も高くなります。 そのため、**show processes cpu** コマンドでは、ルータでのトラフィック処理の負荷がかなり正確に表示されます。

Catalyst 6500/6000 スイッチでの CPU の使用方法は、これとは異なっています。 これらのスイッチでは、ソフトウェアではなく、ハードウェアで転送が決定されます。 そのため、スイッチを通過するほとんどのフレームの転送またはスイッチングの決定をする際には、スーパーバイザ エンジンの CPU は使用されません。

Catalyst 6500/6000 スイッチには CPU が 2 つ備わっています。 一方の CPU はスーパーバイザ エンジンの CPU で、Network Management Processor（NMP; ネットワーク管理プロセッサ）あるいはスイッチ プロセッサ（SP）と呼ばれるものです。 他方の CPU はレイヤ 3 ルーティング エンジンの CPU で、MSFC あるいはルート プロセッサ（RP）と呼ばれるものです。

SP の CPU は次のような機能を実行します。

- MAC アドレス学習とエージングの支援**注**MAC アドレス学習はパス設定（path setup）とも呼ばれます。
- ネットワーク制御を実現するプロトコルおよびプロセスの実行例としては、Spanning Tree Protocol（STP; スパニングツリー プロトコル）、Cisco Discovery Protocol（CDP; Cisco 検出プロトコル）、VLAN Trunk Protocol（VTP; VLAN トランク プロトコル）、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）などがあります。
- スイッチの CPU を宛先とするネットワーク管理トラフィックの処理例としては、Telnet、HTTP、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）のトラフィックなどがあります。

RP の CPU は次のような機能を実行します。

- レイヤ 3 ルーティング テーブルと Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルの構築とアップデート
- Cisco Express Forwarding（CEF; Cisco エクスプレス転送）Forwarding Information Base（FIB; 転送情報ベース）および隣接関係テーブルの生成とそれらのテーブルの Policy Feature Card（PFC; ポリシー フィーチャ カード）へのダウンロード
- RP を宛先とするネットワーク管理トラフィックの処理例としては、Telnet、HTTP、SNMP のトラフィックなどがあります。

トラフィックがソフトウェアに渡される契機となる状態および機能

スイッチを宛先とするパケット

スイッチを宛先とするパケットはすべてソフトウェアに渡されます。 たとえば、次のようなパケットがあります。

- 制御パケット制御パケットは、STP、CDP、VTP、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）、PAgP、Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）、UniDirectional Link Detection（UDLD; 単方向リンク検出）用に受信されます。
- ルーティング プロトコルの更新これらのプロトコルの例としては、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）および Open Shortest Path First Protocol（OSPF プロトコル）があります。
- スイッチを宛先とする SNMP トラフィック
- スイッチへの Telnet および Secure Shell Protocol （SSH）トラフィック。SSH による高 CPU ultilization はとして見られます:CPU が高く行くとき確立される SSH セッションの数を確認するために EEM スクリプトにこれらのコマンドを含めて下さい:show usersshow line
- ARP 要求に対する ARP 応答

特別な処理が必要なパケットおよび条件

次のリストは、ソフトウェアによるパケット処理が必要になる特別なパケット タイプおよび条件を示しています。

- IP オプション、有効期限が切れた Time to Live（TTL; 存続可能期間）、または Advanced Research Projects Agency（ARPA）以外のカプセル化が指定されたパケット
- トンネリングなどの特別な処理が指定されたパケット
- IP フラグメンテーション
- RP または SP からの Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）メッセージが必要なパケット
- Maximum Transmission Unit（MTU; 最大伝送ユニット）のチェックに失敗した場合
- IP チェックサムや長さのエラーなどの IP エラーがあるパケット
- インプットパケットがエラーを少し返せば（のようなシングルビットエラー（SBE））、パケットは処理するソフトウェアのための CPU に送信され訂正されます。 これらのパケットにはバッファが割り当てられ、修正するために CPU リソースが使用されます。
- PBR とリフレクシブ アクセス リストがトラフィック フローのパス内にある場合、パケットのソフトウェア スイッチが入れられ、追加の CPU サイクルが必要になります。
- 隣接関係が同一インターフェイス上にある場合（通信の着信 Interface と送信 Interface が同一である場合）
- 予約パス転送（RPF）チェック失敗するパケットか。**RPF障害**
- Glean/receiveGlean は ARP による解決が必要なパケットを指し、receive は受信ケースに分類されるパケットを指しています。
- Cisco IOS ソフトウェアと CatOS のいずれの場合でも、Supervisor Engine 720 でソフトウェアによってスイッチングされた Internetwork Packet Exchange（IPX）トラフィックIPX トラフィックは、Cisco IOS ソフトウェアが稼働する スーパーバイザ エンジン 2 でもソフトウェアによってスイッチングされますが、CatOS が稼働する スーパーバイザ エンジン 2 ではハードウェアによってスイッチングされます。 Supervisor Engine 1A では、どちらのオペレーティング システムが稼働していても、IPX トラフィックはハードウェアによってスイッチ

ングされます。
- AppleTalk トラフィック
- ハードウェア リソースがいっぱいになった場合これらのリソースには、FIB、Content-Addressable Memory（CAM; 連想メモリ）、Ternary CAM（TCAM; 三値連想メモリ）などが含まれます。

ACL ベースの機能

- Access Control List（ACL; アクセス コントロール リスト）で拒否され、ICMP 到達不能機能がオンになっているトラフィック**注**これはデフォルトです。IP 到達不能が有効になっている場合には、ACL で拒否された一部のパケットは MSFC にリークされます。 ICMP 到達不能であることが必要なパケットは、ユーザが設定可能なレートでリークされます。 デフォルトでは、このレートは 500 パケット/秒（pps）になっています。
- 発信元ホストなどのサポートされていないパラメータに基づく IPX フィルタリング Supervisor Engine 720 では、レイヤ 3 IPX トラフィックの処理は常にソフトウェアで行われます。
- **log** キーワードが付いた、ロギングを必要とするアクセス コントロール エントリ（ACE）この条件は、ACL ログおよび VLAN ACL（VACL）ログの機能に適用されます。 同じ ACL 内のロギング不要の ACE は、引き続きハードウェアで処理されます。 PFC3 が搭載されたスーパーバイザ エンジン 720 では、ACL および VACL のロギング用に MSFC にリダイレクトされるパケットのレート制限がサポートされています。 スーパーバイザ エンジン 2 では、VACL のロギング用に MSFC にリダイレクトされるパケットのレート制限がサポートされています。 スーパーバイザ エンジン 2 上での ACL ロギングのサポートは、Cisco IOS ソフトウェア リリース 12.2S ブランチで予定されています。
- **match length**、**set ip precedence**、あるいは他の非サポート パラメータでポリシー ルーティングされたトラフィック**set interface** パラメータはソフトウェアでサポートされています。ところが、**set interface null 0** パラメータは例外です。 このトラフィックは、PFC2 が搭載されたスーパーバイザ エンジン 2 および PFC3 が搭載されたスーパーバイザ エンジン 720 では、ハードウェアによって処理されます。
- IP 以外および IPX 以外の Router ACL（RACL）IP 以外の RACL はすべてのスーパーバイザ エンジンに適用されます。 IPX 以外の RACL は、PFC が搭載されたスーパーバイザ エンジン 1A および PFC2 が搭載されたスーパーバイザ エンジン 2 だけに適用されます。
- RACL で拒否されたブロードキャスト トラフィック
- ユニキャスト RPF（uRPF; ユニキャスト リバース パス転送）チェックおよび ACL ACE で拒否されたトラフィックこの uRPF チェックは、PFC2 が搭載されたスーパーバイザ エンジン 2 および PFC3 が搭載されたスーパーバイザ エンジン 720 に適用されます。
- 認証プロキシ認証プロキシの対象となるトラフィックは、スーパーバイザ エンジン 720 でレート制限できます。
- Cisco IOS ソフトウェアの IP セキュリティ（IPSec）Cisco IOS の暗号化の対象となるトラフィックは、スーパーバイザ エンジン 720 でレート制限できます。

NetFlow ベースの機能

このセクションで説明する NetFlow ベースの機能は、スーパーバイザ エンジン 2 とスーパーバイザ エンジン 720 だけに適用されます。

- NetFlow ベースの機能の場合は、フローの最初のパケットを常にソフトウェアでチェックする必要があります。 フローの最初のパケットがソフトウェアに到達したら、同じフローの後

続のパケットはハードウェアでスイッチングされます。このフロー調整は、リフレクシブ ACL、Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）および Cisco IOS Server Load Balancing（SLB; サーバ ロード バランシング）に適用されます。**注**スーパーバイザ エンジン 1 では、リフレクシブ ACL の場合に、動的な TCAM エントリを基にして、特定のフローのハードウェア ショートカットが作成されます。 原則は同じです。最初のパケットはソフトウェアに渡されますが、 そのフローの後続のパケットは、ハードウェアでスイッチングされます。

- TCP インターセプト機能を使用すると、3 ウェイ ハンドシェイクおよびセッション クローズがソフトウェアで処理されます。 残りのトラフィックは、ハードウェアで処理されます。**注** 同期（SYN）、SYN 確認応答（SYN ACK）および ACK のパケットで、3 ウェイ ハンドシェイクが行われます。 セッション クローズは、完了（FIN）またはリセット（RST）で行われます。
- Network Address Translation（NAT; ネットワーク アドレス変換）が入ると、トラフィックが次のように処理されます。スーパーバイザ エンジン 720 の場合：NAT が必要なトラフィックは、最初の変換後はハードウェアで処理されます。 フローの最初のパケットの変換はソフトウェアで行われ、そのフローの後続のパケットはハードウェアによってスイッチングされます。 TCP パケットの場合は、TCP 3 ウェイ ハンドシェイクの完了後は、NetFlow テーブルにハードウェア ショートカットが作成されます。スーパーバイザ エンジン 2 およびスーパーバイザ エンジン 1 の場合：NAT が必要なトラフィックはすべて、ソフトウェアでスイッチングされます。
- Context-based Access Control（CBAC; コンテキストベース アクセス制御）では、検査が必要なトラフィックを分類するために、NetFlow ショートカットを使用します。 次に、CBAC によって、このトラフィックだけがソフトウェアに送られます。 CBAC は、ソフトウェアのみの機能です。 検査対象のトラフィックは、ハードウェアではスイッチングされません。**注** 検査の対象となるトラフィックは、スーパーバイザ エンジン 720 でレート制限できます。

マルチキャスト トラフィック

- Protocol Independent Multicast（PIM）のスヌーピング
- インターネット グループ管理プロトコル（IGMP）のスヌーピング（TTL = 1）このトラフィックの宛先は、実際にはルータになっています。
- Multicast Listener Discovery（MLD）のスヌーピング（TTL = 1）このトラフィックの宛先は、実際にはルータになっています。
- FIB の誤り
- マルチキャストの発信元に直接接続されている登録用マルチキャスト パケットこれらのマルチキャスト パケットは、ランデブー ポイントにトンネリングされています。
- IP version 6（IPv6）マルチキャスト

その他の機能

- Network-Based Application Recognition（NBAR）
- ARP 検査（CatOS 使用時のみ）
- ポート セキュリティ（CatOS 使用時のみ）
- DHCP スヌーピング

IPv6 の状況

- ホップバイホップ オプション ヘッダーが設定されたパケット
- ルータの宛先 IPv6 アドレスと同じ宛先 IPv6 アドレスが設定されたパケット
- スコープ施行チェックに不合格だったパケット
- 出力リンクの MTU を超えるパケット
- 1 以下の TTL が設定されたパケット
- 出力 VLAN と同じ入力 VLAN が設定されたパケット
- IPv6 uRPFこの uRPF は、すべてのパケットに対してソフトウェアで処理されます。
- IPv6 のリフレクシブ ACLこれらのリフレクシブ ACL はソフトウェアで処理されます。
- IPv6 の Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)トンネル用の 6to4 プレフィックスこのトンネリングは、ソフトウェアで処理されます。 ISATAP トンネルに入る他のすべてのトラフィックは、ハードウェアによってスイッチングされます。

LCP スケジューラと DFC モジュール

Distributed Forwarding Card（DFC）では、lcp schedular プロセスが CPU 高使用率状態で稼働することに問題はなく、動作に対する問題は発生しません。 LCP スケジューラの機能はファームウェア コードに取り込まれています。 DFC を必要としないすべてのモジュールでは、このファームウェアは Line Card Processor（LCP）と呼ばれる特定のプロセッサで稼働します。 このプロセッサは、ASIC ハードウェアをプログラムし、中央のスーパーバイザ モジュールと通信するために使用されます。

lcp schedular が起動されると、利用可能なプロセス時間がすべて使用されます。 新しいプロセスでプロセッサの時間が必要になると、lcp schedular は、この新しいプロセスにプロセス時間を空け渡します。 この CPU 高使用率に関して、システムのパフォーマンスへの影響はありません。 このプロセスでは、より優先度の高いプロセスが CPU サイクルを必要としていない限り、単純に未使用の CPU サイクルがすべて専有されるだけです。

```
DFC#show process cpuPID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process  22
0         1      0   0.00%  0.00%  0.00%   0 SCP ChilisLC Lis   23           0         1      0
0.00%  0.00%  0.00%   0 IPC RTTYC Messag   24           0         9      0   0.00%  0.00%  0.00%
0 ICC Slave LC Req   25           0         1      0   0.00%  0.00%  0.00%   0 ICC Async mcast
26           0         2      0   0.00%  0.00%  0.00%   0 RPC Sync           27           0
1      0   0.00%  0.00%  0.00%   0 RPC rpc-master     28           0         1      0   0.00%
0.00%  0.00%   0 Net Input          29           0         2      0   0.00%  0.00%  0.00%   0
Protocol Filteri   30           8       105     76   0.00%  0.00%  0.00%   0 Remote Console P
31          40      1530     26   0.00%  0.00%  0.00%   0 L2 Control Task    32          72
986     73   0.00%  0.02%  0.00%   0 L2 Aging Task      33           4        21    190   0.00%
0.00%  0.00%   0 L3 Control Task    34          12       652     18   0.00%  0.00%  0.00%   0
FIB Control Task   35        9148       165  55442   1.22%  1.22%  1.15%   0 Statistics Task
36           4       413      9   0.00%  0.00%  0.00%   0 PFIB Table Manag   37      655016
64690036     10  75.33% 77.87% 71.10%   0 lcp schedular      38           0       762      0
0.00%  0.00%  0.00%   0 Constellation SP
```

CPU 高使用率問題の一般的な原因とソリューション

IP 到達不能

アクセス グループでパケットが拒否されると、MSFC から ICMP 到達不能メッセージが送信されます。 このアクションはデフォルトで実行されます。

ip unreachables コマンドはデフォルトでイネーブルにされているので、ハードウェア内にある拒否されたパケットはほとんどスーパーバイザ エンジンにより廃棄されます。 次に、少数のパケット（最大で 10 pps）はスーパーバイザ エンジンから MSFC に送られ、廃棄されます。 このアク

ションによって、ICMP 到達不能メッセージが生成されます。

拒否されたパケットの廃棄および ICMP 到達不能メッセージの生成によって、MSFC の CPU に負荷がかかります。 負荷を軽減するには、**no ip unreachables** インターフェイス設定コマンドを発行できます。 このコマンドを実行すると、ICMP 到達不能メッセージが生成されなくなり、アクセス グループで拒否されたパケットをすべてハードウェアで廃棄できるようになります。

パケットが VACL によって拒否された場合は、ICMP 到達不能メッセージは送信されません。

NAT 変換

NAT ではハードウェアとソフトウェアの両方の転送が使用されます。 NAT 変換の最初の確立はソフトウェアで行う必要があり、以降の転送はハードウェアで行われます。 NAT では Netflow テーブル (最大 128 KB) も使用されます。 そのため、Netflow テーブルがいっぱいになると、スイッチではソフトウェアによる NAT 転送の適用が開始されることにもなります。 通常、トラフィックの高いバースト状態でこれが発生し、6500 の CPU 使用率が増大することになります。

フロー キャッシュ テーブル内の CEF FIB テーブル スペースの使用

スーパーバイザ エンジン 1 には、128,000 エントリをサポートするフロー キャッシュ テーブルがあります。 ところが、ハッシュ アルゴリズムの有効性に基づく限り、これらのエントリの範囲は 32,000 ~ 120,000 になります。 Supervisor Engine 2 では、PFC に FIB テーブルが作成されて、プログラムされます。 このテーブルには最大 256,000 エントリを収容できます。 PFC3-BXL が搭載されたスーパーバイザ エンジン 720 では、最大 1,000,000 エントリがサポートされます。 このスペースを使い切ると、パケットがソフトウェアでスイッチングされるようになります。 この状態になると、RP の CPU 使用率が高くなる可能性があります。 CEF FIB テーブル内のルート数を調べるには、次のコマンドを使用します。

```
Router#show processes cpuCPU utilization for five seconds:  99.26%                    one
minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs    5Sec
1Min    5Min    TTY Process--- ---------- ---------- -------- ------- ------- ------- --- -----
----------1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle2   2
245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0           1          0
0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0          0.00%   0.00%
0.00% -2  L2L3PatchRev   5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi!-
-- Output is suppressed.26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib            29
0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task  !--- Output is
suppressed.CATOS% show mls cefTotal L3 packets switched:           124893998234Total L3 octets
switched:          53019378962495Total route entries:                    112579  IP route
entries:                        112578  IPX route entries:                         1  IPM
route entries:                            0IP load sharing entries:                  295IPX
load sharing entries:                     0Forwarding entries:
112521Bridge entries:                              56Drop entries:
2IOS% show ip cef summaryIP Distributed CEF with switching (Table Version 86771423), flags=0x0
112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)  112567 leaves, 6888 nodes, 21156688
bytes, 86771426inserts, 86658859invalidations  295 load sharing elements, 96760 bytes, 112359
references  universal per-destination load sharing algorithm, id 8ADDA64A  2 CEF resets, 2306608
revisions of existing leaves  refcounts:  1981829 leaf, 1763584 node!--- You see these messages
if the TCAM space is exceeded:%MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM exception, Some entries will
be software switched%MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM exception cleared, all CEF entries
will be hardware switched
```

スーパーバイザ エンジン 2 では、インターフェイスに RPF チェックを設定すると、FIB エントリの数が半分に減ります。 このように設定すると、より多くのパケットがソフトウェアによってスイッチングされるようになり、結果的に CPU 使用率が高くなる場合があります。

CPU 高使用率の問題を解決するには、経路集約を有効にします。 経路集約により、プロセッサのワークロード、メモリ要求、および帯域幅要求が削減され、複雑なネットワークにおける遅延を最小化することができます。

TCAM の使用と最適化についての詳細は、『Catalyst 6500 シリーズ スイッチでの ACL について』を参照してください。

Optimized ACL Logging (OAL; ACL ロギングの最適化)

Optimized ACL Logging (OAL; ACL ロギングの最適化) を使用すれば、ACL ロギングがハードウェアでサポートされます。 OAL を設定しなければ、ロギングが必要なパケットの処理は MSFC3 上のソフトウェアですべて処理されます。 OAL では、PFC3 上のハードウェアでパケットの許可または廃棄が行われます。 OAL では、ロギング メッセージを生成するために、最適化されたルーチンを使用して MSFC3 に情報が送信されます。

注OAL についての詳細は、『Cisco IOS ACL サポートについて』の「*PFC3 での最適化 ACL*」セクションを参照してください。

CPU に対するパケットのレート制限

スーパーバイザ エンジン 720 では、レート制限機能によって、ソフトウェアに渡すパケットのレートを制御できます。 このレート制御機能は、サービス拒否攻撃の防止に役立ちます。 スーパーバイザ エンジン 2 でも、いくつかのレート制限機能を使用できます。

```
Router#show mls rate-limit   Rate Limiter Type       Status     Packets/s   Burst--------------
------   ----------   ---------   -----         MCAST NON RPF   Off                  -       -
MCAST DFLT ADJ   On              100000     100      MCAST DIRECT CON   Off                  -
-        ACL BRIDGED IN   Off                  -       -       ACL BRIDGED OUT   Off
-       -           IP FEATURES   Off                 -       -          ACL VACL LOG   On
2000       1           CEF RECEIVE   Off                  -       -             CEF GLEAN   Off
-       -      MCAST PARTIAL SC   On              100000     100        IP RPF FAILURE   On
500      10           TTL FAILURE   Off                  -       -ICMP UNREAC. NO-ROUTE   On
500      10ICMP UNREAC. ACL-DROP   On                 500      10         ICMP REDIRECT   Off
-       -           MTU FAILURE   Off                 -       -           LAYER_2 PDU   Off
-       -            LAYER_2 PT   Off                 -       -             IP ERRORS   On
500      10           CAPTURE PKT   Off                  -       -            MCAST IGMP   Off
-       -Router(config)#mls rate-limit ?  all        Rate Limiting for both Unicast and
Multicast packets  layer2     layer2 protocol cases  multicast  Rate limiting for Multicast
packets  unicast    Rate limiting for Unicast packets
```

次に例を示します。

```
Router(config)#mls rate-limit layer2 l2pt 3000
```

CEF によって MSFC にパントされるすべてのパケットをレート制限するには、次の例のようなコマンドを実行します。

```
Router(config)#mls ip cef rate-limit 50000
```

TTL=1 により CPU にパントされるパケット数を削減するには、次のコマンドを発行します。

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

たとえば、これは IPv4 TTL は 1 であることを示す **netdr キャプチャ**の出力です、:

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

CPU に漏出される TTL=1 のパケットにより、CPU 使用率が高まることもあります。 CPU に漏

出するパケット数を制限するには、ハードウェア レート リミッタを設定します。 レート リミッタでは、ハードウェア データ パスからソフトウェア データ パスに漏出されるパケットをレート制限できます。 レート リミッタでは、設定レートを超過するトラフィックを廃棄することにより、ソフトウェア制御パスでの輻輳を防ぎます。 レート制限は、mls rate-limit all ttl-failure コマンドで設定されます。

ケーブル接続の不備による VLAN の物理的マージ

ケーブル接続の不備により、複数の VLAN がマージされた場合にも、CPU 使用率が高くなる可能性があります。 また、VLAN のマージが発生しているポートで STP が無効になっている場合にも、CPU 使用率が高くなる可能性があります。

この問題を解決するには、ケーブル配線の間違いを見つけて修正してください。 使用上の要件から見て、これらのポートで STP を有効にできる場合は、有効にすることもできます。

ブロードキャスト ストーム

ブロードキャストやマルチキャストのパケットが LAN でフラッディングした場合に LAN ブロードキャスト ストームが発生し、これにより、過剰なトラフィックが発生して、ネットワークのパフォーマンスが低下します。 ブロードキャスト ストームを引き起こす可能性があるのは、プロトコル スタックの実装やネットワーク設定でのエラーです。

Catalyst 6500 シリーズ プラットフォームのアーキテクチャ設計により、ブロードキャスト パケットが廃棄されるのは常にソフトウェア レベルでのみです。

ブロードキャスト ストームによる LAN インターフェイスの中断は、ブロードキャスト抑制により防げます。 ブロードキャスト抑制では、LAN で 1 秒間のブロードキャスト アクティビティを測定して、その測定結果を事前に定義されたしきい値と比較するフィルタリングが使用されています。 しきい値に達すると、指定された時間の間、以降のブロードキャスト アクティビティが抑制されます。 デフォルトでは、ブロードキャスト抑制はディセーブルになっています。

注マスターするべきバックアップからの VRRP フラッピングによりブロードキャスト ストームによりによって引き起こされて CPU使用率が高い状態を引き起こすかもしれません。

ブロードキャスト抑制の動作方法を理解して、この機能をイネーブルにするには、次のドキュメントを参照してください。

- ブロードキャスト抑制の設定（Cisco IOS システム ソフトウェア）
- ブロードキャスト抑制の設定（CatOS システム ソフトウェア）

BGP ネクストホップ アドレス トラッキング（BGP スキャナ プロセス）

BGP スキャナは BGP テーブルを走査して、ネクストホップの到達可能性を確認します。 このプロセスでは、BGP で条件プレフィクスのアドバタイズやルート ダンプニングの実施を行うべきかどうかを判断するために、条件付きアドバタイズのチェックも行われます。 デフォルトでは、このプロセスにより 60 秒ごとにスキャンが行われます。

ルータでの BGP スキャナ プロセスで大量のインターネット ルーティング テーブルが搬送されることにより、短い期間ですが CPU の使用率が高まる可能性があります。 1 分間に一度、BGP スキャナでは BGP Routing Information Base（RIB）テーブルの走査を行って、重要なメンテナンス タスクを実行します。 これには、次のようなタスクがあります。

- ルータ BGP テーブルで参照されているネクストホップのチェック
- ネクストホップ デバイスが到達可能であることの確認

このため、BGP テーブルが大きいと、大きさに応じてスキャンおよび検証に時間がかかることになります。 BGP スキャナ プロセスでは、データ ストラクチャをアップデートするために BGP テーブルが走査され、ルート再配布のためにルーティング テーブルが走査されます。 両方のテーブルはルータ メモリに別々に保存されています。 どちらのテーブルも非常に大きくなる場合があり、これにより CPU サイクルが消費されます。

BGP スキャナ プロセスによる CPU 使用率についての詳細は、『*トラブルシューティング：BGP スキャナまたは BGP ルータ プロセスが原因で発生する CPU 高使用率*』の「CPU 高使用率の原因が BGP スキャナにある場合」セクションを参照してください。

BGP ネクストホップ アドレス トラッキング機能と有効/無効にする手順あるいはスキャン間隔の調整についての詳細は、『ネクストホップ アドレス トラッキングに関する BGP サポート』を参照してください。

非 RPF マルチキャスト トラフィック

ユニキャスト ルーティングとは異なり、マルチキャスト ルーティングで有意なのは、それぞれのマルチキャスト データ ストリームの送信元だけです。 これはつまり、マルチキャスト トラフィックを発信するデバイスの IP アドレスのことです。 送信元デバイスが（マルチキャスト グループ内の）個数未指定の受信者にストリームを「プッシュ」するというのが、基本原理になります。 すべてのマルチキャスト ルータでは配布ツリーが作成され、これにより、すべての受信者にトラフィックを配信するためにマルチキャスト トラフィックがネットワーク上で経由するパスが制御されます。 マルチキャスト配布ツリーの 2 つの基本タイプとして、送信元ツリーと共有ツリーがあります。 RPF はマルチキャスト転送での重要概念です。 これにより、ルータではマルチキャスト トラフィックの配布ツリーへの正確な転送が可能になります。 RPF では、既存のユニキャスト ルーティング テーブルを使用して、アップストリームとダウンストリームのネイバーを判別します。 ルータでマルチキャスト パケットが転送されるのは、アップストリーム インターフェイスで受信された場合だけです。 この RPF チェックは、配布ツリーにループが形成されないことを保証するのに有効です。

IEEE 802.3 CSMA/CD 仕様によると、マルチキャスト トラフィックはブリッジド（レイヤ 2）LAN 上の各ルータで常時認識可能です。 802.3 標準では、ブロードキャストやマルチキャスト フレームの表示には最初のオクテットのビット 0 が使用され、このアドレスを持つすべてのレイヤ 2 フレームがフラッディングされます。 これは、CGMP や IGMP スヌーピングが設定されている場合にも当てはまります。 これは、マルチキャスト ルータでは、適切な転送決定（forwarding decision）を行う必要がある場合、マルチキャスト トラフィックが認識されている必要があるためです。 複数のマルチキャスト ルータそれぞれに共通の LAN へのインターフェイスが備わっている場合、データを転送するルータは 1 つだけで、このルータは選出プロセスで選ばれます。 LAN のフラッディング特性により、冗長ルータ（マルチキャスト トラフィックを転送していないルータ）では、このデータはその LAN のアウトバウンド インターフェイスで受信されます。 このデータは誤ったインターフェイスに到着していて、RPF チェックが失敗するため、通常、冗長ルータではこのトラフィックは廃棄されます。 RPF チェックに失敗したトラフィックは、送信元からフローの反対方向に転送されているため、非 RPF トラフィックあるいは RPF 障害パケットと呼ばれます。

MSFC がインストールされた Catalyst 6500 は、フルフレッジ マルチキャスト ルータとして機能するように設定できます。 マルチキャスト マルチレイヤ スイッチング（MMLS）を使用すると、通常、RPF トラフィックはスイッチ内のハードウェアにより転送されます。 ASIC には (*,G) および (S,G) などのマルチキャスト ルーティング ステートから情報が提供されているため、ハードウェア ショートカットを Netflow や FIB のテーブルにプログラムできます。 この非 RPF トラ

フィックが必要な場合も依然として残っており、PIM アサート メカニズム用に (プロセス レベルでの) MSFC CPU で必要とされます。 それ以外の場合は、ソフトウェア ファースト スイッチング パスで廃棄されます (RPF インターフェイスでソフトウェア ファースト スイッチングがディセーブルになっていないことが前提) 。

冗長構成が採用された Catalyst 6500 では、特定のトポロジで非 RPF トラフィックが効率的に処理されない場合があります。 非 RPF トラフィックに関しては、通常、冗長ルータには (*,G) や (S,G) のステートがないため、ハードウェアやソフトウェアのショートカットを作成してパケットを廃棄することはできません。 各マルチキャスト パケットは MSFC ルート プロセッサで個別に検査する必要があり、これが CPU 割り込みトラフィックとされることがよくあります。 レイヤ 3 ハードウェア スイッチングが行われていて、複数のインターフェイス/VLAN が同じルータのセットに接続されている場合、冗長 MSFC の CPU に影響する非 RPF トラフィックは、元のソース レートの「N」倍に増幅されます (「N」はルータが冗長的に接続されている LAN の数です) 。 非 RPF トラフィックのレートがシステムのパケット廃棄容量を超過すると、CPU 高使用率やバッファ オーバーフローが発生したり、ネットワークが全体的に不安定になる可能性があります。

Catalyst 6500 の場合、ワイヤ レートでのフィルタリングをイネーブルにするアクセス リスト エンジンがあります。 特定の状況では、この機能を使用して、sparse (希薄) モード グループ用の非 RPF トラフィックを効率的に処理できます。 sparse (希薄) モードの「スタブ ネットワーク」内で使用できるのは ACL ベースの方法だけで、この場合、ダウンストリームのマルチキャスト ルータ (および対応する受信者) はありません。 さらに、Catalyst 6500 のパケット転送設計により、内部での冗長 MSFC では、この実装を使用できません。 これは、Cisco Bug ID CSCdr74908 (登録ユーザ専用) で概説されています。 dense (稠密) モード グループでは、PIM アサート メカニズムが適切に機能するのためには、非 RPF パケットがルータで認識される必要があります。 dense (稠密) モードのネットワークと sparse (希薄) モードの中継ネットワークで RPF 障害を制御するには、CEF や Netflow ベースのレート制限および QoS などの他のソリューションが使用されます。

Catalyst 6500 には、ワイヤ レートでのフィルタリングをイネーブルにするアクセス リスト エンジンがあります。 この機能を使用して、希薄モード グループの非 RPF トラフィックを効率的に処理できます。 このソリューションを実装するには、「スタブ ネットワーク」の受信インターフェイスにアクセス リストを置いて、「スタブ ネットワーク」から発信されたものではないマルチキャスト トラフィックをフィルタリングします。 このアクセス リストはスイッチのハードウェアにプッシュされます。 このアクセス リストにより、CPU でパケットを常時監視し続ける必要がなくなり、非 RPF トラフィックはハードウェアで廃棄できるようになります。

注このアクセス リストを中継インターフェイスには置かないようにしてください。 これはスタブ ネットワーク (ホストのあるネットワークのみ) を対象にしています。

詳細は、次のドキュメントを参照してください。

- スタブ ネットワーク内での IP マルチキャストによる冗長ルータの問題
- 非 RPF トラフィック処理

show コマンド

show コマンドを発行すると、CPU 使用率が常に 100 % 近辺になります。 **show** コマンドを発行した際に CPU 使用率が高くなるのは正常な状態で、通常、これが続くのは数秒間だけです。

たとえば、**show tech-support** コマンドを発行すると、この出力は割り込み駆動による出力であるため、Virtual Exec プロセスが高くなるのは正常な状態です。 問題となるのは、**show** コマンド以

外の他のプロセスで CPU 使用率が高くなる場合です。

および何かパケットが MSFC（レシーブ、IPオプション、隣接関係無し、等）になぜパントされるか show cef not-cef-switched コマンドに示されています。 次に、例を示します。

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0         0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

提示 ibc は CPU ステータスを監視しているとき **ibc が簡潔な**コマンド CPU キューを示し、使用することができることを示し。

Exec プロセス

Cisco IOS ソフトウェアでの Exec プロセスは、ルータの TTY 回線（コンソール、補助、非同期）での通信を受け持っています。 仮想 Exec プロセスが受け持つのは VTY 回線（Telnet セッション）です。 Exec および Virtual Exec プロセスは優先順位が中程度のプロセスなので、より優先順位の高い（High または Critical）のプロセスがあると、優先順位がより高いプロセスが CPU リソースを獲得します。

これらのセッションで大量のデータが送受信されると、Exec プロセスによる CPU 使用率が高まります。 これらの回線では、ルータが単に 1 文字を送信する場合でも CPU リソースが使用されてしまうということが、この原因です。

- コンソール（Exec）の場合、ルータでは 1 文字ごとに割り込み使用して転送が行われます。
- VTY 回線（Virtual Exec）の場合、Telnet セッションでは 1 文字につき 1 つの TCP パケットを作成する必要があります。

次のリストでは、Exec プロセスで CPU 使用率が高くなる可能性のある理由を詳しく説明しています。

- **コンソール ポートから過剰なデータが送信されている。**show debugging コマンドで、ルータで何らかのデバッグが開始されているかどうかを調べます。**logging console** コマンドの no 形式で、ルータでのコンソール ロギングを無効にします。コンソールに長い出力が表示されているかどうかを確認します。 たとえば、show tech-support コマンドか show memory コマンドを使用します。
- **exec コマンドが非同期回線と補助回線に対して設定されている。**回線に発信トラフィックしかない場合は、この回線の Exec プロセスをディセーブルにします。 この回線に接続されたデバイス（たとえばモデム）から不要なデータが送信された場合に、この回線で Exec プロセスが開始されるのがその理由です。ルータがターミナル サーバとして（他のデバイス コンソールへのリバース Telnet に）使用されている場合、これらの他のデバイスのコンソールに接続されている回線に **no exec** コマンドを設定することが推奨されます。 データはコンソールからもどって来る別の方法で Exec プロセスを開始するかもしれません CPU リソースを使用する。

Virtual Exec で CPU 使用率が高くなる理由には、次のことが考えられます。

- **Telnet セッションで過剰なデータが送信されている。**Virtual Exec プロセスで CPU 使用率が高くなる最も一般的な理由は、ルータから Telnet セッションに過剰なデータが送信されることです。 これが発生する可能性があるのは、**show tech-support** や **show memory** などの出力が長大なコマンドが Telnet セッションで実行される場合です。 各 VTY セッションで転送さ

れるデータの総量は、**show tcp vty <line number>** コマンドで確認できます。

L3 エージング プロセス

L3 エージング プロセスが NetFlow Data Export (NDE) を使用して大量の *ifindex* 値をエクスポートする場合、CPU 使用率は 100 % に達する可能性があります。

この問題が発生する場合は、次の 2 つのコマンドがイネーブルになっているかを確認します。

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

これらのコマンドをイネーブルにする場合は、このプロセスで NDE を使用してすべての宛先と送信元の ifindex 値をエクスポートする必要があります。 L3 エージング プロセスの使用率は、すべての宛先と送信元の *ifindex* 値に対して FIB ルックアップを実行しなければならないために高くなります。 このため、テーブルがいっぱいになり、L3 エージング プロセスのメモリ使用量が増加し、CPU 使用率が 100 % に達します。

この問題を解決するには、次のコマンドをディセーブルにします。

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

値を確認するこれらのコマンドを使用して下さい:

- show mls cef 概略
- show mls cef maximum-routes

BPDU ストーム

スパニング ツリーは、冗長構成のスイッチド ネットワークおよびブリッジ ネットワークにおいてループのないレイヤ 2 環境を維持します。 STP がないと、フレームがループするか、限りなく増殖することになります。 その結果、大量のトラフィックによってブロードキャスト ドメイン内のすべてのデバイスの動作が中断されることになるため、ネットワークのメルトダウンが発生します。

一面では、STP はもともと低速のソフトウェア ベースのブリッジ仕様（IEEE 802.1D）用に開発された初期のプロトコルですが、複雑な構成にすることにより、下記の機能が備わるスイッチングされた大きいネットワークで有効に実装することができます。

- 多数の VLAN
- STP ドメイン内の多数のスイッチ
- マルチベンダーのサポート
- より新しい IEEE 機能拡張

ネットワークでスパニング ツリーの計算が頻繁に発生したり、スイッチでさらに多数の BPDU を処理する必要がある場合、CPU 高使用率が発生したり、BPDU が廃棄される可能性があります。

これらの問題に対応するには、下記の手順のいずれか、またはすべてを実行します。

1. スイッチから VLAN を切り離す。
2. MST のような拡張版の STP を使用する。
3. スイッチのハードウェアをアップグレードする。

さらに、ネットワークでスパニング ツリー プロトコルを実装するベスト プラクティスも参照してください。

- CatOS が稼働する Catalyst 4500/4000、5500/5000 および 6500/6000 シリーズ スイッチの設定と管理のベスト プラクティス
- Cisco IOS が動作している Catalyst 6500/6000 シリーズおよび Catalyst 4500/4000 シリーズ スイッチのベスト プラクティス

SPAN セッション

Catalyst 6000/6500 シリーズ スイッチのアーキテクチャによると、SPAN セッションはスイッチのパフォーマンスに影響しませんが、SPAN セッションに高トラフィック/アップリンク ポートや EtherChannel があると、プロセッサの負荷が増大する可能性があります。 特定の VLAN が 1 つ選出されると、負荷がさらに増大します。 リンク上に不正なトラフィックがあると、負荷がさらに増大する可能性があります。

一部のシナリオでは、RSPAN 機能によりループが発生し、プロセッサの負荷が急激に増大します。 詳細は、「SPAN セッションでブリッジング ループが生成されるのはなぜですか。」を参照してください。

すべてはハードウェアで実行されるので、スイッチでは通常どおりトラフィックを通過させられますが、転送するトラフィックを確認しようとすると CPU に悪影響が出る可能性があります。 SPAN セッションを設定するのは必要な場合だけにすることを推奨いたします。

%CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

TCAM 内の利用可能スペース総量を超過した場合に、このエラー メッセージを受け取ります。 これにより、CPU 高使用率が発生します。 これは FIB TCAM の制限です。 TCAM がいっぱいになると、フラッグがセットされて、FIB TCAM 例外を受け取ることになります。 これにより、TCAM への新規ルートの追加が停止されます。 そのため、すべてソフトウェアでスイッチングされることになります。 ルートを削除しても、ハードウェア スイッチングの再開には無効です。

いったん TCAM が例外ステートに入ってしまうと、このステートから抜けるにはシステムのリロードが必要です。 TCAM にインストールできるルートの最大数は、**mls cef maximum-routes** コマンドで増加されます。

高CPU と動作する Catalyst 6500/6000 に L4 ポートとの IPv6 ACL があります

イネーブル MLS IPv6 ACL 圧縮アドレス ユニキャスト。 このコマンドは IPv6 ACL が L4 プロトコルポート数で一致する場合必要です。 このコマンドが有効に ならない場合、IPv6 トラフィックはソフトウェア処理のための CPU にパントされます。 このコマンドはデフォルトで設定されません。

銅線接続 SPF

Cisco ME 6500 シリーズ イーサネット スイッチでは、銅線接続の SFP は他のタイプの SFP よりもファームウェアの介在がより多く必要で、これにより CPU 使用率が増大します。

銅線接続の SFP を管理するソフトウェア アルゴリズムは、Cisco IOS SXH リリースでは改善されています。

モジュラ IOS

モジュラ IOS ソフトウェアが稼働する Cisco Catalyst 6500 シリーズ スイッチでは、通常の CPU 使用率が非モジュラ IOS ソフトウェアよりも若干高くなります。

モジュラ IOS ソフトウェアでは、パケットごとのコストよりも、アクティビティごとのコストがより多くかかっています。 モジュラ IOS ソフトウェアでは、パケットが多くなくてもプロセスの維持にある程度の CPU が消費されているため、CPU の消費は実際のトラフィックに基づくものではありません。 ところが、処理されるパケットのレートが高まっても、モジュラ IOS ソフトウェアで消費される CPU が非モジュラ IOS ソフトウェアでの消費量を超えることはありません。

CPU 使用率のチェック

CPU 使用率が高い場合は、まず **show processes cpu** コマンドを発行します。 コマンドの出力には、スイッチの CPU 使用率の他に、各プロセスの CPU 使用量も表示されます。

```
Router#show processes cpu CPU utilization for five seconds: 57%/48%; one minute: 56%; five
minutes: 48% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    1
0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager       2          12     18062
0  0.00%  0.00%  0.00%   0 Load Meter          4      164532     13717      11994  0.00%  0.21%
0.17%   0 Check heaps         5           0         1          0  0.00%  0.00%  0.00%   0 Pool
Manager     !--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912
2171455        112  9.25%  8.11%  7.39%   0 SNMP ENGINE       174          68       463
146  0.00%  0.00%  0.00%   0 RPC pm-mp  !--- Output is suppressed.
```

この出力では、CPU の合計使用率は 57 % で、割り込みによる CPU 使用率が 48 % になっています。 上の例では、これらのパーセンテージが太字で示されています。 この割り込みによる CPU 使用率は、CPU によるトラフィックの割り込みスイッチングが原因です。 コマンド出力には、2 つの使用率の違いの原因となったプロセスがリストされています。 この場合、原因は SNMP プロセスです。

CatOS が稼働するスーパーバイザ エンジンでは、出力は次のようになります。

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
```

```
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

この出力では、最初のプロセスは Kernel and Idle で、CPU 使用率がアイドル状態であることを示しています。 他のプロセスが CPU サイクルを使用していない場合は、通常このプロセスの使用率が高くなります。 この例では、SptBpduRx プロセスにより CPU 使用率が高くなっています。

これらのプロセスの 1 つが原因で CPU 使用率が高くなっている場合は、トラブルシューティングを行って、このプロセスの CPU 使用率が高い原因を見極めます。 しかし、CPU 使用率が高い原因が CPU にトラフィックがパントされているためであれば、トラフィックがパントされている理由を見極める必要があります。 このように見極めていけば、どのトラフィックが問題なのかを識別しやすくなります。

トラブルシューティングのために、CPU使用率が高い状態を経験するときスイッチから出力を集めるためにこの EEM スクリプト例を使用して下さい:

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

注 コマンドは CPU がハードウェアの代りにパケットのプロセス スイッチングが高く原因のとき有用です。 それはコマンドが動作するとき CPU に着信 4096 のパケットをキャプチャ します。 コマンドは全く安全で、6500 の高CPU 問題のための最も便利なツールです。 それにより CPU に余分ロードを引き起こしません。

CPU にパントされたトラフィックを判別するユーティリティおよびツール

このセクションでは、パントされたトラフィックを表示するのに便利なユーティリティやツールについて説明します。

Cisco IOS システム ソフトウェア

Cisco IOS ソフトウェアでは、スーパーバイザ エンジンのスイッチ プロセッサは SP と表され、MSFC は RP と表されます。

show interface コマンドにより、インターフェイスの状態に関する基本情報およびインターフェイスのトラフィック レートがわかります。 このコマンドではエラー カウンタも表示されます。

```
Router#show interface gigabitethernet 4/1GigabitEthernet4/1 is up, line protocol is up
(connected)  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
Internet address is 100.100.100.2/24  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255  Encapsulation ARPA, loopback not set  Keepalive
```

```
set (10 sec)  Half-duplex, 100Mb/s  input flow-control is off, output flow-control is off  Clock
mode is auto  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output
hang never  Last clearing of "show interface" counters never  Input queue: 5/75/1/24075
(size/max/drops/flushes); Total output drops: 2  Queueing strategy: fifo  Output queue: 0/40
(size/max)  30 second input rate 7609000 bits/sec, 14859 packets/sec  30 second output rate 0
bits/sec, 0 packets/sec  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast  L3 out Switched:
ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes     2982871 packets input, 190904816 bytes, 0 no
buffer     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles     1 input errors, 1 CRC, 0
frame, 28 overrun, 0 ignored     0 input packets with dribble condition detected     1256
packets output, 124317 bytes, 0 underruns     2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred     0 lost carrier, 0 no carrier     0 output buffer
failures, 0 output buffers swapped out
```

この出力では、着信トラフィックがレイヤ 2 でスイッチングされているのではなく、レイヤ 3 でスイッチングされていることが読み取れます。 これは、トラフィックが CPU にパントされていることを示しています。

show processes cpu コマンドを使用すれば、これらのパケットが通常のトラフィックのパケットか制御パケットかがわかります。

```
Router#show processes cpu | exclude 0.00              CPU utilization for five seconds: 91%/50%;
one minute: 89%; five minutes: 47% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY
Process   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps       98
121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input         245      209336    894828
233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

パケットがプロセス スイッチングされている場合、IP Input プロセスの実行のメモリ使用率が高くなっています。 これらのパケットを表示するには、次のコマンドを実行します。

show buffers input-interface

```
Router#show buffers input-interface gigabitethernet 4/1 packetBuffer information for Small
buffer at 0x437874D4  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280  linktype 7
(IP), enctype 1 (ARPA), encsize 14, rxtype 1  if_input 0x505BC20C (GigabitEthernet4/1),
if_output 0x0 (None)  inputtime 00:00:00.000 (elapsed never)  outputtime 00:00:00.000 (elapsed
never), oqnumber 65535  datagramstart 0x8060F7A, datagramsize 60, maximum size 308  mac_start
0x8060F7A, addr_start 0x8060F7A, info_start 0x0  network_start 0x8060F88, transport_start
0x8060F9C, caller_pc 0x403519B4  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000,
ttl: 63,  TOS: 0 prot: 17, source port 63, destination port 6308060F70:
000A 42D17580            ..BQu.08060F80: 00000000 11110800 4500002E 00000000
........E.......08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?08060FA0:
001A261F 00010203 04050607 08090A0B  ..&.............08060FB0: 0C0D0E0F 101164
......d
```

トラフィックが**割り込みスイッチングされている**場合、**show buffers input-interface** コマンドではそのパケットを表示できません。 割り込みスイッチング用に RP にパントされたパケットを表示するには、Switched Port Analyzer (SPAN; 交換ポートアナライザ) で RP ポートのキャプチャを行います。

注割り込みスイッチングとプロセス交換の CPU 使用率に関する詳細は、次の文書を参照してください。

- 『*Cisco ルータの CPU 使用率が高い場合のトラブルシューティング*』の「CPU 高使用率の原因が割り込みにある場合」セクション

RP インバンドおよび SP インバンドの SPAN

Cisco IOS ソフトウェアの RP または SP ポートに対する SPAN は Cisco IOS ソフトウェア リリ

ース 12.1(19)E 以降で使用可能です。

コマンド構文は次のとおりです。

test monitor session *1-66* **add {rp-inband | sp-inband} [rx | tx | both]**
Cisco IOS ソフトウェア 12.2 SX リリースでは、次の構文を使用します。

test monitor add *{1..66}* **{rp-inband | sp-inband} {rx | tx | both}**
注SXH リリースの場合は、**monitor session** コマンドを使用してローカル SPAN セッションを設定してから、次のコマンドを使用して、その SPAN セッションを CPU に関連付けする必要があります。

source {cpu {rp | sp}} | *single_interface* **|** *interface_list* **|** *interface_range* **|** *mixed_interface_list* **|** *single_vlan* **|** *vlan_list* **|** *vlan_range* **|** *mixed_vlan_list***} [rx | tx | both]**
注これらのコマンドについての詳細は、『*Catalyst 6500 リリース 12.2SX ソフトウェア コンフィギュレーション ガイド*』の「ローカル SPAN の設定 (SPAN コンフィギュレーション モード) 」を参照してください。

次に RP コンソールの例を示します。

```
Router#monitor session 1 source interface fast 3/3!--- Use any interface that is
administratively shut down.Router#monitor session 1 destination interface 3/2
```
ここで SP コンソールに移動します。 次に例を示します。

```
Router-sp#test monitor session 1 add rp-inband rx
```
注Cisco IOS 12.2 SX リリースでは、このコマンドは **test monitor add 1 rp-inband rx** に変更されています。

```
Router#show monitor Session 1---------Type : Local SessionSource Ports :Both : Fa3/3Destination
Ports : Fa3/2SP console:Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1
Egress Source Ports: 3/3 Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans:
<empty>Destination Ports: 3/2
```
注Cisco IOS 12.2 SX リリースでは、このコマンドは **test monitor show 1** に変更されています。

次に SP コンソールの例を示します。

```
Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1 Egress Source Ports: 3/3
Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans: <empty>Destination Ports:
3/2
```
CatOS システム ソフトウェア

CatOS システム ソフトウェアが稼働するスイッチでは、スーパーバイザ エンジンで CatOS が稼働し、MSFC で Cisco IOS ソフトウェアが稼働します。

show mac コマンドを使用すると、MSFC にパントされたフレームの数を確認できます。 ポート 15/1 がスーパーバイザ エンジンから MSFC への接続です。

注

```
Console> (enable) show mac 15/1Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast-
------- -------------------- -------------------- --------------------15/1
193576                    0                   1Port     Xmit-Unicast         Xmit-Multicast
Xmit-Broadcast-------- -------------------- -------------------- --------------------15/1
3                    0                   0Port     Rcv-Octet            Xmit-Octet-------- ----
---------------- --------------------15/1                 18583370                    0MAC
```

```
Dely-Exced MTU-Exced  In-Discard Out-Discard-------- ---------- ---------- ---------- ----------
-15/1              0          -          0           0
```
この数字が急速に増加している場合は、パケットが MSFC にパントされていることを示しており、CPU 高使用率の原因となります。 次に、パケットを次の方法で表示できます。

- MSFC ポート 15/1 または 16/1 に対する SPAN
- sc0 に対する SPAN

MSFC ポート 15/1 または 16/1 に対する SPAN

発信元を MSFC ポート 15/1 (または 16/1)、宛先をイーサネット ポートにした SPAN セッションをセットアップします。

次に例を示します。

```
Console> (enable) set span 15/1 5/10Console> (enable) show spanDestination     : Port 5/10Admin
Source    : Port 15/1Oper Source     : NoneDirection       : transmit/receiveIncoming Packets:
disabledLearning        : enabledMulticast       : enabledFilter          : -Status          :
active
```
ポート 5/10 でスニファ トレースを収集している場合、スニファ トレースに表示されるのは、MSFC で送受信されるパケットです。 MSFC を宛先とするパケットだけをキャプチャして、MSFC から送出されるパケットをキャプチャしないようにするには、SPAN セッションを **tx** で設定します。

sc0 に対する SPAN

スーパーバイザ エンジンの CPU に向かうフレームをキャプチャするには、SPAN セッションを **sc0** インターフェイスで送信元として設定します。

```
Console> (enable) set span ?  disable                    Disable port monitoring  sc0
Set span on interface sc0  <mod/port>                 Source module and port numbers  <vlan>
Source VLAN numbers
```
注オプティカル サービス モジュール (OSM) では、トラフィックの SPAN キャプチャを実行できません。

推奨事項

スーパーバイザ エンジンの CPU 使用率は、スイッチのハードウェア転送能力を反映していません。 それでも、スーパーバイザ エンジンの CPU 使用率のベースライン値を取得して、監視する必要があります。

1. 通常のトラフィック パターンおよび負荷が発生している安定した状態のネットワークで、スイッチのスーパーバイザ エンジンの CPU 使用率のベースライン値を取得します。どのプロセスの CPU 使用率が最も高いかに注意してください。
2. CPU 使用率をトラブルシューティングする際には、次の質問点を考慮します。どのプロセスの使用率が最も高いか。 これらのプロセスは、ベースライン値とは異なっているか。 CPU は常にベースライン値よりも高い使用率になっているか。 それとも、ときどき高使用率が瞬間的に発生して、ベースラインのレベルに戻るのか。Topology Change Notification (TCN; トポロジ変更通知) がネットワークにあるか。**注**フラッピング ポートまたは STP PortFast が無効になっているホスト ポートがあれば、TCN が発生します。管理サブネットまたは VLAN に過剰なブロードキャストまたはマルチキャストのトラフィックがあ

るか。スイッチに SNMP ポーリングなどの管理トラフィックが過剰にあるか。

3. 高い CPUタイムの間に（CPU が 75% のまたはそれ以上にとき）、これらのコマンドから出力を集めて下さい:show clockshow versionソートされる show processes cpushow proc cpu 履歴show log
4. できれば、ユーザ データ トラフィックのある VLAN、特にブロードキャスト トラフィックの多い VLAN から管理 VLAN を切り離します。このタイプのトラフィックの例としては、IPX RIP/Service Advertising Protocol（SAP）、AppleTalk およびその他のブロードキャスト トラフィックなどがあります。 そのようなトラフィックは、スーパーバイザ エンジンの CPU 使用率に影響を与える可能性があり、極端な場合は、スイッチの正常な動作を妨げる可能性もあります。
5. RP にトラフィックがパントされているために CPU 使用率が高くなっている場合は、どのトラフィックがなぜパントされているのかを判別します。この判別を行うには、「CPU にパントされたトラフィックを判別するユーティリティおよびツール」セクションで説明されているユーティリティを使用します。

関連情報

- Sup720 で Catalyst 6500's の高CPU のトラブルシューティングための役に立つコマンド
- 「Common CatOS Error Messages on Catalyst 6000/6500 Series Switches（Catalyst 6000 および 6500 シリーズ スイッチでの一般的な CatOS エラー メッセージ）」
- Cisco IOS ソフトウェアが稼働する Catalyst 6500/6000 シリーズ スイッチでの一般的なエラー メッセージ
- Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 シリーズ スイッチのハードウェアと一般的な問題のトラブルシューティング
- スイッチド キャンパス ネットワークにおけるユニキャスト フラッディング
- 製品サポート：Cisco Catalyst 6500 シリーズ スイッチ
- 断続的な高CPU 問題の間のデータを収集するための EEM スクリプト
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems