Cisco 7600 トラブルシューティング ガイド

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルでは、Cisco 7600 ルータのトラブルシューティングについて説明します。

内容

このマニュアルの内容は、次のとおりです。

マニュアルの変更履歴

リビジョン	日付	変更点
OL-28248-01-J	2012 年 11 月	最初のバージョン

Cisco 7600 での問題のトラブルシューティング

ここでは、問題の考えられる原因と解決策について説明し、問題をトラブルシューティングできるようにします。

隔離された BFD のフラップ

問題：2 台のルータ間の障害をできる限り早く検出するために、双方向フォワーディング検出（BFD）が実装されています。ログには、キープアライブ信号の損失に起因する問題が BFD で検出されたことが示されています。しかし、リンクのどちら側でもパケットのドロップは見られず、リンク上でエラーも発生していません。また、他のプロトコルのフラップもありません。

考えられる原因：Cisco 7600 ルータでは、BFD がスーパーバイザに実装されているので、プラットフォーム内部でのキープアライブ メッセージの遅延が原因となって BFD フラップが発生することがあります。

解決策：

- CPU 使用率が高いと、BFD のキープアライブ メッセージが遅延する可能性があります。CPU が使用不能にならないようにするには、**process-max-time 50** コマンドまたは **hw-module rp process-max-time 50** コマンドを使用します。これにより、活発な BFD タイマーが原因で CPU が使用不能になることがありません。また、これらのコマンドによって、プロセスの最長実行時間がデフォルトの 200 ミリ秒から 50 ミリ秒に短くなります。
- タイマーを極端な値に設定しないでください。推奨の最小値に設定するには、**bfd interval 100 min_rx 100 multiplier 3** コマンドを使用します。
- BFD セッションをラインカードにオフロードします（ES+ の場合のみ）。これにより、処理がスーパーバイザからラインカードに移動します。詳細については、次のリンクを参照してください。
  http://www.cisco.com/en/US/docs/routers/7600/install_config/ES40_config_guide/es40_chap4.html#wp1720514
  また、ラインカードの CPU 使用率が高い場合は、最大処理時間を短縮します。**hw-module slot ‘x’ process-max-time 50** コマンドを使用します。
- DFC ではないカードに属するインターフェイスで設定した BFD セッションでは、他のラインカードの物理的な活性挿抜（OIR）をルータで実行したときにフラップが発生することがあります。この原因は、物理的な活性挿抜の際にバックプレーン バス上で発生する短時間のバス停止です。DFC ではないカードのインターフェイスでは、BFD タイマーを 999 という大きい値に設定することをお勧めします。

上記のトラブルシューティングで解決しない場合は、シスコの Technical Assistance Center（TAC）または High Touch Technical Support（HTTS）でケースを開いてください。

プロセッサでの過剰な CPU 使用率

問題：パントされたトラフィックが高いレートで発生することに起因して、ルート プロセッサ（RP）またはスイッチ プロセッサ（SP）の CPU 使用率が高くなります。

考えられる原因：RP および SP は主にコントロール プレーン パケットに使用しますが、ポリシー フィーチャ カード（PFC）および分散フォワーディング カード（DFC）では特定用途向け集積回路（ASIC）のレベルで転送するパケット転送を扱います。このことから、プロセッサの CPU 使用率は低い値にとどまります。プロセッサによる使用率が高い場合（50% を超える場合）は、この点を確認する必要があります。CPU 使用率が高くなる原因として、PFC または DFC によって高いレートでプロセッサにトラフィックがパントされていることが最も多く考えられます。

解決策：

まず、トラフィックの送信元を特定します。詳細は、以下の URL にあるガイドを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a00804916e0.shtml

プロセッサに送信される入力パケットをキャプチャするには、以下のオプションを使用します。パケットのキャプチャはプロセッサで実行されるわけではないので、CPU の使用率が 100% でも、これらのオプションを使用できます。

オプション A：Netdr ツールを使用します。

- このツールでは、プロセッサに直接接続しているシステム コントローラ ASIC 上でパケット ヘッダーをキャプチャします。これは、パケットがプロセッサに到達する前の位置に置かれた最後の ASIC です。このツールでは、最大 4096 個のパケットをキャプチャします。
- **debug netdr capture rx** コマンドを使用します。**show netdr capture** コマンドを使用して、このパケットを表示できます。同様に、SP については、**remote command switch debug netdr capture rx** コマンドを使用してパケットをキャプチャします。キャプチャしたパケットを表示するには、**remote command switch show netdr capture** コマンドを使用します。TAC または HTTS でケースを開いて、詳細な分析ができるように、これらのコマンドの出力を送信します。

オプション B：RP または SP のインバンド モニタリング セッションを使用します。

- RP または SP の SPAN セッションはオプションです。トラフィックは複製され、ネットワーク アナライザまたはスニファを接続したポートから送信されます。
- まず、管理上はシャットダウンしている任意の送信元インターフェイスを使用してモニタリング セッションを設定します。宛先インターフェイスは、外部アナライザに接続したインターフェイスです。

  monitor session *session_number* **source interface** *interface*
  monitor session *session_number* **destination interface** *interface*

- 次に、SP コンソールから次の設定を適用します（SP コンソールにアクセスするには、**remote login switch** コマンドを使用します）。

  test monitor session *session_number* **add rp-inband rx** <-- RP の SPAN をイネーブル化

  test monitor session *session_number* **add sp-inband rx** <-- SP の SPAN をイネーブル化

CPU 使用率の上昇を防止するために 7600 ルータに用意されているさまざまな方法については、次の URL にあるガイドを参照してください。

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#9

http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/dos.html

VLAN インターフェイスの表示インターフェイス上の不正確なレート カウンタまたは値のないレート カウンタ

問題：すべてのレイヤ 2 スイッチド トラフィックに対しては、スイッチ仮想インターフェイス（SVI）のレート カウンタの値がゼロであることが **show int vlan** コマンドの出力に示されます。レイヤ 3 スイッチド トラフィックに対しては、SVI のレート カウンタの値が **show int vlan** コマンドの出力に誤って示されます。

考えられる原因：**show int vlan x** コマンドでレートを表示する場合、定義上はそのレートの計算にレイヤ 2 スイッチド パケットが考慮されません。したがって、レイヤ 2 スイッチド パケットに対してはレート カウンタはゼロのままです。

レイヤ 3 トラフィックの場合、SVI のレート カウンタはさまざまなラインカードを受信元としていますが、それらから受信する値はキャッシュされたものであり、リアル タイムの値ではないことから、カウンタの値が正しくないことがあります。実際の値に比べて、レート カウンタの値が低くなる場合もあれば、高くなる場合もあります。

解決策：これは、プラットフォームによる制限であり、ソフトウェアで対応できる解決策はありません。入力および出力のパケット カウンタは正確です。また、物理ポートのカウンタは、ラインカードから受信するリアルタイム カウンタなので正確です。インターフェイス カウンタは、ラインカードからスーパーバイザに定期的に送信されます。多くの場合、その送信間隔は約 10 秒です。これも、正しくないレートが報告される原因となることがあります。

正しくないペイロード CRC によるパケットのドロップ

問題：MPLS を設定した SIP-400 または Enhanced Felxwan で、次のエラー メッセージが表示されます。

エラー メッセージ　`%HYPERION-5-HYP_INTR_INFO: HY_FD_PP_EC_EC_ERR_INT[0x1] bad payload CRC exceeds threshold.`

このエラー メッセージは、正しくないペイロード巡回冗長検査（CRC）によってパケットのドロップが発生していることを示しています。

考えられる原因：Hyperion ASIC が書き換えの前後で MPLS パケットの CRC を計算する方法に原因があると考えられます。エラーが検出されると、パケットのドロップが発生します。この誤計算は、ES20 ラインカードでも同様に発生することがあります。ES20 の場合は、ラインカードがクラッシュします。

解決策：**mls mpls recir-agg** コマンドを使用します。トラフィック エンジニアリング用としてマルチキャスト VPN またはポイントツーポイント GRE トンネルを設定している場合は、**mls mpls tunnel-recir** コマンドを使用します。

スイッチング バスがアイドル状態であることを示すエラー メッセージ

問題：スイッチング バスがアイドル状態であることを示すエラー メッセージが PFC で表示されます。スーパーバイザでは、PFC について次のエラー メッセージが表示されます。

エラー メッセージ `%EARL-2-SWITCH_BUS_IDLE: Switching bus is idle for two seconds.`

ラインカードでは、DFC について次のエラー メッセージが表示されます。

エラー メッセージ `%EARL-DFC2-2-SWITCH_BUS_IDLE: Switching bus is idle for five seconds. The card grant is 0.`

考えられる原因：EARL（スーパーバイザ上の PFC）によって EARL バスにパケットが送信されているかどうかが、タイマーで定期的に確認されています。ルータ上にある DFC ごとに同様のタイマーが存在します。PFC では 2 秒以内、DFC では 5 秒以内に、EARL がパケットをスイッチングしていない場合は、このエラー メッセージが出力されます。ルータでアイドル状態のバスが検出されると、プラットフォームの回復メカニズムが呼び出されます。

解決策：ラインカードの活性挿抜（OIR）でこのエラーが表示されることがあります。カードの差し込み動作が速すぎる場合や遅すぎる場合に、このエラーが発生することがあります。活性挿抜でこのエラーが表示されない場合は、ハードウェアに問題があります。ライン カードを接続し直す必要があります。これで問題が解決しない場合は、ラインカードの交換が必要です。次のコマンドの出力を収集し、TAC または HTTS に送信します。

- **show platform software module 'x' swbus idle info** <-- エラーが発生するモジュール
- **show platform software earl reset data**
- **show platform software earl reset history**
- **show tech-support**

SPI での相互接続または VPLS の不具合

問題：SPI での相互接続または VPLS が動作しません。

考えられる原因：

ハードウェア要件が満たされていないと、SVI での相互接続もバーチャル プライベート LAN サービス（VPLS）も当初から動作しません。リンク フラップ後に、VPLS や SVI での相互接続が動作しなくなることもあります。

解決策：

SVI での相互接続や VPLS を設定する場合は、次の制限が適用されるかどうかを確認します。

- ES20 の 10 ギガバイト インターフェイス上のコア側 SVI では VPLS VC がアクティブになりません。
- 2.48 Gbps を超えると、SVI の集約ポリサーには相互接続を設定できません。
- コア側ラインカードには、SIP-400、SIP-600、ES20 または ES+ のいずれかのラインカードを使用する必要があります。

モジュラまたは Generic Online Diagnostic の障害

問題：モジュラの障害または Generic Online Diagnostic の障害

考えられる原因：Generic Online Diagnostic（GOLD）の障害は、モジュール、占有スロット、スーパーバイザ、またはシャーシ自体に問題があることを示しています。頻度は低いものの、ソフトウェアの不具合が原因で GOLD の障害が発生することもあります。

（注） GOLD によるテストの詳細は、次を参照してください。
http://www.cisco.com/en/US/docs/routers/7600/ios/15S/configuration/guide/diagtest.html

解決策：

1. **hw-module module X reset** コマンドを使用してモジュールをリロードします。
2. モジュールを取り付け直します。

（注） 新品のモジュールをシャーシに取り付けている場合は、モジュールを取り外し、バックプレーンのピンが曲がっていないことを確認します。

3. デュアル スーパーバイザの場合は、スーパーバイザのスイッチオーバーを実行します。
4. シャーシにある別のスロットにモジュールを移動します。
5. モジュールを別のシャーシに取り付けてみます。

接続性の問題

問題：接続性の問題

考えられる原因：物理的な問題、キュー ウェッジ、または設定の間違いが原因で、接続性の問題が発生することがあります。

解決策：

1. 一般的な健全性チェックを実行します。
   a. 該当のインターフェイスがアップ状態かどうかを確認します。
   b. 該当のラインカードのステータスが OK かどうかを確認します。
   c. ログにエラー メッセージが記録されているかどうかを確認します。
2. ARP の設定が両方のデバイスで正しいかどうかを確認します。
3. パケット スニファまたは **debug netdr cap rx** コマンドを使用して、パケット フローが影響を受ける方向を確認します。

   たとえば、次のように入力します。

   A - > B（A から B の方向で ICMP エコー要求のドロップが発生）

   A < - B（B から A の方向で ICMP エコー応答のドロップが発生）
4. パケット スニファまたは **show counter interface** コマンドのカウンタを使用して、出力方向または入力方向のどちらでパケットにドロップが発生しているかを確認します。
5. 問題のあるインターフェイスを特定したところで、エラー カウンタを確認します。

パケット損失

問題：パケット損失

考えられる原因：パケット損失は、ルータの両端間で基本的な双方向の接続が確認されることです。多くのパケットから、一定数のパケットが失われます。エンド デバイス間の接続には、複数の中間デバイスが介在していることがあるので、パケット損失が発生しているデバイスの特定が困難になります。

解決策：

1. パケット パスのトポロジを作成します。
2. パケット損失に明らかなパターンがあるかどうかを確認します。
3. パケット スニファまたは **debug netdr cap rx** コマンドを使用して、パケット損失が影響を受ける方向を確認します。

   たとえば、次のように入力します。

   A - > B（A から B の方向で ICMP エコー要求のドロップが発生）

   A < - B（B から A の方向で ICMP エコー応答のドロップが発生）
4. パケット損失が発生するデバイスを特定します。これはパケット スニファを使用して検出できます。
5. 該当のデバイスでパケット スニファまたは **show counter interface** コマンドのカウンタを使用して、出力方向または入力方向のどちらでパケットにドロップが発生しているかを確認します。
6. 問題のあるインターフェイスを特定したところで、エラー カウンタを確認します。

入力のドロップ

問題：入力のドロップ

考えられる原因：入力ではオーバーランが原因でドロップが発生する可能性があります。オーバーランとは、インターフェイス ASIC がバッファを使い切った状況です。オーバーランは、ハードウェアでスイッチングされたパケットの損失です。通常、これは、複数の入力インターフェイスが同じ出力インターフェイスにトラフィックを送信したときに、出力ラインカードのオーバーサブスクリプションが原因となって発生します。別の原因として、ネットワーク トラフィックの急激な増加も多く見られます。

解決策：

1. **TestFabricFlowControlStatus** コマンドを使用します。
2. **diagnostic monitor module test** コマンドを使用します。

   ```
   sup720_04(config)# diagnostic monitor module 5 test 33
   ```
3. モニタ間隔を 100 ミリ秒に設定します。

   ```
   diagnostic monitor interval module 5 test 33 00:00:00 100 0
   ```
4. **show diagnostic event** コマンドを使用して、フロー制御が機能していることを確認します。

   次に出力例を示します。

   ```
   RateReduction: 12/0, [fpoe:7], Fab->LC = R0%/CU0%  /PU73%, LC->Fab = R100%/CU0%/PU61%,
   SP CPU = 23%
   ```
   R0% であれば、フロー制御が全面的に機能しています。

   R100% であれば、フロー制御は機能していません。

   FAB->LC はフロー制御の方向を示します。ここでは、ファブリックのフローでラインカードを制御しているので、ラインカードからこれ以上のトラフィックをファブリックに送信することはできません。

（注） 出力のオーバーサブスクライブでは、過負荷になった出力ラインカードのフローでファブリックを制御しています。その結果、ファブリックのフローで入力ラインカードを制御することになり、それによって入力インターフェイスでオーバーランが発生します。フロー制御の方向を確認できれば、トラフィックの一部を代替パスにリルートするか、帯域幅を引き上げることでこの問題を解決できます。

関連資料

Cisco 7600 シリーズ ルータの関連資料は、次のとおりです。

- 『*Cisco 7600 Series Router Installation Guide*』
- 『*Cisco 7600 Series Router Module Installation Guide*』
- *Cisco 7600 Series Router SIP, SSC, and SPA Hardware Installation Guide*
- *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*
- 『*Cisco 7600 Series Router Cisco IOS Command Reference*』
- 『*Cisco 7600 Series Internet Router System Message Guide*』
- 『*Release Notes for Cisco IOS Release 12.2SRA on the Cisco 7600 Series Routers*』
- 『Cisco IOS Configuration Guides and Command References』: Cisco 7600 シリーズ ルータのマニュアルで扱っていない Cisco IOS ソフトウェア機能を設定する場合には、次の資料を参照してください。
  - 『*Configuration Fundamentals Configuration Guide*』
  - 『*Configuration Fundamentals Command Reference*』
  - 『*Bridging and IBM Networking Configuration Guide*』
  - 『*Bridging and IBM Networking Command Reference*』
  - 『*Interface Configuration Guide*』
  - 『*Interface Command Reference*』
  - 『*Network Protocols Configuration Guide*』*Part 1*、*2*、*3*
  - 『*Network Protocols Command Reference*』*Part 1*、*2*、*3*
  - 『*Security Configuration Guide*』
  - 『*Security Command Reference*』
  - 『*Switching Services Configuration Guide*』
  - 『*Switching Services Command Reference*』
  - 『*Voice, Video, and Home Applications Configuration Guide*』
  - 『*Voice, Video, and Home Applications Command Reference*』
  - 『*Software Command Summary*』
  - 『*Software System Error Messages*』
  - 『*Debug Command Reference*』
  - 『*Internetwork Design Guide*』
  - 『*Internetwork Troubleshooting Guide*』
  - 『*Configuration Builder Getting Started Guide*』

  Cisco IOS コンフィギュレーション ガイドは次の URL にあります。

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
- 管理情報ベースについては、次の URL を参照してください。

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版のすべての技術マニュアルの一覧が示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/