CHAPTER 31

# ファブリックのトラブルシューティング

この章では、スイッチの問題を解決するために使用する基本的なトラブルシューティング方法について説明します。この章の内容は、次のとおりです。

# トラブルシューティングのツールおよび技術

シスコ スイッチの監視およびトラブルシューティングには、複数の技術およびツールを使用できます。これらのツールは完全な統合型マルチレベル分析ソリューションを提供します。

**Fabric Manager Server —** Cisco Fabric Manager Server は、ストレージ ネットワーク パフォーマンスに関する長期の詳細情報を提供します。ファブリック全体のパフォーマンス傾向を分析するには、Performance Manager を使用します。これは、ネットワークのホットスポットを解決するための、より詳細な分析の開始ポイントになります。

**Device Manager —** Fabric Manager Server によってパフォーマンスの問題が検出された場合には、Cisco Device Manager を使用して、ポート単位の統計情報をリアルタイムで表示できます。プロトコルの詳細、エラー数、廃棄数、バイト数、およびフレーム数が表示されます。サンプリングは 2 秒おきに実行でき、値はテキスト形式、または円グラフ、棒グラフ、面グラフ、折れ線グラフで表示できます。

**Traffic Analyzer —** Fabric Manager Server からファイバ チャネル用 Cisco Traffic Analyzer を起動して、トラフィックを詳細に分析することもできます。Cisco Traffic Analyzer を使用すると、VSAN（仮想 SAN）およびプロトコル別にトラフィックを分類して、Logical Unit Number（LUN）レベルで SCSI トラフィックを調べることができます。

**Protocol Analyzer —** より詳細な調査が必要な場合は、Cisco Traffic Analyzer のコンテキスト内でファイバ チャネル用 Cisco Protocol Analyzer を起動することができます。Cisco Protocol Analyzer を使用すると、ファイバ チャネルおよび Wireshark 用にシスコ社が開発した SCSI デコーダを使用して、ファイバ チャネル フレームの実際のシーケンスを容易に調査できます。

**Port Analyzer Adapter（PAA）—** Fabric Manager Server および Device Manager は SNMP（簡易ネットワーク管理プロトコル）を使用して統計情報を収集します。内蔵のスイッチ統計情報カウンタがすべて活用されます。

Cisco Traffic Analyzer と Cisco Protocol Analyzer を統合すると、ファイバ チャネル トラフィックそのものを分析でき、スイッチ分析機能が拡張されます。シスコの Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）は、他の機能に影響しない柔軟な技術によってこれらのソリューションを実現し、1 つまたは複数のポートからファブリック内の別のスイッチ ポートに、選択的にトラフィックをミラーリングできます。

Cisco PAA は、SPAN トラフィックをイーサネット ヘッダーにカプセル化し、分析できるように PC またはワークステーションに転送します。SPAN を使用した場合は、ファイバ チャネルの制御トラフィックおよびデータ プレーン トラフィックを使用できます。イーサネット パケットは PAA によってブロードキャストされるので、IP ネットワーク間ではルーティングできません。ハブおよびスイッチは、同じイーサネット サブネット内にある場合に使用できます。PAA と PC 間の直接接続もサポートされています。PAA ではファイバ チャネル データが切り捨てられるため、イーサネット トラフィックを削減できます。

Cisco Traffic Analyzer および Cisco Protocol Analyzer では、SPAN トラフィックを PC またはワークステーションにトランスポートするために PAA が必要です。

**（注）** Cisco Traffic Analyzer は Cisco PAA 2 と組み合わせた場合に最適に機能します。これは、切り捨てられたデータ長が Cisco PAA 2 によって提供され、正確なバイト数の報告が可能になるためです。

## Cisco Traffic Analyzer

ファイバ チャネル用 Cisco Traffic Analyzer は SPAN トラフィック、または Cisco Protocol Analyzer を使用してキャプチャされたトラフィックのリアルタイム分析を実行します。複数の Cisco PAA からのファイバ チャネル トラフィックを集約して、Cisco Traffic Analyzer で分析できます。

1 つの SPAN 宛先ポートに送信できる SPAN 発信元数には制限があります。集約により、Cisco Traffic Analyzer が統合レポート セットで分析可能な情報量が拡張されます。

（注）　集約機能は、単一 PC とのイーサネット接続によって収集される情報に限定されます。複数の PC 間で集約することはできません。

Cisco Traffic Analyzer は Web サーバを介してレポートを表示するため、レポートはローカルまたはリモートで表示できます。トラフィック分析機能は「ntop」オープンソース ソフトウェアによって提供されます。このソフトウェアは、ファイバ チャネルと SCSI の分析、および拡張された SPAN 用 ISL（スイッチ間リンク）ヘッダー サポートを追加するためにシスコが拡張した機能です。ntop は Cisco.com ソフトウェア ダウンロード センターの Cisco Port Analyzer Adapter から入手できます。また、インターネット（http://www.ntop.org/ntop.html）から入手することもできます。シスコの拡張 ntop は、Microsoft Windows および Linux の各オペレーティング システムで稼働します。

ファイバ チャネル用 Cisco Traffic Analyzer は、ネットワーク全体の統計情報に関するレポートを表示します。Summary Traffic レポートには、フレーム サイズ範囲ごとのトラフィックの割合が表示されます。トラフィックの割合は、SCSI、ELS などのプロトコルごとに分類されます。分析中の SPAN トラフィックの平均スループットおよびピーク スループットも表示されます。

Cisco Traffic Analyzer を使用すると、VSAN 単位でファイバ チャネル トラフィックを分析できます。Domain Traffic Distribution グラフは、特定の VSAN のスイッチで送受信されたトラフィック量（バイト）を示します。FC Traffic Matrix グラフは、ファイバ チャネルの発信元と宛先の間で送受信されたトラフィック量を示します。VSAN ごとの合計バイト数およびフレーム数も表示されます。

ホストおよびストレージ ポートごとに統計情報を分析できます。SCSI 読み取りトラフィックと書き込みトラフィックの割合、SCSI トラフィックとその他のトラフィックの割合、および送信バイト / フレームと受信バイト / フレームの割合を表示できます。各ポートで送受信されたデータのピークおよび平均スループット値を表示できます。

## Cisco Protocol Analyzer

ファイバ チャネル用 Cisco Protocol Analyzer を使用すると、ファイバ チャネル トラフィック フレームをリアルタイムで表示したり、またはキャプチャ ファイルから取り込んで表示することができます。ファイバ チャネルおよび SCSI デコーダにより、トラフィックをフレーム レベルで表示および分析できます。完全にデコードするために応答と要求が比較され、ナビゲーションが大幅に簡単になります。応答とステータス間の応答時間が表示されます。

Cisco Protocol Analyzer は VSAN を認識するため、VSAN をキャプチャおよびディスプレイ フィルタの基準として使用することができます。カラムに VSAN 番号も表示できます。プロトコル配信割合や、特定のファイバ チャネル発信元と宛先ペア間で転送される合計バイトまたはフレーム数に関するサマリー統計情報を表示できます。ファイル キャプチャおよびフィルタリング制御も実行できます。キャプチャされたファイルは、Cisco Protocol Analyzer または Cisco Traffic Analyzer で分析できます。

操作が簡単な多数の機能が追加されています。特定の基準を満たすフレームを検索して、マークを付けることができます。フレーム（パケット）リストのエントリを色分けして、目的の項目を強調したり、必要に応じてカラムを追加または削除することができます。

プロトコル分析機能は Wireshark オープンソース ソフトウェアによって提供されます。このソフトウェアは、ファイバ チャネルおよび SCSI プロトコルをデコードしたり、SPAN 用の拡張 ISL ヘッダーをサポートしたりするために、シスコによって拡張されたものです。Wireshark は Cisco.com ソフトウェア ダウンロード センターの Cisco Port Analyzer Adapter から入手できます。Wireshark はインターネット（http://www.wireshark.org）から入手することもできます。Wireshark は Microsoft Windows、Solaris、および Linux の各オペレーティング システムで稼働します。

# スイッチ デバイス状態の分析

Switch Health オプションを使用すると、特定のスイッチのコンポーネント ステータスを判別できます。

Fabric Manager でスイッチ ヘルス オプションを使用して特定のスイッチのコンポーネント ステータスを判断する手順は、次のとおりです。

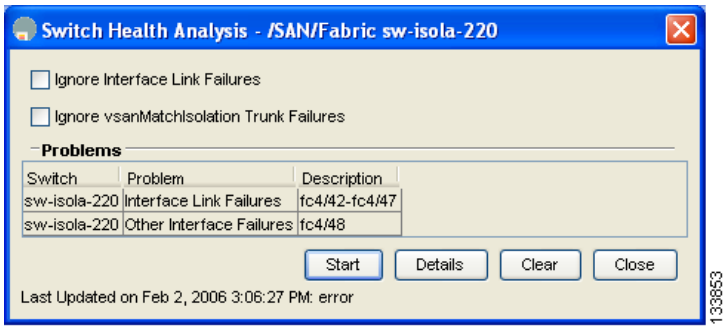
**ステップ 1**　**Tools > Switch Health** を選択します。

Switch Health Analysis ウィンドウが表示されます。

**ステップ 2**　**Start** をクリックして、選択したスイッチに現在影響を与えている問題を調べます。

Switch Health Analysis ウィンドウに問題が表示されます（図 31-1 を参照）。

**図 31-1　Switch Health Analysis の結果**




**ステップ 3**　**Clear** をクリックして、Switch Health Analysis ウィンドウの内容を削除します。

**ステップ 4**　**Close** をクリックして、ウィンドウを閉じます。

# スイッチ ファブリック設定の分析

Fabric Configuration オプションを使用すると、現在の設定を特定のスイッチまたはポリシー ファイルと比較して、スイッチの設定を分析することができます。スイッチの設定をファイルに保存し、ファイル内の設定とすべてのスイッチを比較することができます。

Fabric Manger で Fabric Configuration オプションを使用してスイッチの設定を分析する手順は、次のとおりです。

**ステップ 1**　**Tools > Fabric Configuration** を選択します。

Fabric Configuration Analysis ダイアログボックスが表示されます。

**ステップ 2**　選択したスイッチを別のスイッチと比較するか、またはポリシー ファイルと比較するかを決定します。

- スイッチと比較する場合は、**Policy Switch** をオンにし、ドロップダウン矢印を選択して、スイッチのリストを表示します。
- ポリシーと比較する場合は、**Policy File** を選択します。このオプションの右にある **...** ボタンをクリックして、ファイル システムをブラウズし、ポリシー ファイル（*.XML）を選択します。

**ステップ 3**　**Rules** をクリックして、Fabric Configuration Analysis ツールを実行する場合に適用する規則を設定します。

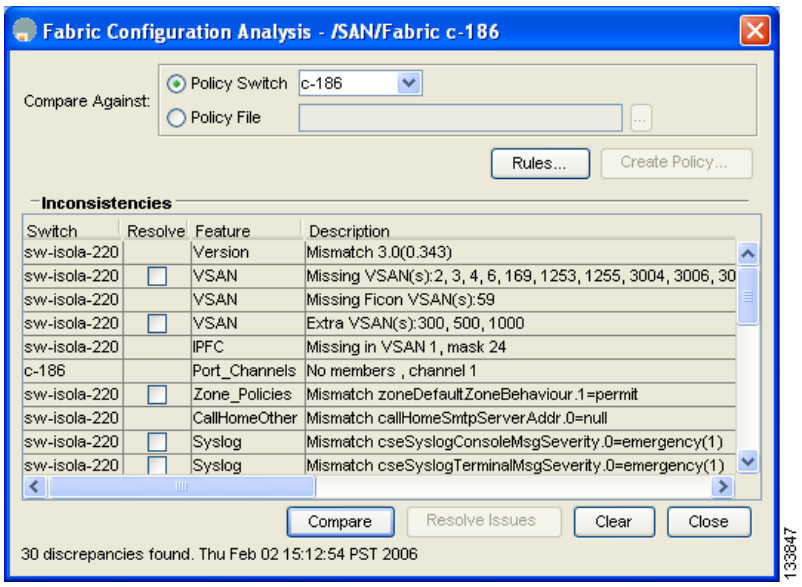
Rules ウィンドウが表示されます。

**ステップ 4**　必要に応じて規則を変更し、**OK** をクリックします。

**ステップ 5**　**Compare** をクリックします。

設定が分析され、比較によって検出された問題点が表示されます（図 31-2 を参照）。

**図 31-2　Fabric Configuration Analysis の結果**



**ステップ 6**　解決する問題点に対応する Resolve カラムのチェックボックスをオンにします。

**ステップ 7**　この問題を解決するには、**Resolve Issues** をクリックします。

**ステップ 8**　**Clear** をクリックして、ウィンドウの内容を削除します。

**ステップ 9**　**Close** をクリックして、ウィンドウを閉じます。

# エンドツーエンド接続の分析

End to End Connectivity オプションを使用すると、スイッチ ファブリック内のデバイス間の接続およびルートを判別できます。接続ツールは ping テストを使用し、エンド デバイスの各ペアが同じ VSAN 内または同じアクティブ ゾーン内にあるかを調べて、各ペアが相互に通信可能かどうかをチェックします。このオプションは、ファイバ チャネル ネットワーク用に変更された ping および traceroute コマンドのバージョンを使用します。

Fabric Manager で End to End Connectivity オプションを使用して接続およびルートを判別する手順は、次のとおりです。

**ステップ 1**　**Tools > End to End Connectivity** を選択します。

End to End Connectivity Analysis ダイアログボックスが表示されます。

**ステップ 2**　接続を確認する VSAN を VSAN ドロップダウン リストから選択します。

**ステップ 3**　分析対象をすべてのアクティブ ゾーンにするか、またはデフォルト ゾーンにするかを選択します。

**ステップ 4**　**Ensure that members can communicate** をクリックして、選択されたエンド ポイント間のファイバ チャネルに ping を実行します。

**ステップ 5**　パケット数、各パケットのサイズ、およびタイムアウト（ミリ秒）を識別します。

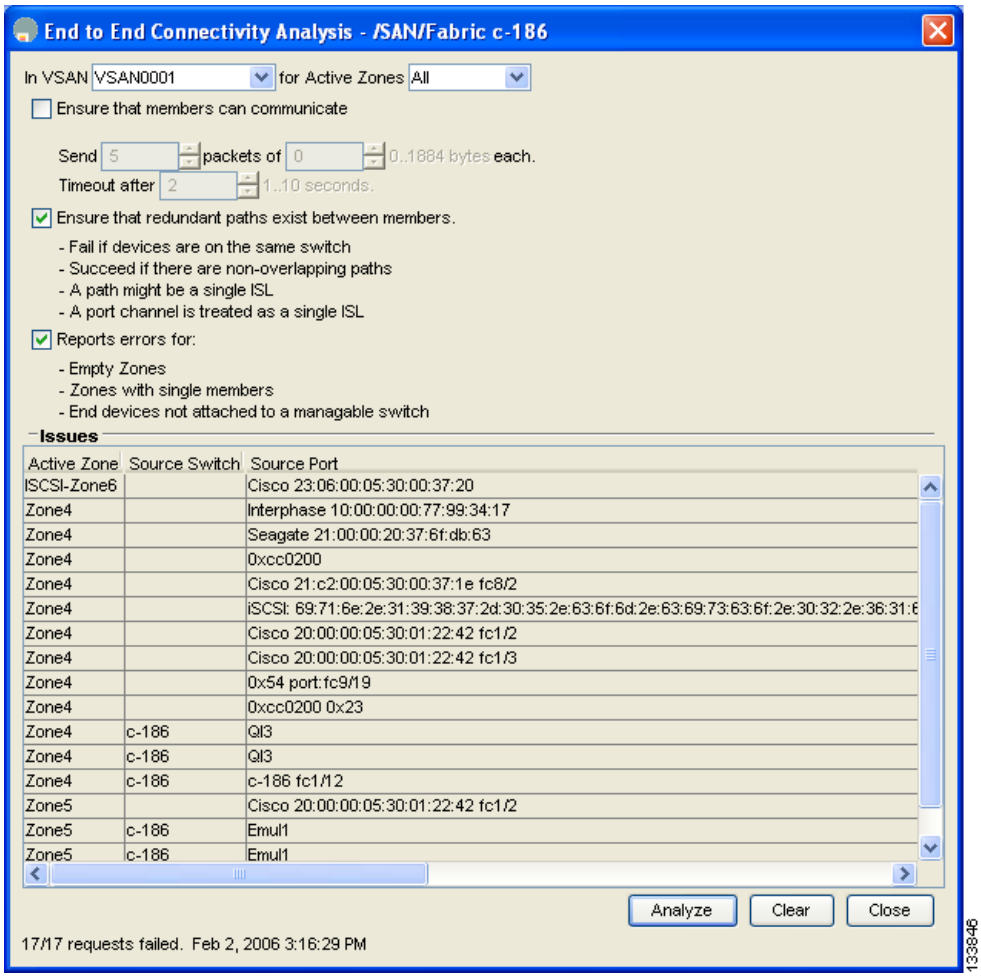
**ステップ 6**　**Ensure that redundant paths exist between members** チェックボックスをオンにして、エンドポイント間の冗長パスを分析します。

**ステップ 7**　**Report errors for** チェックボックスをオンにして、ゾーンおよびデバイス エラーのレポートを表示します。

**ステップ 8**　**Analyze** をクリックします。

End to End Connectivity Analysis ウィンドウに、選択されたエンド ポイントが接続先スイッチおよび接続に使用されている発信元および宛先ポートとともに表示されます。図 31-3 を参照してください。

**図 31-3　End to End Connectivity Analysis の結果**




出力には、失敗したすべての要求が表示されます。

- Ignoring empty zone — 空のゾーンには要求が発行されません。
- Ignoring zone with single member — メンバーが 1 つしかないゾーンには要求が発行されません。
- Source/Target are unknown — ポートに対応するネーム サーバが存在しないか、または検出中にポートが検出されませんでした。
- Both devices are on the same switch — 同一スイッチ上に両方のデバイスがあります。
- No paths exist between the two devices — 2 つのデバイス間にはパスが存在しません。
- VSAN does not have an active zone set and the default zone is denied — VSAN 上にアクティブ ゾーン セットがなく、デフォルトのゾーンが拒否されます。
- Average time micro secs — 遅延値が、指定されたしきい値を超過しました。

**ステップ 9**　**Clear** をクリックして、ウィンドウの内容を削除します。

**ステップ 10**　**Close** をクリックして、ウィンドウを閉じます。

# ping ツールの使い方（fcping）

ping ツールを使用すると、別のスイッチから使用しているスイッチ上のポートの接続を確認できます。

Fabric Manager で ping ツールを使用して接続を確認する手順は、次のとおりです。

**ステップ 1**　**Tools > Ping** を選択します。

Fabric ペインでホストおよびストレージ デバイスを右クリックし、コンテキスト メニューから選択することもできます。

Ping ダイアログボックスが表示されます。

**ステップ 2**　Source Switch ドロップダウン リストで発信元スイッチを選択します。

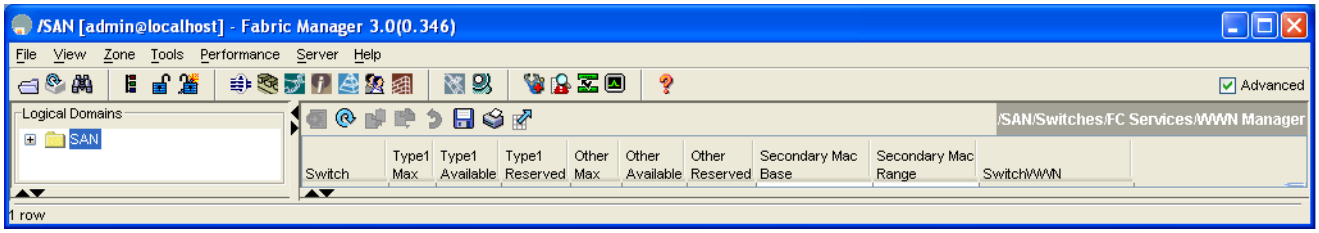
**ステップ 3**　VSAN ドロップダウン リストで、接続を確認する VSAN を選択します。

**ステップ 4**　Target Endport ドロップダウン リストで、接続を確認するターゲット エンド ポートを選択します。

**ステップ 5**　**Start** をクリックして、スイッチと選択したポート間に ping を実行します。

Ping Results ダイアログボックスが表示されます（図 31-4 を参照）。

**図 31-4　ping の結果**




**ステップ 6**　**Clear** をクリックしてウィンドウの内容をクリアし、新しい ping を実行します。または **Close** をクリックしてウィンドウを閉じます。

# Trace Route（fctrace）などのトラブルシューティング ツールの使い方

Fabric Manager Tools メニューで次のオプションを使用すると、選択されたオブジェクトとの接続を確認したり、その他の管理ツールを開くことができます。

- Trace Route — Fabric ペインで現在選択されている 2 つのエンド デバイス間の接続を確認します。
- Device Manager — Fabric ペインで選択されたスイッチごとに Device Manager を起動します。
- Command Line Interface — Fabric ペインで選択されたスイッチとの Telnet または Secure Shell（SSH; セキュア シェル）セッションを開きます。

Fabric Manager で Trace Route オプションを使用して接続を確認する手順は、次のとおりです。

**ステップ 1**　**Tools > Trace Route** を選択します。

Trace Route ダイアログボックスが表示されます。

**ステップ 2**　Source Switch ドロップダウン リストで発信元スイッチを選択します。

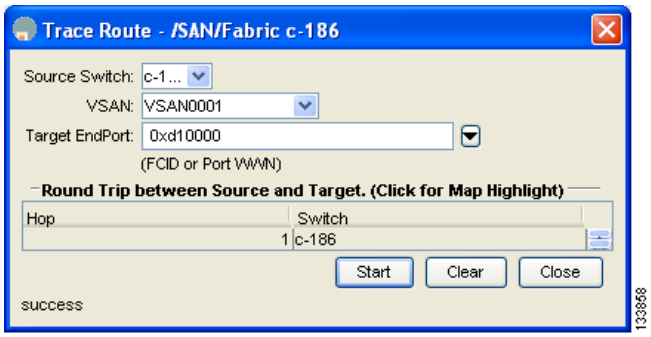
**ステップ 3**　VSAN ドロップダウン リストで、接続を確認する VSAN を選択します。

**ステップ 4**　Target Endport ドロップダウン リストで、接続を確認するターゲット エンド ポートを選択します。

**ステップ 5**　**Start** をクリックして、スイッチと選択したポート間の traceroute を実行します。

ダイアログボックスの下部に結果が表示されます（図 31-5 を参照）。

**図 31-5　正しいトレース ルートの結果**




**ステップ 6**　**Clear** をクリックしてウィンドウの内容をクリアし、新しい traceroute を実行します。または **Close** をクリックしてウィンドウを閉じます。

# ゾーン マージ結果の分析

Zone メニューの Zone Merge オプションを使用すると、接続された 2 つのスイッチのゾーン設定に互換性があるかどうかを判別できます。

Fabric Manager で Zone Merge オプションを使用してゾーン設定に互換性があるかどうかを判別する手順は、次のとおりです。

**ステップ 1**　**Zone > Merge Analysis** を選択します。

Zone Merge Analysis ダイアログボックスが表示されます。

**ステップ 2**　各ドロップダウン リストでスイッチを選択します。

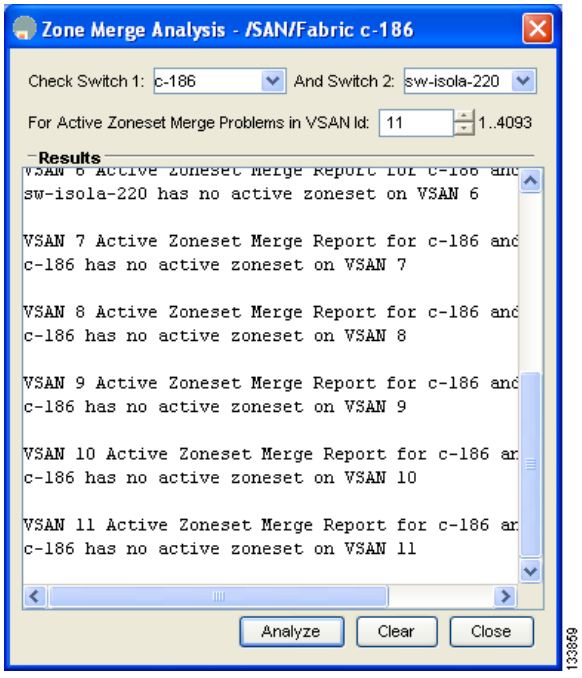
**ステップ 3**　ゾーン マージ分析を実行する VSAN を選択します。

**ステップ 4**　必要に応じてステップ 3 を繰り返します。

**ステップ 5**　**Analyze** をクリックします。

Zone Merge Analysis ウィンドウに、選択された 2 つのスイッチのゾーン設定に関する不整合が表示されます。図 31-6 を参照してください。

**図 31-6　Zone Merge Analysis の結果**




**ステップ 6**　**Clear** をクリックして、ウィンドウの内容を削除します。

**ステップ 7**　**Close** をクリックして、ウィンドウを閉じます。

# show tech support コマンドの使用

**show tech support** コマンドは、ご使用のスイッチに関する大量の情報を収集してトラブルシューティングを行う場合に便利です。この出力は、テクニカル サポート担当者に問題を報告する場合に提供できます。

Fabric Manager では、ファブリック内の 1 つまたは複数のスイッチに対して **show tech support** コマンドを入力できます。各コマンドの結果は、指定したディレクトリ内のテキスト ファイル（各スイッチに 1 つずつ）に書き込まれます。これらのファイルを表示するには、Fabric Manager を使用します。

Fabric Manager マップを JPG ファイルとして保存することもできます。ファイルはシード スイッチの名前で保存されます（172.22.94.250.jpg など）。

すべてのファイル（**show tech support** コマンドの出力およびマップ ファイル イメージ）を zip ファイルに圧縮し、zip ファイルをテクニカル サポートに送信できます。

Fabric Manager で **show tech support** コマンドを入力する手順は、次のとおりです。

**ステップ 1**　**Tools > Show Tech Support** を選択します。

Show Tech Support ダイアログボックスが表示されます。

**ステップ 2**　各スイッチのチェックボックスをオンにして、テクニカル サポート情報を表示するスイッチを選択します。

**ステップ 3**　タイムアウト値を設定します。

デフォルトは 30 秒です。

**ステップ 4**　テキスト ファイル（**show tech support** コマンド情報を含む）を書き込むフォルダを選択します。

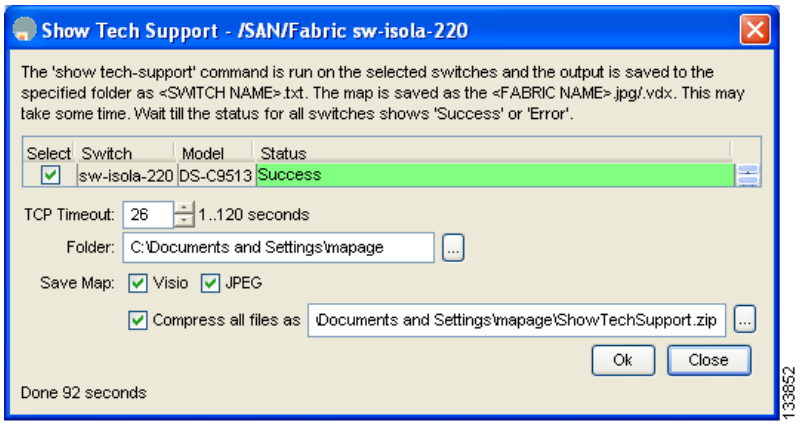
**ステップ 5**　マップのスクリーンショットを JPG ファイルとして保存する場合は、**Save Map** チェックボックスをオンにします。

**ステップ 6**　ファイルを zip ファイルに圧縮するには、**Compress all files as** チェックボックスをオンにします。

**ステップ 7**　指定したスイッチで **show tech support** コマンドを開始するには、**OK** をクリックします。**show tech support** コマンドを使用しないで Show Tech Support ダイアログボックスを閉じるには、**Close** ボタンをクリックします（図 31-7 を参照）。

各スイッチの横にある Status カラム内に、ステータスがハイライト表示されます。イエローのハイライト表示は、このスイッチ上で **show tech support** コマンドが現在実行中であることを示します。レッドのハイライト表示は、エラーを示します。図 31-7 に示すようなグリーンのハイライト表示は、**show tech support** コマンドが正常に終了したことを示します。

**図 31-7　show tech support コマンドの正しい結果**




**ステップ 8**　プロンプトが表示されたら、該当するスイッチのフィールドにユーザ名とパスワードを入力します。

**（注）**　Fabric Manager からスイッチに **show tech support** コマンドを正常に入力するには、スイッチにこのユーザ名およびパスワードを設定する必要があります。Fabric Manager はこのユーザ名およびパスワードが設定されていないスイッチにはログインできず、エラーが戻されます。

**（注）**　Fabric Manager を使用しないで **show tech support** ファイルを表示する場合は、任意のテキスト エディタでファイルを開くことができます。各ファイルには、スイッチの IP アドレスと .TXT 拡張子の名前が付いています（111.22.33.444.txt など）。

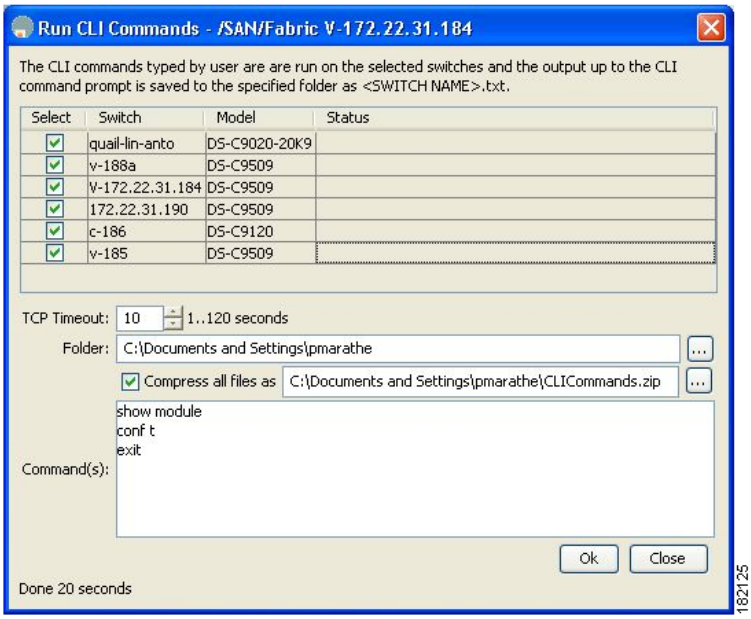
# CLI コマンドの実行

Run CLI コマンド機能を使用して、複数のスイッチで CLI（コマンドラインインターフェイス）コマンドを実行できます。Fabric Manager を使用して CLI コマンドを実行する手順は、次のとおりです。

**ステップ 1**　**Tools > Run CLI Commands** を選択します。

すべてのスイッチが選択された Run CLI Commands ダイアログボックスが表示されます（図 31-8 を参照）。

**図 31-8　Run CLI Commands ダイアログボックス**




**ステップ 2**　CLI コマンドを実行しない場合は、スイッチのチェックボックスをオフにします。

**ステップ 3**　ファイルの保存場所を指定します。

（注）　スイッチごとにレポートが発行されます。レポートを見て、CLI コマンド エラー実行されていないことを確認します。

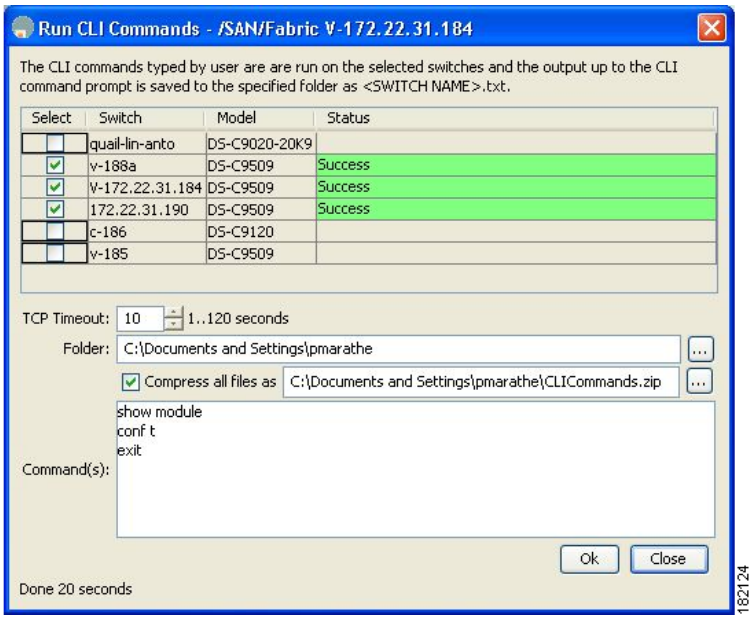
**ステップ 4**　Commands(s) テキスト ボックスにコマンドを入力します。入力するコマンドがコンフィギュレーションモード コマンドであれば、**exit** コマンドも入力します。

（注）　実行コマンドは、コンフィギュレーションモードでは指定できません。

**ステップ 5**　**OK** をクリックして CLI コマンドを実行します。

各スイッチのステータスを示す Run CLI コマンド ダイアログボックスが表示されます（図 31-9 を参照）。

**図 31-9　Run CLI Commands ステータス**




**ステップ 6**　**Close** をクリックして、ダイアログボックスを閉じます。

## 夏時間の調整

（注）　2007 年の米国夏時間は 3 月の第 2 日曜から始まり、11 月の第 1 日曜に終わります。

Fabric Manager の Run CLI コマンド機能を使用して、スイッチの時刻変更設定を行います。Command(s) テキスト ボックスに次のコマンドを入力します。

```
configure
no clock summer-time
clock summer-time daylight_timezone_name 2 Sunday March 02:00 1 Sunday November 02:00
60
```

# その他のスイッチの検索

Locate Switches オプションは SNMPv2 を使用し、読み取り専用コミュニティ ストリング public を指定して、SNMP 要求に応答するデバイスを検出します。この機能を使用できるのは、次の場合です。

- 管理 IP アドレスを提供する FC-GS3 FCS 標準が実装されていないサードパーティ製スイッチが含まれている場合
- サブネット内のその他のシスコ スイッチを検出する必要があるにもかかわらず、ファブリックに物理的に接続されていない場合

Fabric Manager を使用して現在検出されているファブリックに含まれないスイッチを検出する手順は、次のとおりです。

**ステップ 1**　**File > Locate Switches and Devices** を選択します。

Locate Switches ダイアログボックスが表示されます。

**ステップ 2**　Comma Separated Subnets フィールドに特定のサブネットに属す特定のアドレス範囲を入力して、スイッチの検索範囲を制限します。

サブネット 192.168.199.0 に属すシスコ スイッチを検索するには、次のストリングを使用します。

**192.168.100.[1-254]**

カンマで区切って、複数の範囲を指定できます。たとえば、2 つのサブネット 192.168.199.0 および 192.169.100.0 内のすべてのデバイスを検索するには、次のストリングを使用します。

**192.168.100.[1-254], 192.169.100.[1-254]**

**ステップ 3**　Read Community フィールドに適切な読み取りコミュニティ ストリングを入力します。

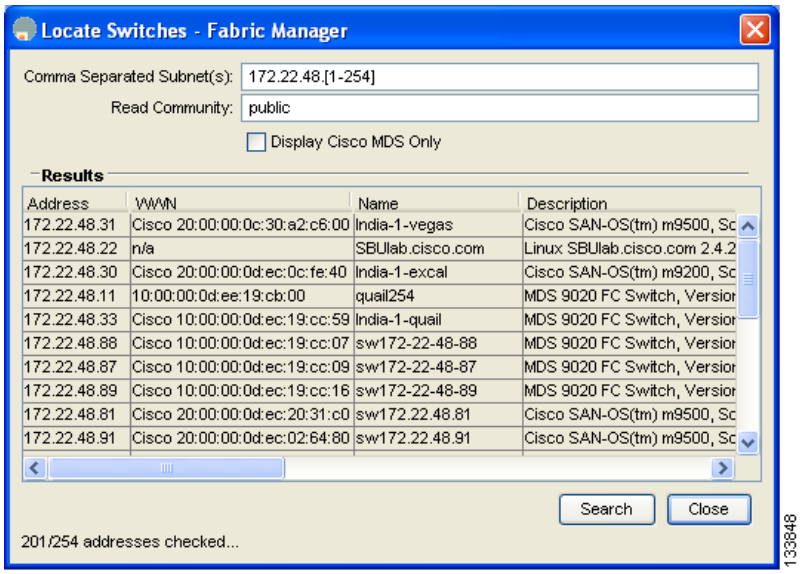
このストリングのデフォルト値は **public** です。

**ステップ 4**　**Display Cisco Nexus 5000 family Only** をクリックして、ネットワーク ファブリック内の Nexus 5000 シリーズ スイッチだけを表示します。

**ステップ 5**　**Search** をクリックして、ネットワーク ファブリック内のスイッチおよびデバイスを検出します。

Locate Switches ウィンドウに検出結果が表示されます（図 31-10 を参照）。

**図 31-10　スイッチおよびデバイスの検索結果**




**（注）**　デバイス ロケータがネットワーク ファブリック内のデバイス検出を試みるごとに、画面左下にある数字が増加します。検出プロセスが完了した場合、この数字は表示行数を示します。

**ステップ 6**　**Close** をクリックして、ダイアログボックスを閉じます。

# ファイバ チャネルの TOV

ファイバ チャネル プロトコルに関連するスイッチのタイマー値を変更するには、次の Timeout Value（TOV）を設定します。

- Distributed Services TOV（D_S_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 5,000 ミリ秒です。
- Error Detect TOV（E_D_TOV）— 有効範囲は 1,000 ～ 10,000 ミリ秒です。デフォルトは 2,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。
- Resource Allocation TOV（R_A_TOV）— 有効範囲は 5,000 ～ 10,000 ミリ秒です。デフォルトは 10,000 ミリ秒です。この値は、ポート初期化中に他端と比較されます。

**（注）** Fabric Stability TOV（F_S_TOV）定数は設定できません。

**注意** D_S_TOV、E_D_TOV、および R_A_ TOV 値は、スイッチ内のすべての VSAN を一時停止するしないかぎり、グローバルに変更できません。

Fabric Manager を使用してタイムアウトを設定する手順は、次のとおりです。

**ステップ 1**　Logical Domains ペインで **SAN** を選択して、すべての VSAN を含めます。

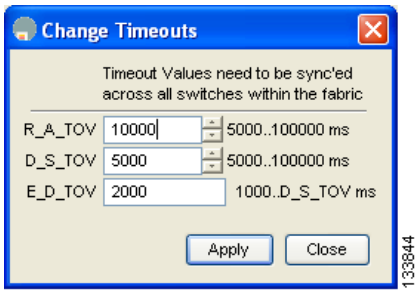
**ステップ 2**　Physical Attributes ペインで **Switches** を展開して **FC Services** を展開し、**Timers & Policies** を選択します。

Information ペインにスイッチのタイマーが表示されます。

**ステップ 3**　**Change Timeouts** をクリックして、タイムアウト値を設定します。

Change Timeouts ダイアログボックスが表示されます（図 31-11 を参照）。

**図 31-11　Change Timeouts ダイアログボックス**




**ステップ 4**　R_A_TOV（Resource Allocation Timeout Value）、D_S_TOV（Distributed Services Timeout Value）、E_D_TOV（Error Detect Timeout Value）の値を表示します。

**ステップ 5**　**Apply** をクリックします。

**ステップ 6**　**Close** をクリックして、ダイアログボックスを閉じます。

---

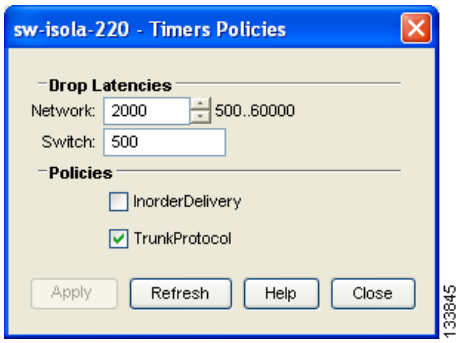
Device Manager でタイマー ポリシーを設定する手順は、次のとおりです。

---

**ステップ 1**　**FC** > **Advanced** > **Timers/Policies** を選択します。

ダイアログボックスに単一スイッチのタイマー ポリシーが表示されます（図 31-12 を参照）。

**図 31-12　Device Manager のタイマー ポリシー設定**




**ステップ 2**　ドロップダウン リストからネットワークを選択し、スイッチを指定します。

**ステップ 3**　**InOrderDeliver** および **Trunk Protocol** またはどちらかのチェックボックスをオンにします。

**ステップ 4**　**Apply** をクリックします。

**ステップ 5**　**Close** をクリックして、ダイアログボックスを閉じます。

---

## VSAN ごとのタイマー設定

VSAN を指定して fctimer を発行し、VSAN に異なる TOV を設定して FC や IP トンネルなどに特別にリンクさせることができます。個別の VSAN に、異なる E_D_TOV、R_A_TOV、D_S_TOV 値を設定できます。タイマー値が変更されると、アクティブな VSAN は一時停止してアクティブになります。

**注意**　以前のバージョンでは VSAN ごとの FC タイマーをサポートしておらず、中断のないダウングレードは実行できません。

**（注）**　この設定はファブリックのすべてのスイッチに伝播する必要があります。ファブリックのすべてのスイッチが同じ値に設定されていることを確認してください。

Fabric Manager を使用して VSAN ごとの FC タイマーを設定する手順は、次のとおりです。

**ステップ 1**　Logical Domains ペインで、タイマーを設定する VSAN を選択します。

ポリシー選択時に VSAN を指定しない場合、変更された値はスイッチのすべての VSAN に適用されます。

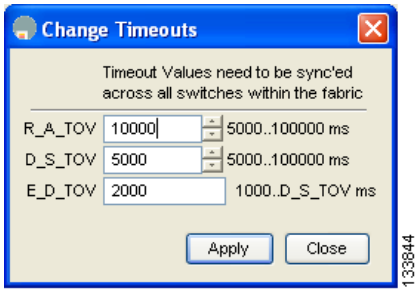
**ステップ 2**　Physical Attributes ツリーで **Switches** を展開して **FC Services** を展開し、**Timers & Policies** を選択します。

Information ペインに、選択した VSAN のスイッチのタイムアウトだけが表示されます。

**ステップ 3**　**Change Timeouts** をクリックして、タイムアウト値を設定します。

Change Timeouts ダイアログボックスが表示されます（図 31-13 を参照）。

**図 31-13　Fabric Manager で VSAN ごとに変更するタイムアウト**




**ステップ 4**　図 31-13 に示すように、タイムアウト値を変更します。

**ステップ 5**　R_A_TOV（Resource Allocation Timeout Value）、D_S_TOV（Distributed Services Timeout Value）、E_D_TOV（Error Detect Timeout Value）の値を表示します。

**ステップ 6**　**Apply** をクリックします。

**ステップ 7**　**Close** をクリックして、ダイアログボックスを閉じます。

# ファブリック アナライザの設定

ファイバ チャネル プロトコル アナライザは、リンク上でフレームおよび順序付きセットをキャプチャし、デコードして、分析します。既存のファイバ チャネル アナライザは、ワイヤ スピードでトラフィックをキャプチャできます。これらは高価であり、フレームのデコードに対するサポートは制限されています。また、既存のアナライザはトラフィックのスヌーピング時に、リンク上のトラフィックを中断させます。

Cisco Fabric Analyzer を使用すると、ユーザは接続を中断したり、分析箇所にローカルに接続することなく、スイッチからファイバ チャネル制御トラフィックをキャプチャして、デコードすることができます。

シスコのファイバ チャネル プロトコル アナライザは、次の 2 つの一般的なパブリックドメイン ソフトウェア アプリケーションに基づいています。

- libpcap — http://www.tcpdump.org を参照
- Wireshark — http://www.wireshark.com を参照

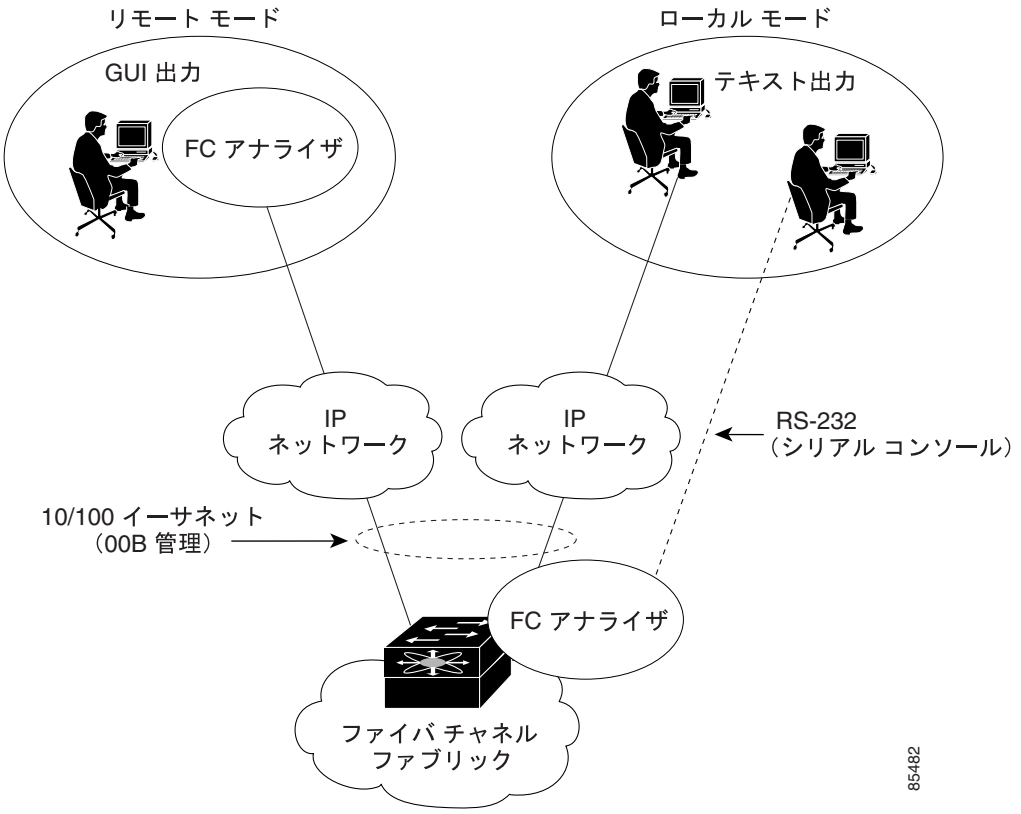
（注）　Cisco Fabric Analyzer は、データ トラフィックでなく、制御トラフィックのキャプチャおよびデコードに役立ちます。制御パスのキャプチャに最適であり、高速データ パスのキャプチャを想定してはいません。

## Cisco Fabric Analyzer の概要

Cisco Fabric Analyzer は 2 つの異なるコンポーネントで構成されます（図 31-14 を参照）。

- ソフトウェア — Cisco Nexus 5000 シリーズ スイッチで稼働し、2 つのキャプチャ モードをサポートします。
  - テキストベース アナライザ — ローカル キャプチャをサポートし、キャプチャされたフレームをデコードします。
  - デーモン — リモート キャプチャをサポートします。
- GUI ベース クライアント — Windows や Linux など、libpcap をサポートするホスト上で稼働し、Cisco Nexus 5000 シリーズ スイッチのリモート キャプチャ デーモンと通信します。

**図 31-14　Cisco Fabric Analyzer の使用法**




## ローカル テキストベース キャプチャ

このコンポーネントは、Cisco Nexus 5000 シリーズ スイッチのスーパーバイザ モジュールに送受信されるトラフィックをキャプチャする、コマンドライン駆動のテキストベース インターフェイスです。このデコーダには完全な機能性があり、迅速にデバッグする場合や、リモート キャプチャ デーモンがイネーブルでないときに使用する場合に役に立ちます。また、このツールは Cisco Nexus 5000 シリーズ スイッチからアクセスされるため、スイッチごとにアクセスを制限する役割ベース ポリシーによって保護されています。

## リモート キャプチャ デーモン

このデーモンはリモート キャプチャ コンポーネントのサーバ側にあります。ホストで稼働する Wireshark アナライザはクライアント側にあります。これらは Remote Capture Protocol（RPCAP）を使用して相互に通信します。RPCAP は、TCP ベースの制御接続、および TCP（デフォルト）または UDP に基づく TCP ベースまたは UDP ベースのデータ接続の 2 つのエンドポイントを使用します。制御接続はキャプチャをリモート制御する場合に使用します（キャプチャの開始や停止、またはキャプチャ フィルタの指定）。リモート キャプチャを実行できるのは、明示的に設定されたホストに対してのみです。この技術の利用により、ネットワーク内の不正なマシンがネットワーク内の制御トラフィックをスヌーピングするのを防ぎます。

RPCAP はファイアウォールの制限に基づいて、2 つの設定接続モードをサポートします。

- パッシブ モード（デフォルト）— 設定されたホストがスイッチとの接続を開始します。複数のホストをパッシブ モードに設定したり、複数のホストを接続して、同時にリモート キャプチャを受信できます。
- アクティブ モード — スイッチが、設定されたホストとの通信を（一度に 1 つずつ）開始します。

キャプチャ フィルタを使用すると、クライアントに実際に送信されるトラフィック量を制限できます。キャプチャ フィルタはスイッチでなく、Wireshark のクライアント側で指定されます。

### GUI ベース クライアント

Wireshark ソフトウェアは、PC やワークステーションなどのホスト上で稼働し、リモート キャプチャ デーモンと通信します。このソフトウェアは、http://www.wireshark.org のパブリック ドメインから入手できます。Wireshark GUI フロントエンドはカラー表示、フィルタ定義中のグラフィックによる支援、および特定のフレームの検索など、豊富なインターフェイスをサポートします。これらの機能については、Wireshark の Web サイトを参照してください。

Wireshark によるリモート キャプチャが、Cisco Nexus 5000 シリーズ スイッチからのファイバ チャネル フレームのキャプチャおよびデコードをサポートしている場合、Wireshark が稼働するホストをスイッチにファイバ チャネル接続する必要はありません。スイッチで稼働するリモート キャプチャ デーモンは、帯域外イーサネット管理ポートを介して、キャプチャされたフレームを送信します。この機能を使用すると、デスクトップまたはラップトップからファイバ チャネル フレームをキャプチャし、デコードできます。

## Cisco Fabric Analyzer の設定

Cisco Fabric Analyzer は、2 つのキャプチャのいずれかを実行するように設定できます。

- ローカル キャプチャ — ローカル キャプチャは、永続ストレージに保存したりスタンバイに同期することはできません。ローカル キャプチャはファブリック アナライザのテキスト バージョンを、コンソール画面から直接起動します。キャプチャはローカル ファイル システムにも保存できます。
- リモート キャプチャ — リモート キャプチャは永続ストレージに保存できます。また、必要に応じてスタンバイ スーパーバイザ モジュールと同期化したり、ステートレス再起動を発行できます。

Cisco Fabric Analyzer 機能を使用するには、トラフィックがスーパーバイザ モジュールを通過している必要があります。

## リモート IP アドレスへのキャプチャの送信

**注意**　スーパーバイザ モジュール上で制御トラフィックをキャプチャするには、eth2 インターフェイスを使用する必要があります。

リモート トラフィックをキャプチャするには、次のいずれかのオプションを使用します。

- キャプチャ インターフェイスは、Wireshark でリモート デバイスとして指定できます。

  ```
  rpcap://<ipaddress or switch hostname>/eth2
  ```

  たとえば、

  ```
  rpcap://cp-16/eth2
  rpcap://17.2.1.1/eth2
  ```

- キャプチャ インターフェイスは、キャプチャ ダイアログボックス内で指定するか、または Wireshark の起動時にコマンドラインに -i オプションを使用して指定します。

  ```
  wireshark -i rpcap://<ipaddress|hostname>[:<port>]/<interface>
  ```

  たとえば、

  ```
  wireshark -i rpcap://172.22.1.1/eth2
  ```

  または

  ```
  wireshark -i rpcap://customer-switch.customer.com/eth2
  ```

**（注）**　たとえば、Windows 2000 で設定する場合は、デスクトップの［**スタート**］をクリックし、［**ファイル名を指定して実行 ...**］を選択します。続いて、ファイル名を指定して実行ウィンドウの名前フィールドに必要なコマンドライン オプションを入力します。

## キャプチャされたフレームの表示

ディスプレイ フィルタ機能を使用することにより、キャプチャされたフレームを選択的に表示できます。たとえば、キャプチャされたすべてのフレームでなく、Exchange Link Protocol（ELP）要求フレームだけを表示できます。この機能はキャプチャされたフレームの表示だけを制限します。キャプチャされたフレーム、または保存されたフレームには影響しません。ディスプレイ フィルタを指定、使用、および保存する手順については、Wireshark Web サイト（http://www.wireshark.org）を参照してください。

次に、この機能の使用方法を示します。

- 指定された VSAN 内のすべてのパケットを表示するには、次の式を使用します。

  ```
  mdshdr.vsan == 2
  ```

- すべての SW_ILS フレームを表示するには、次の式を使用します。

  ```
  fcswils
  ```

- クラス F フレームを表示するには、次の式を使用します。

  ```
  mdshdr.sof == SOFf
  ```

- すべての FSPF フレームを表示するには、次の式を使用します。
  ```
  swils.opcode == HLO || swils.opcode == LSU || swils.opcode == LSA
  ```
- すべての FLOGI フレームを表示するには、次の式を使用します。
  ```
  fcels.opcode == FLOGI
  ```
- VSAN 1 内のすべての FLOGI フレームを表示するには、次の式を使用します。
  ```
  fcels.opcode == FLOGI && mdshdr.vsan == 2
  ```
- すべてのネーム サーバ フレームを表示するには、次の式を使用します。
  ```
  dNS
  ```

## ディスプレイ フィルタの定義

ディスプレイ フィルタで制限されるのは表示可能なフレームであり、キャプチャ対象のフレームではありません（任意の view コマンドと同様）。表示するフィルタは、GUI アプリケーションを使用して、複数の方法で定義できます。

- 自動定義
- 手動定義
- 支援付きの手動定義
- ローカル キャプチャにおける手動のみの定義
- 支援なし

定義に関係なく、各フィルタを保存し、名前で識別する必要があります。

（注）　GUI 支援機能は Wireshark の一部です。詳細については、http://www.wireshark.org を参照してください。

## キャプチャ フィルタ

リモート キャプチャ中にキャプチャ フィルタ機能を使用すると、キャプチャするフレームを制限できます。この機能は、キャプチャされて、リモート スイッチからホストに送信されるフレームを制限します。たとえば、クラス F フレームだけをキャプチャできます。キャプチャ フィルタは、リモート キャプチャで消費される帯域幅を制限する場合に便利です。

ディスプレイ フィルタと異なり、キャプチャ フィルタではキャプチャ対象が、指定されたフレームに限定されます。完全に新しいキャプチャを指定しないかぎり、他のフレームは表示されません。

キャプチャ フィルタの構文は、ディスプレイ フィルタの構文と異なります。キャプチャ フィルタは、libpcap フリーウェアと併用される Berkeley Packet Filter（BPF）ライブラリを使用します。有効なすべてのファイバ チャネル キャプチャ フィルタ フィールドのリストについては以降で説明します。

キャプチャ フィルタの設定手順については、Wireshark Web サイト（http://www.wireshark.org）を参照してください。

次に、この機能の使用方法を示します。

- 指定された VSAN のフレームだけをキャプチャするには、次の式を使用します。
  ```
  vsan = 1
  ```

- クラス F フレームだけをキャプチャするには、次の式を使用します。
  `class_f`
- クラス ファイバ チャネル ELS フレームだけをキャプチャするには、次の式を使用します。
  `els`
- ネームサーバ フレームだけをキャプチャするには、次の式を使用します。
  `dns`
- SCSI コマンド フレームだけをキャプチャするには、次の式を使用します。
  `fcp_cmd`

（注）　この機能は libpcap の一部です。詳細については、http://www.tcpdump.org を参照してください。

## 使用可能なキャプチャ フィルタ

ここでは、使用可能なキャプチャ フィルタを示します。

```
o vsan
o src_port_idx
o dst_port_idx
o sof
o r_ctl
o d_id
o s_id
o type
o seq_id
o seq_cnt
o ox_id
o rx_id
o els
o swils
o fcp_cmd   (FCP Command frames only)
o fcp_data (FCP data frames only)
o fcp_rsp   (FCP response frames only)
o class_f
o bad_fc
o els_cmd
o swils_cmd
o fcp_lun
o fcp_task_mgmt
o fcp_scsi_cmd
o fcp_status
o gs_type      (Generic Services type)
o gs_subtype   (Generic Services subtype)
o gs_cmd
o gs_reason
o gs_reason_expl
o dns   (name server)
o udns (unzoned name server)
o fcs   (fabric configuration server)
o zs    (zone server)
o fc    (use as fc[x:y] where x is offset and y is length to compare)
o els   (use as els[x:y] similar to fc)
o swils (use as swils[x:y] similar to fc)
o fcp   (use as fcp[x:y] similar to fc)
o fcct (use as fcct[x:y] similar to fc)
```

# WWN の設定

スイッチの WWN は、イーサネット MAC（メディア アクセス制御）アドレスと同等です。MAC アドレスと同様に、デバイスごとに WWN を一意に対応付ける必要があります。主要スイッチを選択するとき、およびドメイン ID を割り当てるときは、WWN を使用します。WWN は、スイッチのスーパーバイザ モジュールのプロセスレベル マネージャである WWN マネージャによって、各スイッチに割り当てられます。

Cisco Nexus 5000 シリーズ スイッチは、3 つの Network Address Authority（NAA）アドレス フォーマットをサポートします（表 31-1 を参照）。

**表 31-1　NAA WWN の標準フォーマット**

| NAA アドレス | NAA タイプ | WWN フォーマット | |
|---|---|---|---|
| IEEE 48 ビット アドレス | タイプ 1 = 0001b | 000 0000 0000b | 48 ビット MAC アドレス |
| IEEE 拡張 | タイプ 2 = 0010b | ローカルに割り当て | 48 ビット MAC アドレス |
| IEEE 登録 | タイプ 5 = 0101b | IEEE 企業 ID：24 ビット | VSID：36 ビット |

**注意**　WWN の変更は、管理者や、スイッチの動作に精通した担当者が実行してください。

## リンク初期化 WWN の使用法

ELP および Exchange Fabric Protocol（EFP）は、リンク初期化中に WWN を使用します。使用方法の詳細は、Cisco SAN-OS ソフトウェア リリースごとに異なります。

ELP と EFP のどちらも、リンク初期化中にデフォルトで VSAN WWN を使用します。ただし、ELP の使用方法はピア スイッチの使用方法に応じて変わります。

- ピア スイッチの ELP が sWWN を使用する場合、ローカル スイッチも sWWN を使用します。
- ピア スイッチの ELP が VSAN WWN を使用する場合、ローカル スイッチも VSAN WWN を使用します。

# セカンダリ MAC アドレスの設定

セカンダリ MAC アドレスを割り当てる手順は、次のとおりです。

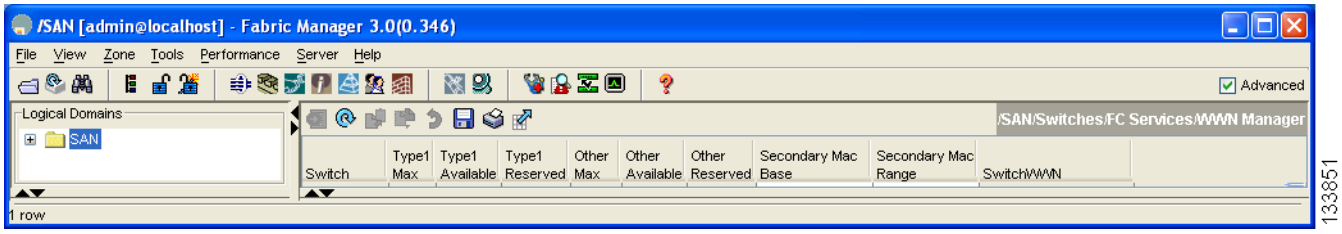
**ステップ 1**　Logical Domains ペインで SAN（または VSAN）を選択します。

Information ペインにスイッチのリストが表示されます。

**ステップ 2**　Physical Attributes ペインで **Switches** を展開して **FC Services** を展開し、**WWN Manager** を選択します。

**ステップ 3**　Information ペインをスクロールし、セカンダリ MAC アドレスを設定するスイッチを表示します（図 31-15 を参照）。

**図 31-15　セカンダリ MAC アドレスの設定**




**ステップ 4**　**Secondary Mac Base** フィールドにセカンダリ MAC アドレスを入力します。

**ステップ 5**　**Secondary Mac Range** フィールドにセカンダリ MAC アドレスを入力します。

**ステップ 6**　**Apply Changes** アイコンをクリックします。

# WWN 情報の表示

WWN 設定のステータスを表示する手順は、次のとおりです。

**ステップ 1**　Logical Domains ペインで SAN（または VSAN）を選択します。

Information ペインにスイッチのリストが表示されます。

**ステップ 2**　Physical Attributes ペインで、**Switches > FC Services > WWN Manager** を選択します。

SAN または VSAN に各スイッチの WWN 情報が表示されます。

# HBA の FC ID 割り当て

ファイバ チャネル標準では、任意のスイッチの Fx ポートに接続された N ポートに、一意の FC ID を割り当てる必要があります。使用する FC ID 数を保護するために、Cisco Nexus 5000 シリーズ スイッチは特殊な割り当て方式を使用します。「HBA の FC ID 割り当て」（p.31-29）を参照してください。

# デフォルト設定

表 31-2 に、この章で説明した機能のデフォルト設定値を示します。

**表 31-2　拡張機能のデフォルト設定値**

| パラメータ | デフォルト |
|---|---|
| CIM サーバ | ディセーブル |
| CIM サーバ セキュリティ プロトコル | HTTP |
| D_S_TOV | 5,000 ミリ秒 |
| E_D_TOV | 2,000 ミリ秒 |
| R_A_TOV | 10,000 ミリ秒 |
| fc trace 呼び出しのタイムアウト時間 | 5 秒 |
| fcping 機能によって送信されるフレーム数 | 5 フレーム |
| リモート キャプチャ接続プロトコル | TCP |
| リモート キャプチャ接続モード | パッシブ |
| ローカル キャプチャ フレームの制限 | 10 フレーム |
| FC ID の割り当てモード | auto モード |
| ループ モニタリング | ディセーブル |