Wiresharkを使用したOTVソリューションのトラブルシューティング

内容

概要

このドキュメントでは、Cisco OTVソリューションのトラブルシューティングにおける、既知のフリーウェアパケットキャプチャおよび分析ツールであるWiresharkの使用について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- NexusシリーズスイッチのOverlay Transport Virtualization(OTV)
- マルチプロトコルラベルスイッチング(MPLS)レイヤ2仮想プライベートネットワーク(VPN)の基礎
- Wiresharkは、無料でオープンソースのパケットアナライザ(https://www.wireshark.org)

使用するコンポーネント

このドキュメントの情報は、Nexus 7000 シリーズ スイッチ プラットフォームに基づいています。

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ました。このド

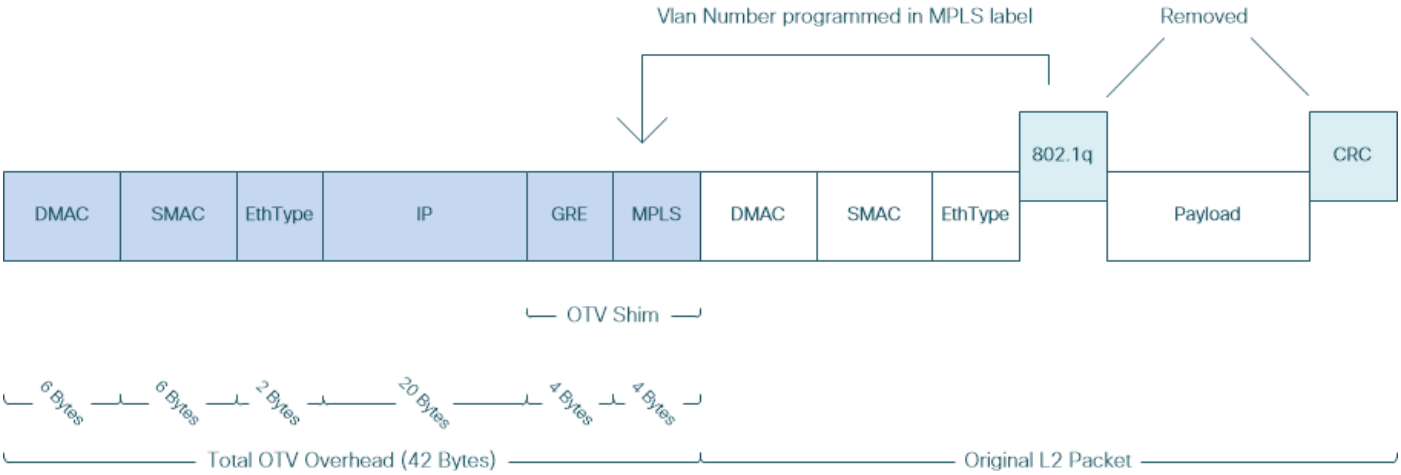
キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

問題の説明

VPN環境でネットワークの問題をトラブルシューティングする際には、カプセル化されたパケットのキャプチャと分析を行う技術の1つが必要です。ただし、Cisco OTVネットワーク環境では、このアプローチには特定の課題があります。Wiresharkなどの一般的に使用されるパケット分析ツール、 a 無料およびオープンソースパケットアナライザ OTVカプセル化トラフィックの内容が正しく解釈されない可能性があります。したがって、通常、データ分析を正常に実行するには、カプセル化されたデータをOTVパケットから抽出するなどの手間のかかる回避策が必要です。

OTVパケット形式

OTVカプセル化は、パケットの全体的なMTUサイズを42バイト増やします。これは、元のレイヤ2フレームからCRCフィールドと802.1Qフィールドを削除し、OTV Shim（VLANおよびオーバーレイID情報も含む）と外部IPヘッダーを追加するOTVエッジデバイスの動作の結果です。



MPLS L2VPNソリューションでは、アンダーレイネットワーク内のデバイスに、MPLSパケットペイロードを正しくデコードするための十分な情報がありません。MPLSコアネットワークでのパケット転送はラベルに基づいて行われるため、アンダーレイネットワークでのMPLSパケットの内容を詳細に分析する必要はありません。

ただし、OTVパケットのデータ分析がトラブルシューティングやモニタリングの目的で必要な場合は、これは課題となります。

Wiresharkなどのパケット分析ツールは、通常のMPLSパケット解析ルールを適用して、MPLSヘッダーに続くパケットデータのデコードを試みます。ただし、通常はMPLS L2VPNヘッドエンドルータとテールエンドルータの間で実行されるコントロールワードネゴシエーションの結果に関する情報がない場合があるため、パケット分析ツールはデフォルトの解析動作に戻り、MPLSヘッダーに続くパケットデータに適用されます。

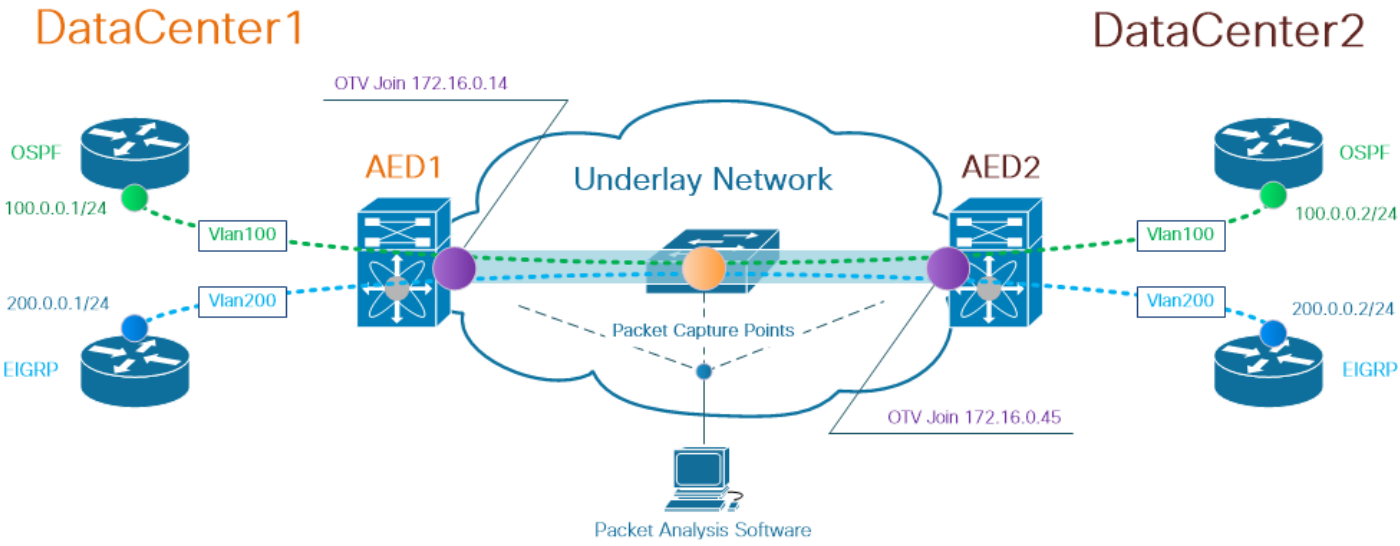
> **注**：Any Transport Over MPLS(ATOM)などのMPLS L2VPNソリューションでは、疑似配線エンドポイントが制御語パラメータの使用をネゴシエートします。制御語は、MPLSラベルスタックと疑似配線パケットのレイヤ2ペイロードの間にあるオプションの4バイトフィー

ルドです。コントロールワードは、汎用およびレイヤ2ペイロード固有の情報を伝送します。Cビットが1に設定されている場合、アドバタイジングプロバイダーエッジ(PE)は、シグナリングされる疑似回線のすべての疑似回線パケットにコントロールワードが存在することを想定します。Cビットが0に設定されている場合、コントロールワードは存在しません。

その結果、デフォルトのWireshark解析動作ではOTVパケットの内容が正しく解釈されない可能性があるため、OTVネットワークのトラブルシューティングプロセスがより複雑になります。

トポロジ

次に、単純なOTVネットワークのネットワークダイアグラムを示します。Vlan 100とVlan 200のルータは、2つのデータセンター（DataCenter1とDataCenter2）間にそれぞれOSPFとEIGRPの隣接関係を確立します。DataCenter Interconnect(DCI)は、N7kスイッチ間にOTVトンネルを使用して実装されます。図では、AED1とAED2として示されています。



注:Cisco OTVソリューションでは、Authoritative Edge Device(AED)の役割の概念を使用します。この役割は、特定のサイトでOTVトラフィックをカプセル化およびカプセル化解除するネットワークデバイスに割り当てられます。

トンネリングソリューションでよく見られる課題は、特定の種類のオーバーレイパケット（IGP、FHRPなど）がアンダーレイネットワークの特定のポイントに到達するかどうかを確認することです。例として、OSPFとEIGRPのオーバーレイトラフィックを使用します。

パケット キャプチャ

ネットワークでパケットキャプチャを実行するには、複数の方法があります。1つのオプションは、Cisco CatalystおよびCisco Nexusスイッチングプラットフォームで使用可能なCisco Switched Port Analyzer(SPAN)機能を使用することです。

トラブルシューティングプロセスの一部として、複数のポイントでパケットキャプチャを実行する必要がある場合があります。アンダーレイネットワークのOTV Joinインターフェイスおよびインターフェイスは、SPANパケットキャプチャポイントとして使用できます。

解決方法

Wiresharkのデフォルト解析エンジンは、OTVカプセル化オーバーレイパケットの最初の数バイトを、Pseudowire Emulation Edge-to-Edge(PWE3)コントロールワードの一部として誤って解釈する可能性があります。

> **注**：MPLS擬似回線エミュレーションエッジツーエッジ(PWE3)コントロールワードは、このドキュメントの残りの部分で*はコントロールワード*と呼ばれています。

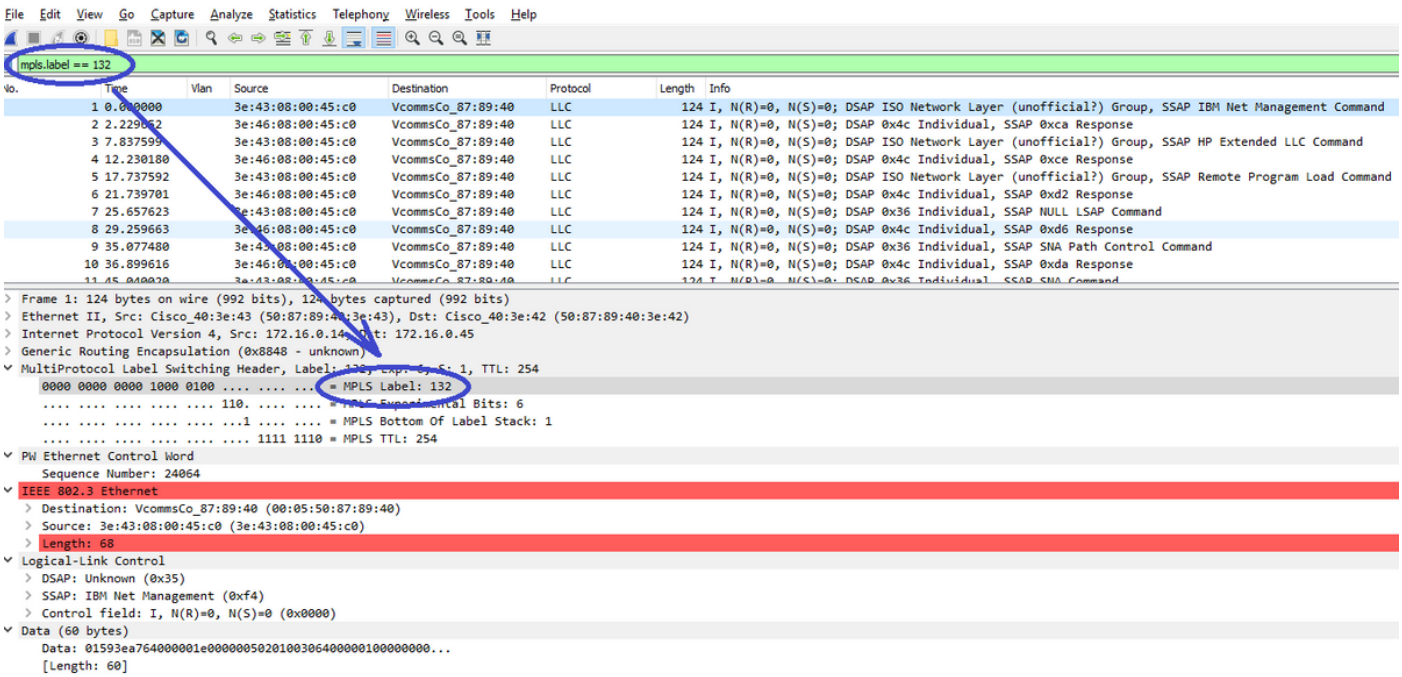
Wiresharkパケット分析ツールがOTVカプセル化パケットの内容を正しく解釈するには、パケットデコードプロセスを手動で調整する必要があります。

> **注**：OTVヘッダーで使用されるMPLSラベルは、オーバーレイVLAN番号+ 32と同じです。

Vlan 100のパケットのデコード

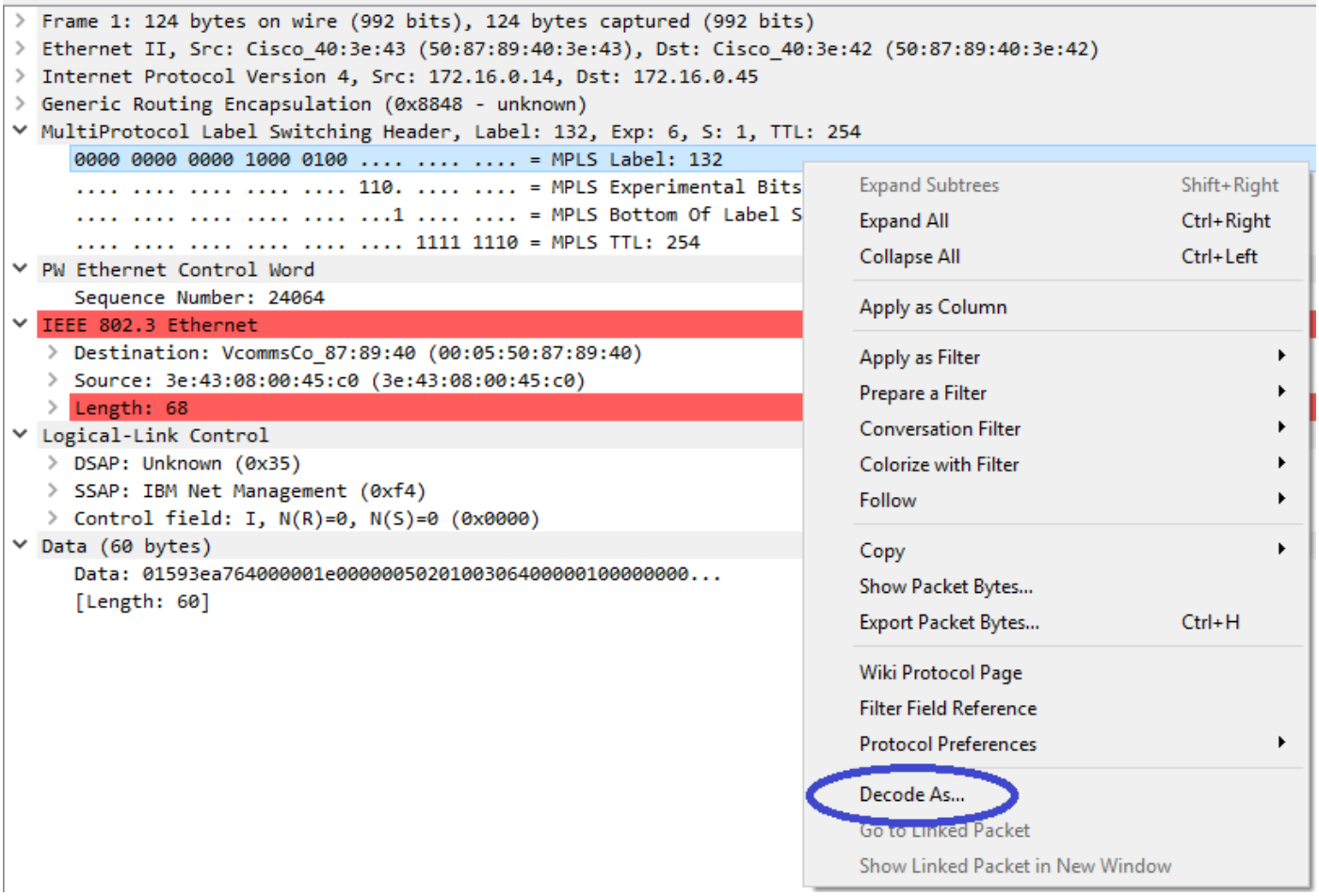
デコードプロセスの最初のステップとして、OTV拡張VLAN 100の内容を伝送するOTVカプセル化パケットのみを表示します。使用されるフィルタは、VLAN 100を表すmpls.label == 132です。

> **注**：OTV経由で拡張された特定のVLANのOTVカプセル化パケットを表示するには、Wiresharkの表示フィルタmpls.label == <<vlan number extended over OTV> + 32>を使用します



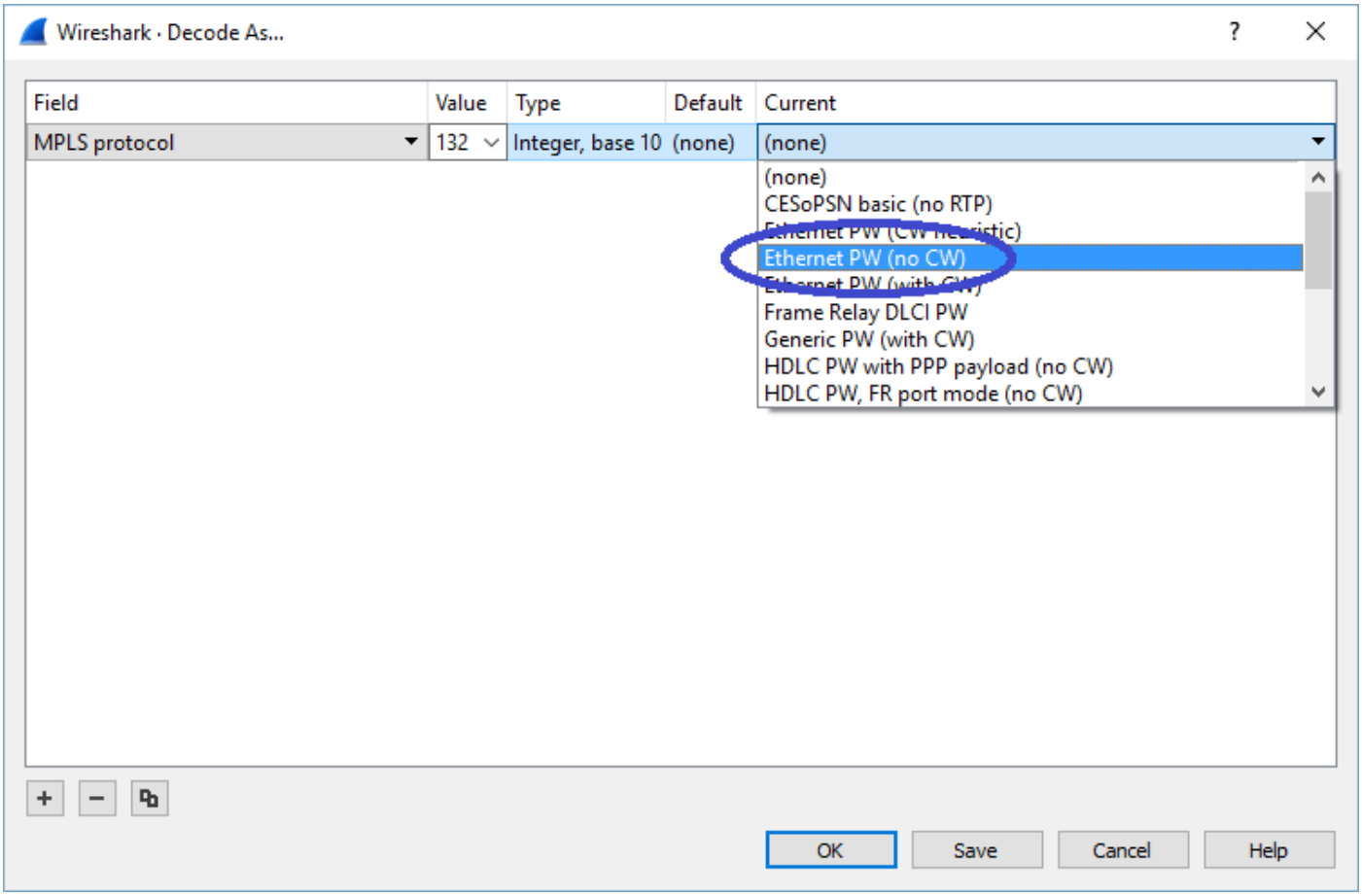
OTV経由で拡張されたVlan 100のOTVカプセル化パケットを表示する

デフォルトでは、WiresharkはMPLS L2VPNパケットのコンテンツの最初の4バイトをコントロールワードとして解釈します。これは、OTVカプセル化パケットに対して修正する必要があります。これを行うには、任意のパケットのMPLSラベルフィールドを右クリックし、[*Decode As...*]を*選択します。* オプション.



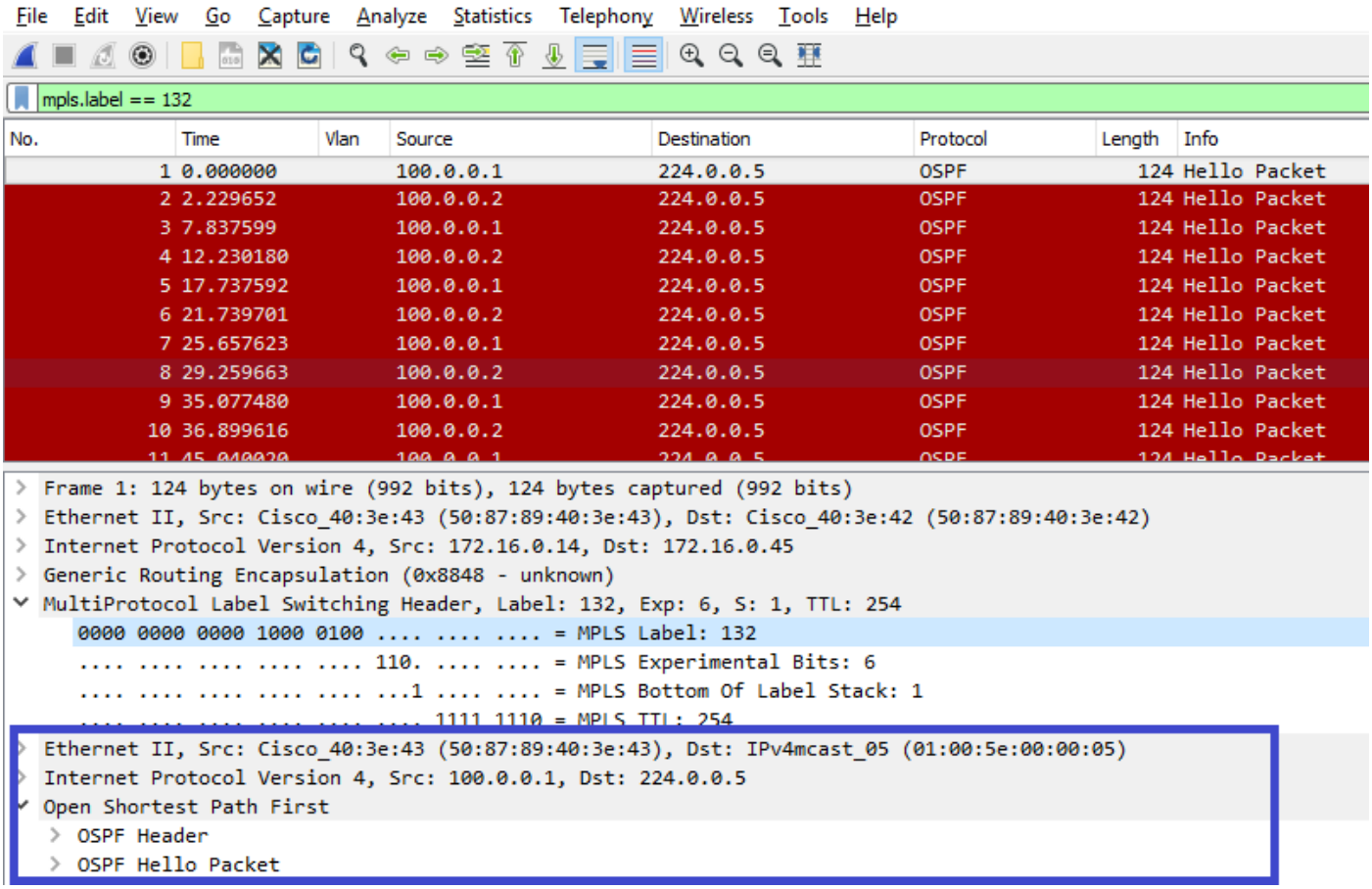
[MPLS label]フィールドを右クリックし、[Decode As...]オプションを選択します

次のステップは、カプセル化されたコンテンツにコントロールワードがないことをWiresharkに通知することです。



[no CW]オプションを選択します

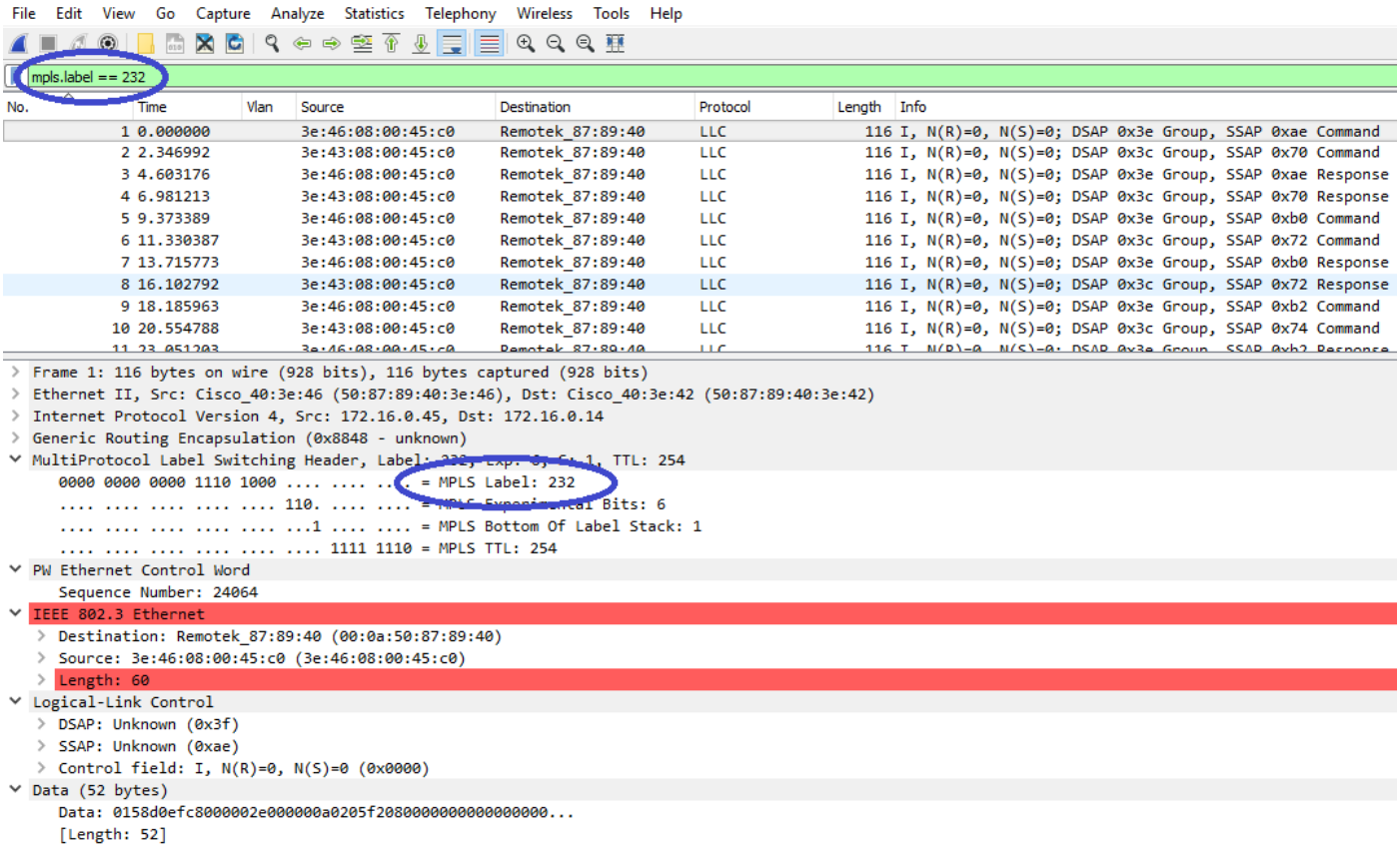
[OK]ボタンをクリックしてこの変更を送信すると、Wireshark分析ツールはOTVカプセル化パケットの内容を正しく表示します。



Wiresharkは、OTVカプセル化パケットの内容を正しく表示します

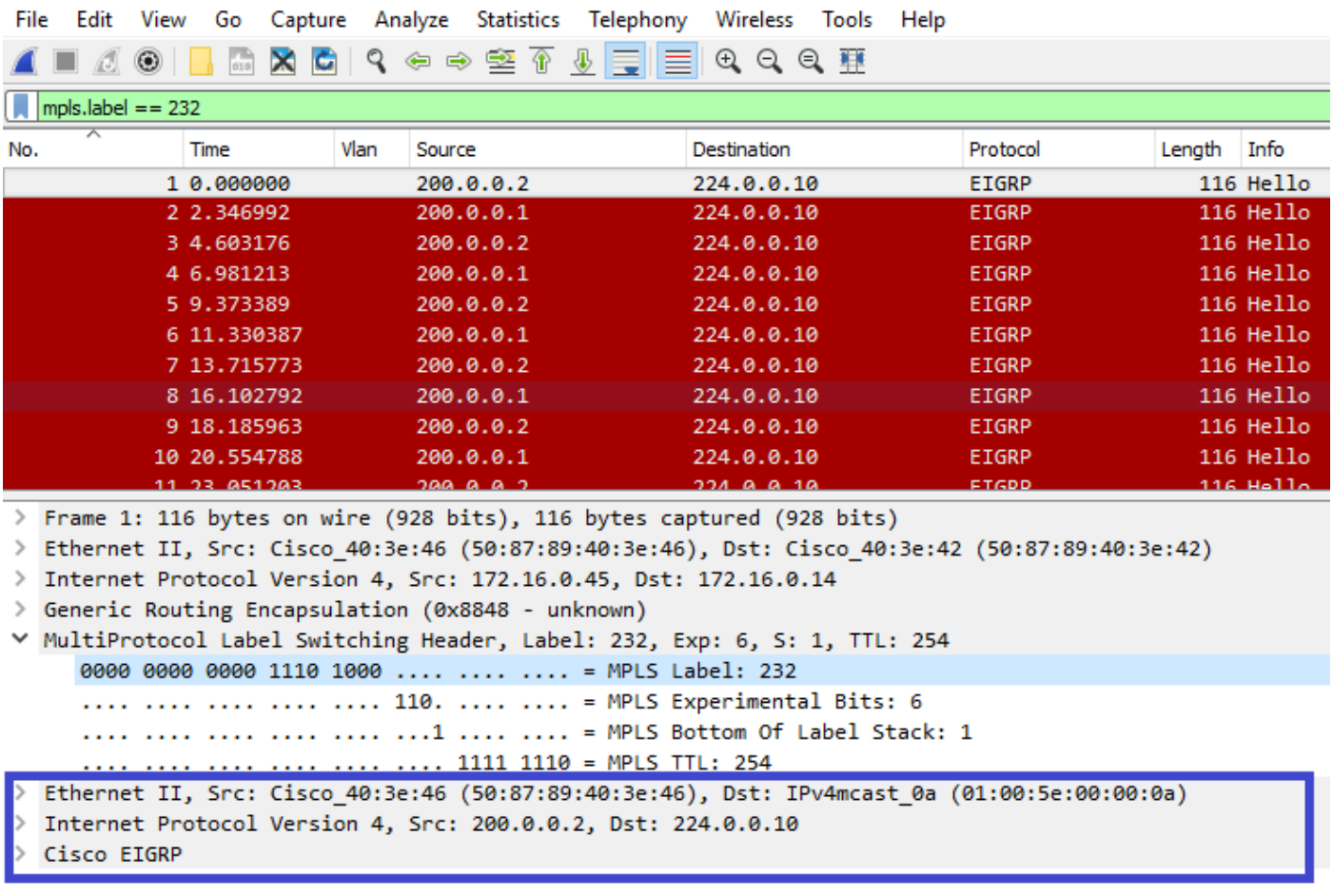
Vlan 200のパケットのデコード

上記の手順は、OTVを介して拡張されたVLANに適用できます。たとえば、Wiresharkフィルタを使用してVLAN 200のパケットのみを表示すると、分析ツールに次の出力が表示されます。



OTVで拡張されたVLAN 200のパケットを表示する

WiresharkがMPLSパケットの最初の数バイトをPW Control Wordとして解釈しないように指示されると、デコードプロセスは正常に完了します。



WIresharkは、Vlan 200トラフィックをEIGRPパケットとして正しく表示します

Editcapを使用したOTVヘッダーの削除

通常、Wiresharkのインストールには、Editcapというコマンドラインパケット編集ツールが*付属します*。このツールは、キャプチャされたパケットからOTVオーバーヘッドを永久に削除できます。これにより、Wiresharkの解析動作を手動で調整しなくても、Wiresharkグラフィカルユーザインターフェイス(GUI)でキャプチャされたパケットを簡単に表示および分析できます。

WindowsプラットフォームでEditcapを実行

Windowsオペレーティングシステムでは、*editcap.exe*はデフォルトでc:\Program Files\Wireshark>ディレクトリにインストールされます。

このツールを – Cフラグを*付けて実行*し、OTVオーバーヘッドを削除し、結果を.pcapファイルに*保存*します。

```
c:\Users\cisco\Desktop> "c:\Program Files\Wireshark\editcap.exe" -C 42 otv-underlay-capture.pcap
otv-underlay-capture-no-header.pcap
c:\Users\cisco\Desktop>
```

Mac OSプラットフォームでのEditcapの実行

Mac OSオペレーティングシステムでは、 editcapは/usr/local/binフォルダにあります。

```
CISCO:cisco$ /usr/local/bin/editcap -C 42 otv-underlay-capture.pcap otv-underlay-capture-no-
header.pcap
CISCO:cisco$
```

キャプチャされたパケットからOTVヘッダーを削除し、*Editcap*ツールMPLSヘッダーの一部としてエンコードされたVlan情報が失われ、OTV shimの一部になります。特定のVLANのトラフィックのみを分析する必要がある場合、*Editcapツールを使用してOTVヘッダーを削除する前に、「mpls.label == <<vlan number extended over OTV> + 32>' Wireshark GUIフィルタを使用してください。*

結論

Cisco OTVソリューションのトラブルシューティングには、コントロールプレーンの動作とデータプレーンのカプセル化の両方の観点から、テクノロジーを十分に理解する必要があります。知識を効果的に活用することで、Wiresharkなどのフリーウェアパケット分析ツールは、OTVパケット分析において非常に強力であることを証明できます。さまざまなパケット表示オプションに加えて、一般的なWiresharkのインストールでは、パケット分析を簡素化できるパケット編集ツールが提供されます。これにより、特定のトラブルシューティングセッションに最も関連するパケットコンテンツの部分にトラブルシューティングを集中させることができます。