OTV ソリューションを解決するのに Wireshark を使用して下さい

目次

概要

この資料は Wireshark の使用、Cisco OTV ソリューションの解決のよく知られている な フリーウェア パケットキャプチャおよび分析ツールを、示したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- オーバーレイ トランスポート仮想化（OTV）（OTV）Nexus シリーズ スイッチで
- マルチプロトコル ラベル スイッチング（MPLS）レイヤ2 仮想 な 私用 Netwoks（VPN）の基本
- Wireshark、自由なおよびオープン ソース 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 文書に記載されている 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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中

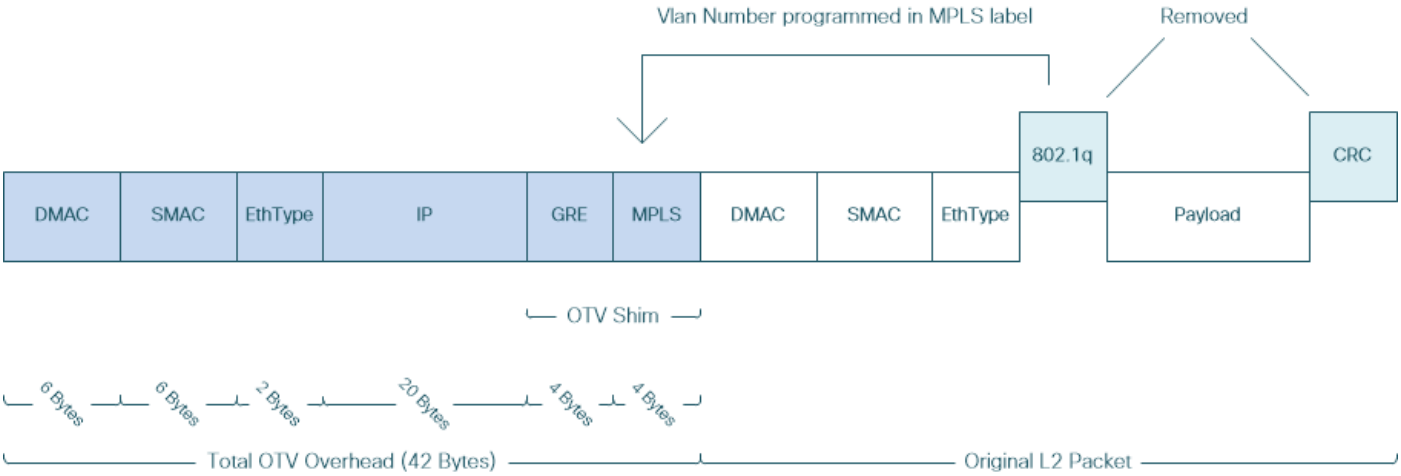
のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

問題の説明

VPN環境のネットワーク上の問題をトラブルシューティングするとき、手法の 1 つはカプセル化されたパケットのキャプチャおよび分析を伴います。 ただし、Cisco OTV ネットワーク環境でこのアプローチはある特定のチャレンジに会います。 広く使われたパケット 分析ツールは、Wireshark のような、自由なおよびオープン ソース パケットアナライザ、正しく OTV カプセル化されたトラフィックのコンテンツを解読しないかもしれません。 正常にデータ 解析を行うために通常 OTV パケットからのカプセル化 された データの抽出のようなそれ故に困難な回避策が、必要となります。

OTV パケットフォーマット

OTV カプセル化は 42 バイトにつきパケットの全面的な MTU サイズを増加します。 これはオリジナル レイヤ2 フレームから CRC および 802.1Q フィールドを削除し、OTV シム (VLAN およびオーバーレイ ID 情報がまた含まれています) および外部 IP ヘッダを付加する OTV エッジ デバイスのオペレーションの結果で。



MPLS L2VPN ソリューションでは、下敷きネットワークのデバイスに十分な情報が正しく MPLS パケット ペイロードをデコードするありません。 通常、これは従って下敷きネットワークの MPLS パケットのコンテンツの詳細な分析が必要とならない MPLS コアネットワークのパケット転送がラベルに基づいていた実行されたので、問題ではないです。

ただしこれは OTV パケットのデータ 解析が目的を解決することおよび/または監視するために必要となる場合チャレンジを示します。

パケット 分析ツールは、Wireshark のような、ルールを解析する規則的な MPLS パケットの適用によって MPLS ヘッダに続くパケットデータをデコードするように試みます。 ただし、それは MPLS L2VPN ヘッドエンドおよびテールエンド ルータの間で普通実行された 制御 ワード ネゴシエーションの結果についての情報がないかもしれないので、パケット 分析ツールはデフォルト解析動作に戻って落ち、MPLS ヘッダに続くパケットデータにそれを適用します。

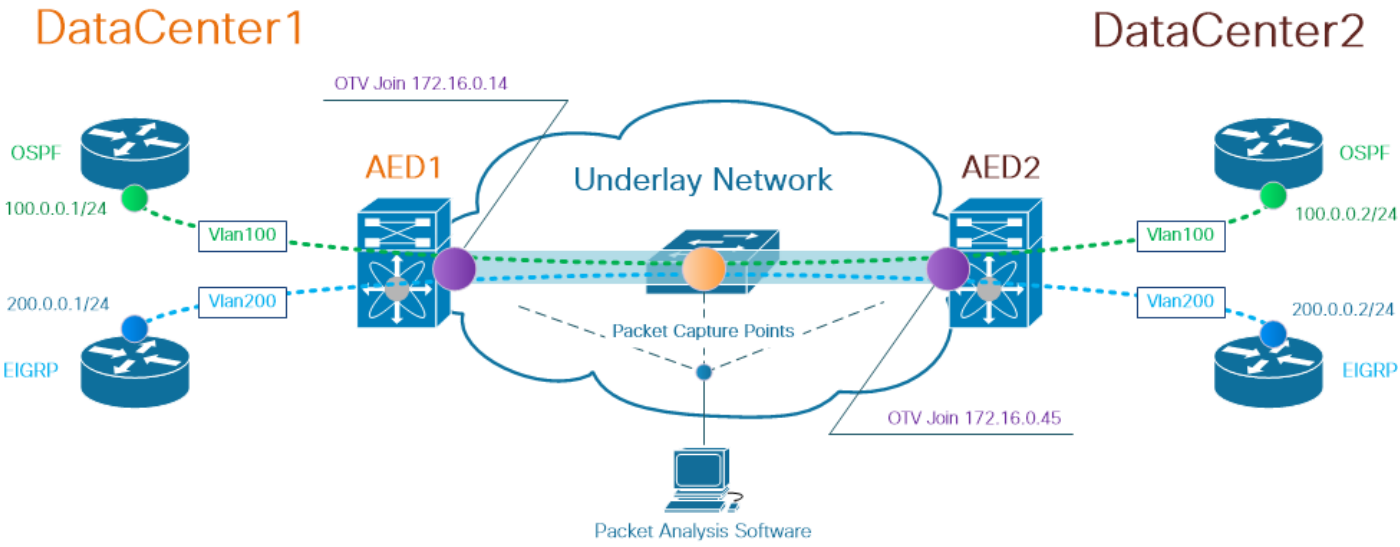
> **注:** MPLS （ 原子 ）上のあらゆる転送するのような MPLS L2VPN ソリューションでは、pseudowire エンド ポイントは制御 ワード パラメータの使用をネゴシエートします。 制御

ワードは pseudowire パケットに MPLS ラベルスタックとレイヤ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。 制御 ワードはジェネリックおよびレイヤ2 ペイロード仕様情報を伝えます。 C ビットが 1 に設定 される場合、アドバタイジング Provider Edge （PE）は信号を送られている pseudowire の各 pseudowire パケットにあると制御 ワードが期待します。 C ビットが 0 に設定 される場合、制御 ワードはあると期待されません。

従ってその結果、動作を解析するデフォルト Wireshark は OTV パケットのコンテンツを正しく解読しないかもしれ OTV ネットワークのトラブルシューティング プロセスを複雑にします。

トポロジ

以下は簡単な OTV ネットワークのネットワークダイアグラムです。 VLAN 100 および VLAN 200 確立する OSPF および 2 データセンター間の EIGRP 隣接関係のルータ、DataCenter1 および DataCenter2、それぞれ。 データセンター相互接続（DCI）は AED1 としてダイアグラムで表示される N7k スイッチと AED2 間の OTV トンネルと設定されます。



注: Cisco OTV ソリューションは特定のサイトで OTV トラフィックをカプセル化し、カプセル化を解除するネットワークデバイスに割り当てられる保証された エッジ デバイス（AED）ロールの概念を使用します。

頻繁にトンネリング ソリューションで見られるチャレンジはオーバーレイ パケット（IGP、FHRP、等）の特定の種類が下敷きネットワークのある特定のポイントにそれを作るかどうか確かめることです。 OSPF および EIGRP オーバーレイ トラフィックは一例として使用されます。

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行う複数の方法があります。 1 つのオプションは Cisco スイッチド ポート アナライザ（SPAN） 機能、利用可能 な Catalyst および Cisco Nexus スイッチング プラットフォームを on Cisco 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、複数のポイントのパケットキャプチャは実行された必要がある場合もあります。 下敷きネットワークの OTV 加入 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することができます。

解決策

Wireshark デフォルト解析エンジンは MPLS パケット交換網上の MPLS L2VPN で一般的に使用される Pseudowire エミュレーション エッジ ツー エッジ（PWE3）制御 ワードの一部であるように OTV カプセル化されたオーバーレイ パケットのはじめの幾つかのバイトを誤解するかもしれません。

> **注:** MPLS Pseudowire エミュレーション エッジ ツー エッジ（PWE3）制御 ワードはようにこの資料の他の*制御 ワード*参照されます。

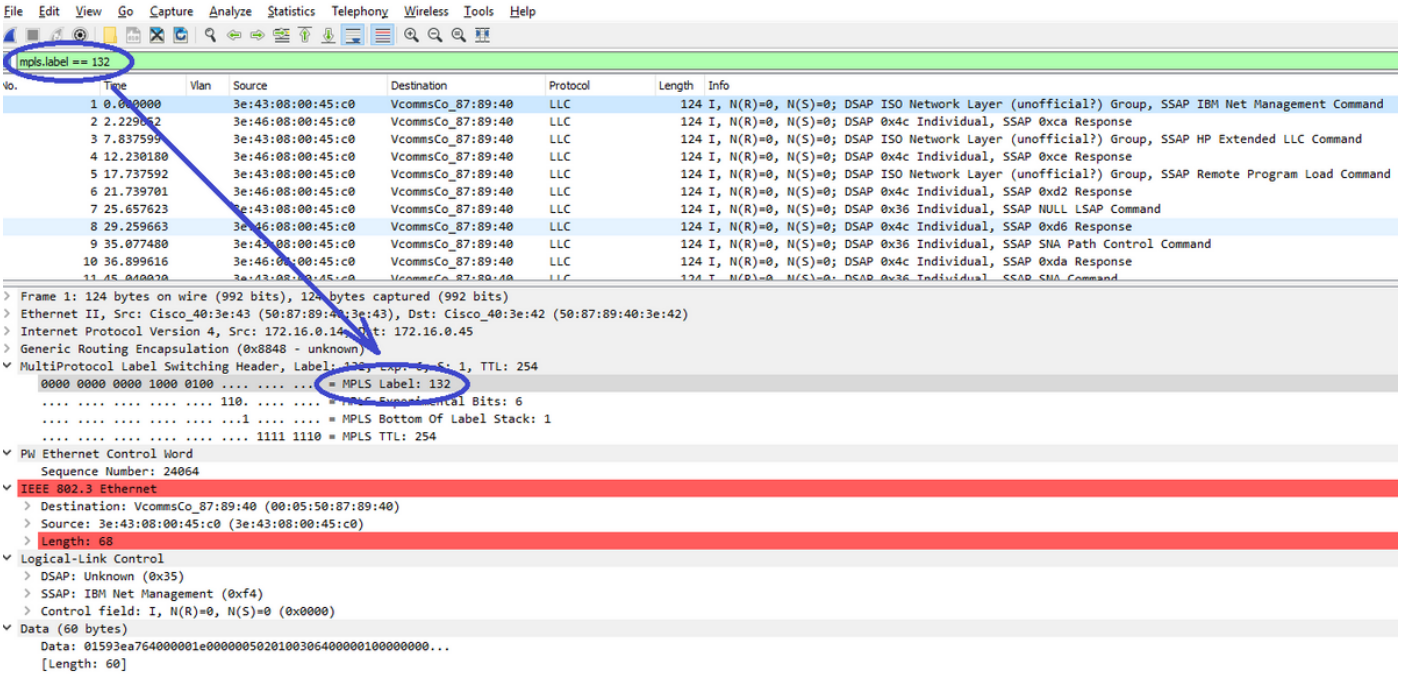
Wireshark パケット 分析ツールを確認するためにパケット デコード プロセスに OTV カプセル化されたパケットのコンテンツを、手動調整です必要正しく解読します。

> **注:** OTV ヘッダで使用される MPLS ラベルはオーバーレイ VLAN ナンバーに + 32 匹敵します。

VLAN 100 のデコード パケット

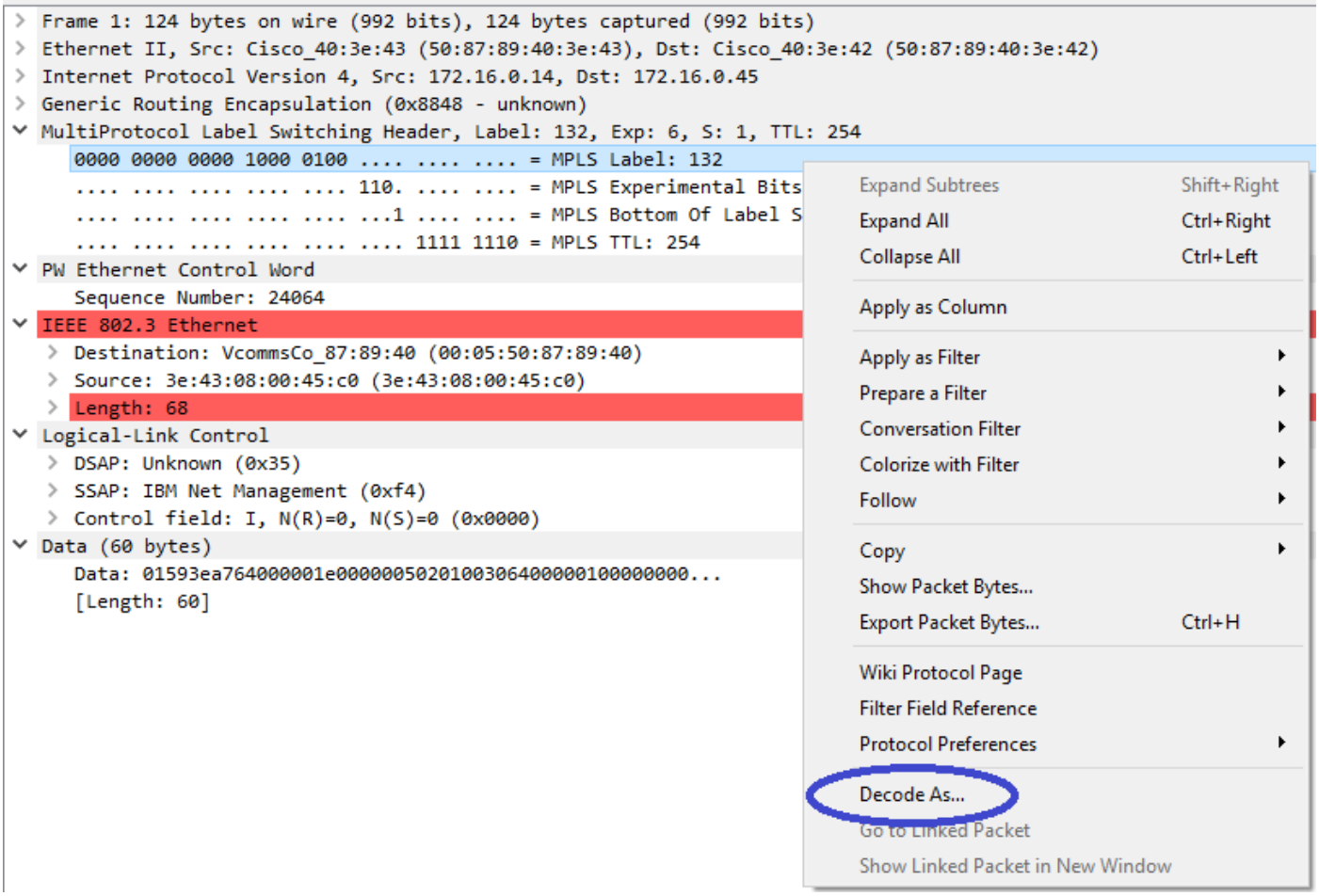
手始めとしてデコード プロセスの、OTV 拡張 VLAN 100 のコンテンツを運ぶ OTV カプセル化されたパケットだけ表示する。 使用されるフィルタは VLAN 100 を表す mpls.label == 132 です。

> **注:** 表示する OTV に伸びた特定のVLAN のためのパケットを使用します次の Wireshark ディスプレイ フィルタを OTV カプセル化しました: mpls.label == <<vlan 数はに OTV> + 32> 伸びました



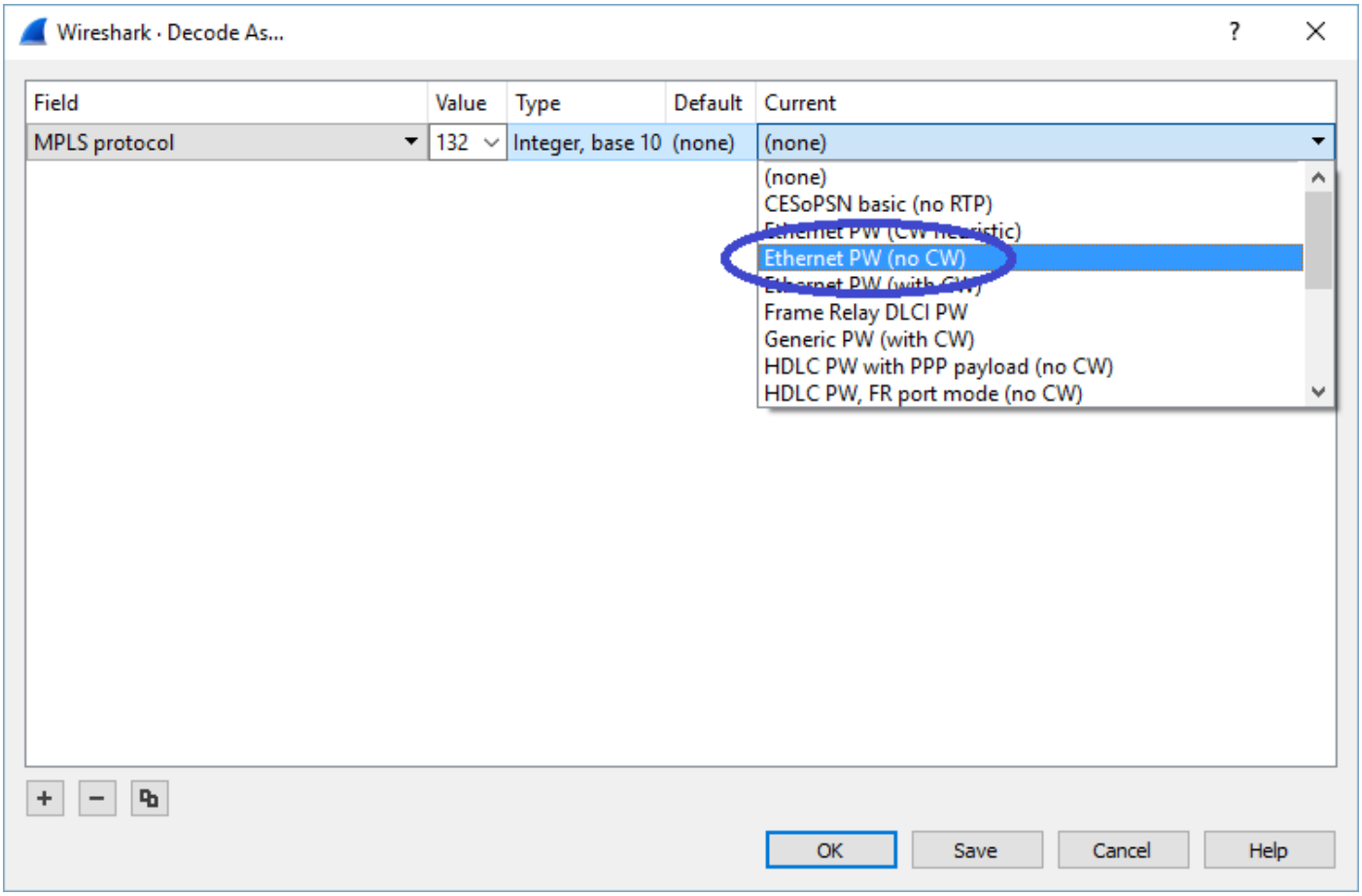
OTV に伸びる VLAN 100 のための OTV カプセル化されたパケットを表示する

デフォルトで Wireshark は制御 ワードとして MPLS L2VPN パケットのコンテンツの最初の 4 バイトを解読します。 これは OTV カプセル化されたパケットを修正される必要があります。 これを、パケットの何れかの MPLS ラベル フィールドの右クリックは...オプションとしてするために、*デコード*を選択し。



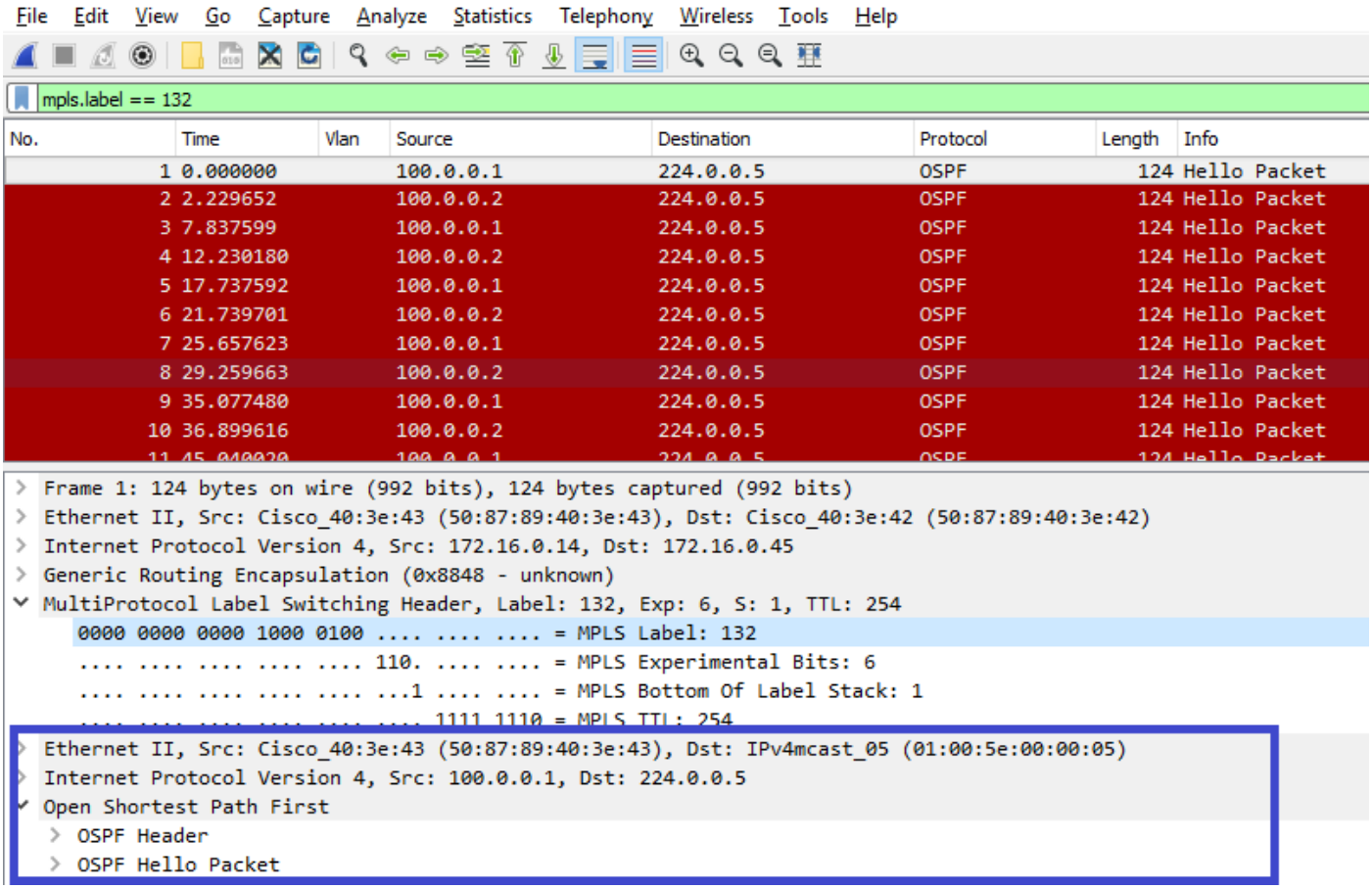
MPLS ラベル フィールドを右クリックし、...オプションとしてデコードを選択して下さい

次のステップはカプセル化されたコンテンツに制御 ワードがないように Wireshark に言うことです。



オプションを"no CW"を 選択する

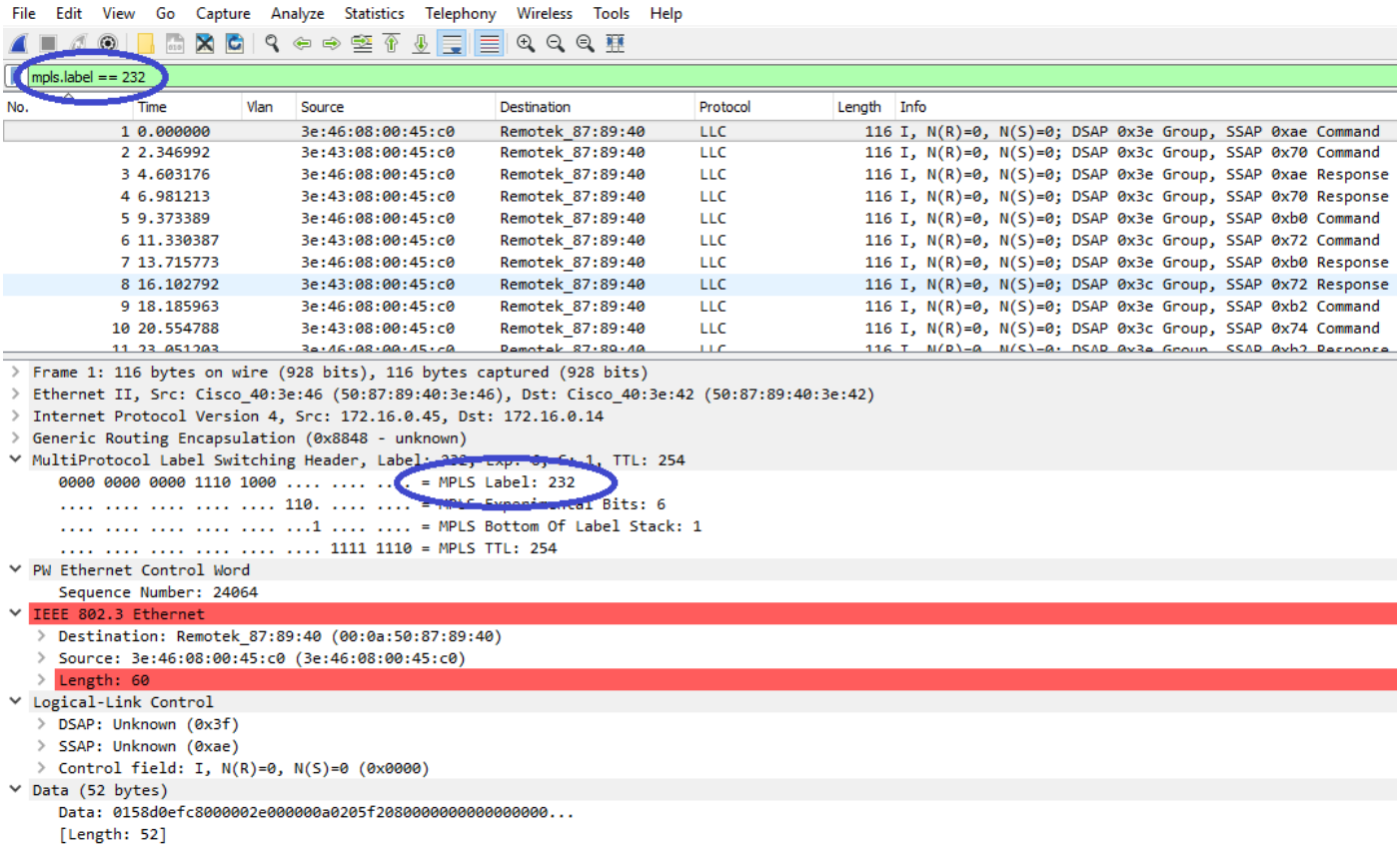
この変更がボタンを『OK』 をクリック することによって入ったら、Wireshark 分析ツールは OTV カプセル化されたパケットのコンテンツを正しく表示する。



OTV カプセル化されたパケットの正しの Wireshark ディスプレイ コンテンツ

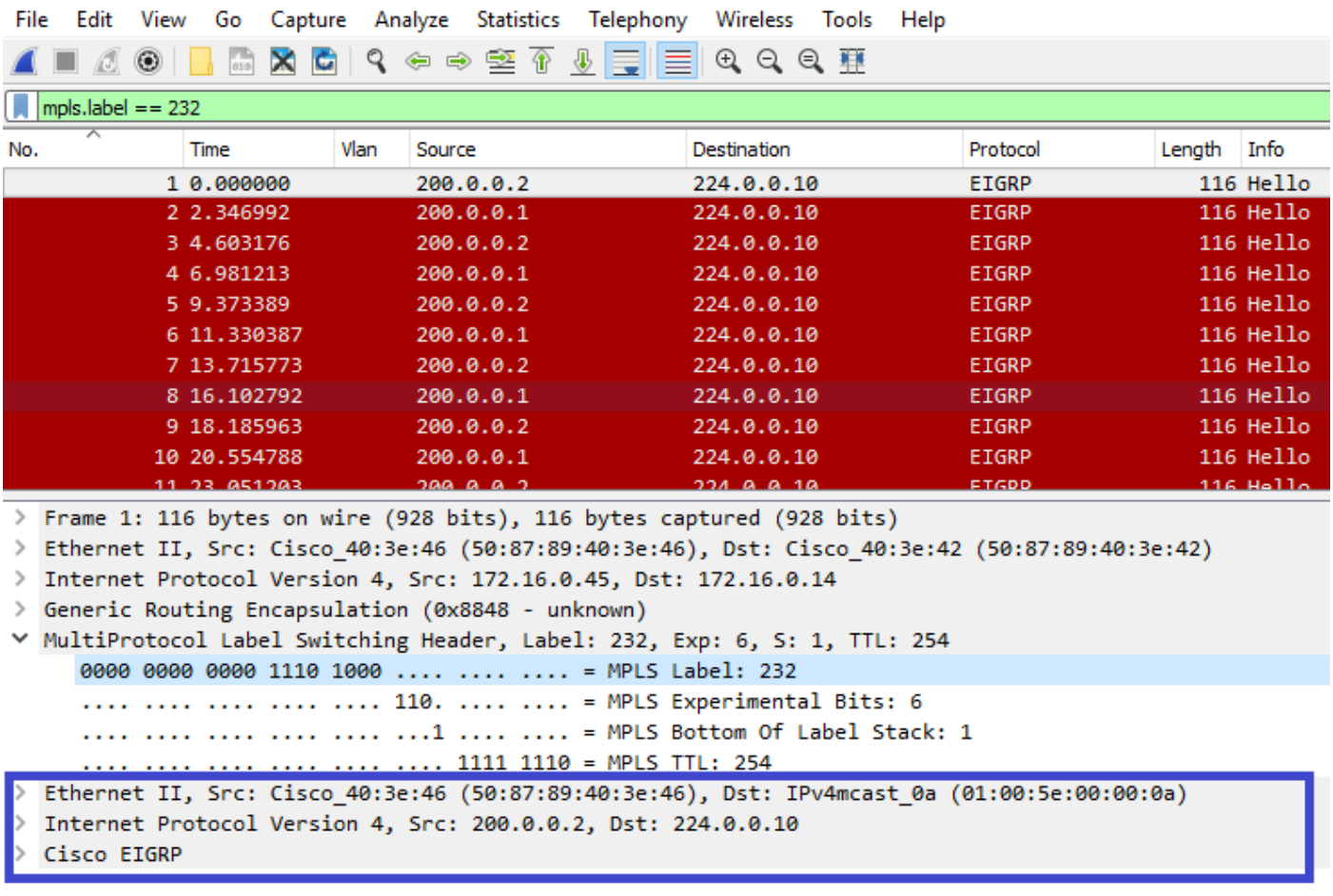
VLAN 200 のデコード パケット

ステップの上で OTV に伸びるあらゆる VLAN に適当でであって下さい。 たとえば、VLAN 200 のパケットだけ表示する Wireshark フィルタを使用して分析ツールで出力するために次を得ます。



OTV に伸びる VLAN 200 のためのパケットを表示する

Wireshark が PW 制御 ワードとして MPLS パケットのはじめの幾つかのバイトを解読しないように指示されたらプロセスを正常に完了できますデコードして下さい。



WIreshark は EIGRP パケットとして正しく VLAN 200 トラフィックを表示する

OTV ヘッダを削除するのに Editcap を使用して下さい

通常、Wireshark インストールはコマンド・ライン パケット編集ツールによって呼出される *Editcap* が付いています。 このツールはキャプチャされるパケットから OTV オーバーヘッドを永久削除にすることができます。 これは手動で Wireshark の解析動作を調節する必要なしで Wireshark グラフィカル ユーザ インターフェイス（GUI）のキャプチャされるパケットの容易なディスプレイおよび分析を、可能にします。

Windows プラットフォームの Editcap を実行して下さい

ON ウィンドウ オペレーティング システムは c:\Program Files\Wireshark > ディレクトリに、*editcap.exe* デフォルトでインストールされています。

実行して下さいこのツールをと- OTV オーバーヘッドを取除き、*.pcap* ファイルの結果を保存する *C* フラグ。

```
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 プラットフォームの Editcap を実行して下さい

Mac OS オペレーティング システムで、editcap は /usr/local/bin フォルダで利用できます。

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

キャプチャされるパケット withEditcaptool から OTV ヘッダを削除することによって、1 つは次々と OTV シムの部品である、MPLS ヘッダの一部として符号化される VLAN 情報を失います。「Editcaptool と OTV ヘッダを削除する前にに OTV> + 32>' Wireshark GUI フィルタ拡張される mpls.label == <<vlan 数を使用するために忘れないようにして下さい*特定のVLAN のだけトラフィックの分析が必要となる場合。*

結論

Cisco OTV ソリューションを解決することはコントロール プレーン オペレーションおよびデータ平らなカプセル化観点からの両方テクノロジーのよい理解を、必要とします。 実際にはナレッジを適用して、Wireshark のようなフリーウェア パケット 分析ツールは OTV パケット 分析の非常に強力証明できます。 さまざまなパケット ディスプレイ オプションに加えて、Wireshark 典型的なインストールはパケット 分析を簡素化できるパケット編集ツールを提供します。 これは特定のトラブルシューティング セッションに最も関連しているパケットコンテンツの方に焦点を合わせるために解決することを割り当てます。