使用Wireshark對OTV解決方案進行故障排除

目錄

簡介

本檔案將示範使用眾所周知的免費封包擷取和分析工具Wireshark來排解Cisco OTV解決方案的疑難問題。

必要條件

需求

思科建議您瞭解以下主題：

- Nexus系列交換器上的重疊傳輸虛擬化(OTV)
- 多重協定標籤交換(MPLS)第2層虛擬私人網路(VPN)基礎資訊
- Wireshark，免費和開源資料包分析器(https://www.wireshark.org)

採用元件

本檔案中的資訊是根據Nexus 7000系列交換器平台。

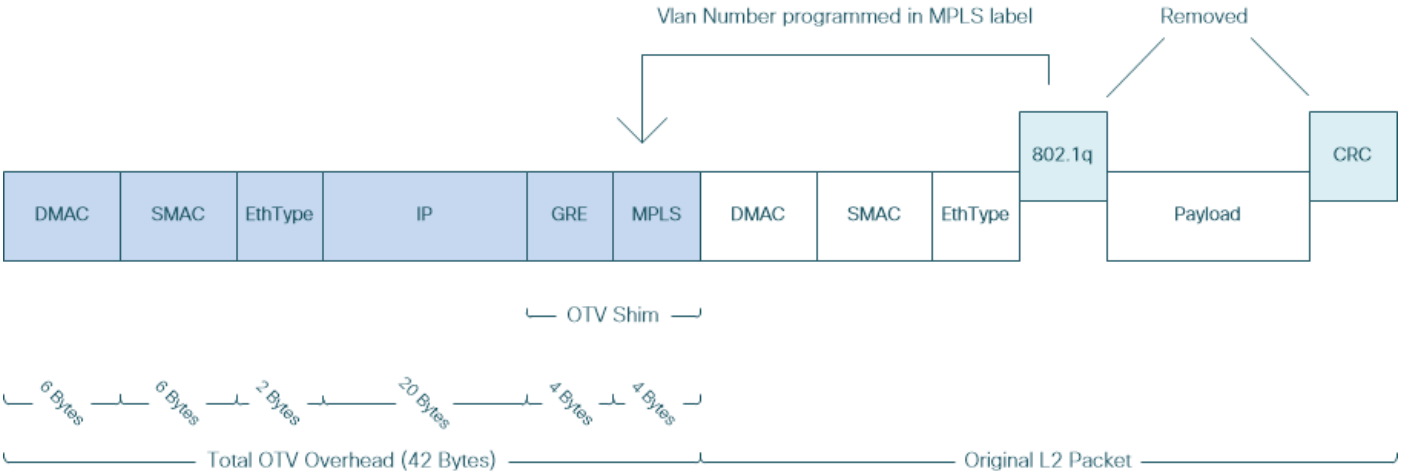
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題描述

當排除VPN環境中的網路故障時，其中一個技術涉及捕獲和分析封裝的資料包。但是，在Cisco OTV網路環境中，這種方法面臨一定的挑戰。常用的資料包分析工具，如Wireshark， 答 自由開源資料包分析器， 可能無法正確解釋OTV封裝流量的內容。因此，為了成功執行資料分析，通常需要費力的解決方法，例如從OTV資料包提取封裝的資料。

OTV資料包格式

OTV封裝將資料包的總MTU大小增加42位元組。這是OTV邊緣裝置操作的結果，該裝置從原始第2層幀中刪除CRC和802.1Q欄位，並新增OTV填充碼（也包含VLAN和重疊ID資訊）和外部IP報頭。



在MPLS L2VPN解決方案中，底層網路中的裝置沒有足夠的資訊來正確解碼MPLS資料包負載。通常，這不是問題，因為MPLS核心網路中的分組轉發是基於標籤執行的，因此不需要對底層網路中的MPLS分組的內容進行深入分析。

但是，如果出於故障排除和/或監控目的需要OTV資料包的資料分析，則會帶來挑戰。

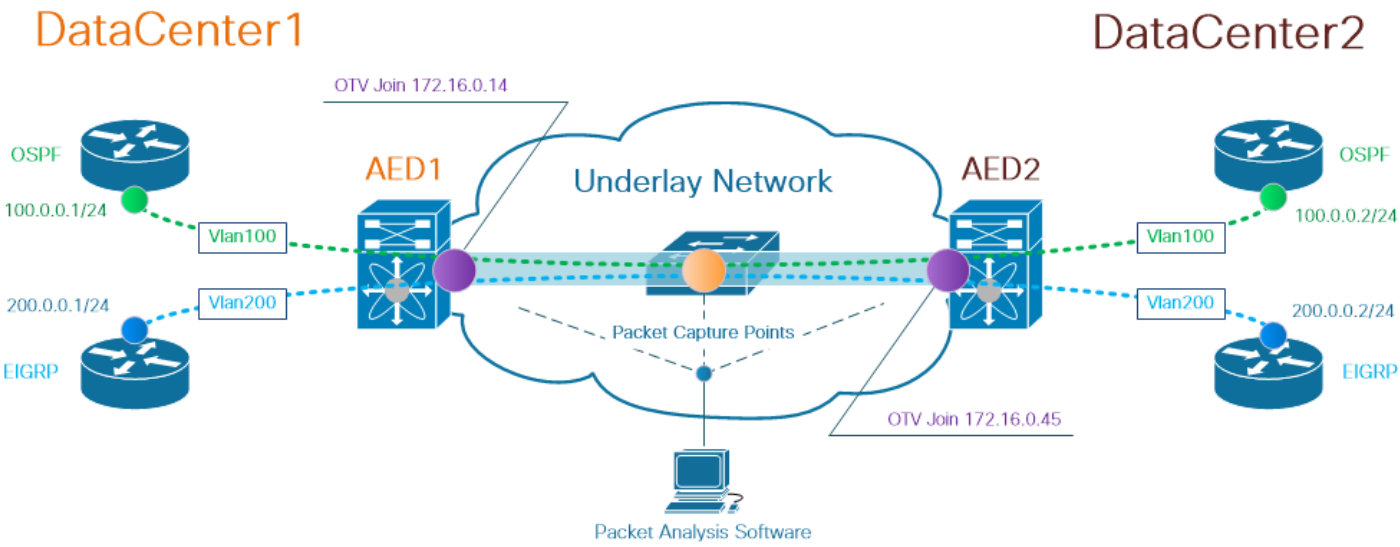
封包分析工具（例如Wireshark）嘗試透過應用常規MPLS封包解析規則來解碼遵循MPLS標頭的分包資料。但是，由於它可能沒有關於控制字協商結果的資訊（控制字協商通常在MPLS L2VPN頭端和尾端路由器之間執行），因此資料包分析工具回退到預設解析行為，並將其應用於遵循MPLS報頭的資料包資料。

> **附註**：在MPLS L2VPN解決方案(例如通過MPLS的任何傳輸(ATOM))中，偽線端點會協商使用控制字參數。控制字是位於MPLS標籤堆疊和偽線資料包第2層負載之間的可選4位元組欄位。控制字攜帶通用和第2層負載特定資訊。如果C位設定為1，則廣告提供商邊緣(PE)期望控制字出現在所發訊號的偽線上的每個偽線資料包中。如果C位設定為0，則不會出現控制字。

因此，預設的Wireshark解析行為可能無法正確解釋OTV資料包的內容，從而使OTV網路的故障排除過程更加複雜。

拓撲

以下是簡單OTV網路的網路圖。Vlan 100和Vlan 200中的路由器在兩個資料中心（DataCenter1和DataCenter2）之間建立OSPF和EIGRP鄰接關係。資料中心互聯(DCI)通過OTV隧道在N7k交換機之間實施，如圖所示，為AED1和AED2。



> **注意**:Cisco OTV解決方案使用授權邊緣裝置(AED)角色的概念，該角色分配給在特定站點封裝和解封OTV流量的網路裝置。

通道解決方案中經常遇到的難題是驗證特定型別的重疊封包（IGP、FHRP等）是否到達底層網路中的某些點。以OSPF和EIGRP重疊流量為例。

封包擷取

在網路中執行資料包捕獲的方法有多種。一個選項是使用Cisco Catalyst和Cisco Nexus交換平台上提供的Cisco交換埠分析器(SPAN)功能。

作為故障排除過程的一部分，可能需要在多個點執行資料包捕獲。底層網路中的OTV加入介面和介面可用作SPAN資料包捕獲點。

解決方案

Wireshark預設解析引擎可能錯誤地解釋OTV封裝的重疊資料包的前幾個位元組，好像它們是偽線模擬邊緣到邊緣(PWE3)控制字的一部分，該控制字通常在MPLS分組交換網路上的MPLS L2VPN中使用。

> **附註**：MPLS偽線模擬邊緣到邊緣(PWE3)控制字在本文檔的其餘部分中稱為控制字。

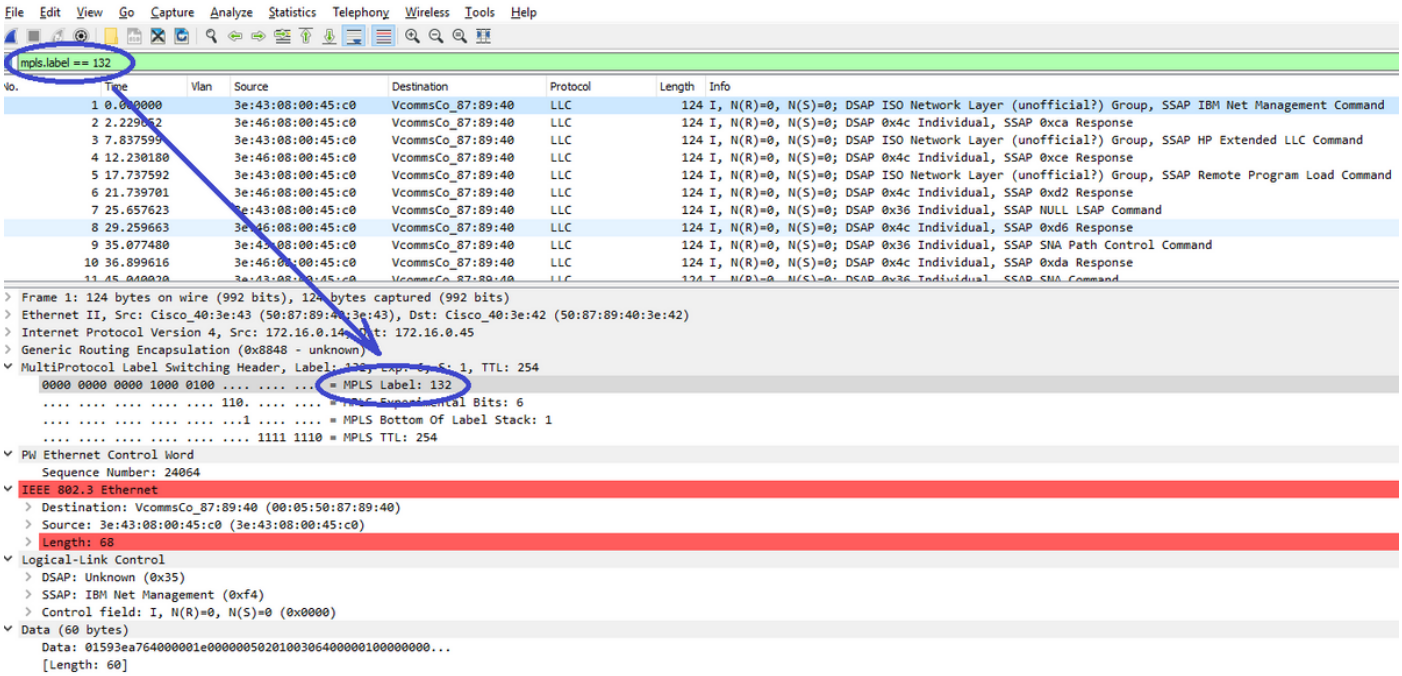
為確保Wireshark資料包分析工具正確解釋OTV封裝資料包的內容，需要對資料包解碼過程進行手動調整。

> **附註**：OTV報頭中使用的MPLS標籤等於重疊VLAN編號+ 32。

解碼Vlan 100中的資料包

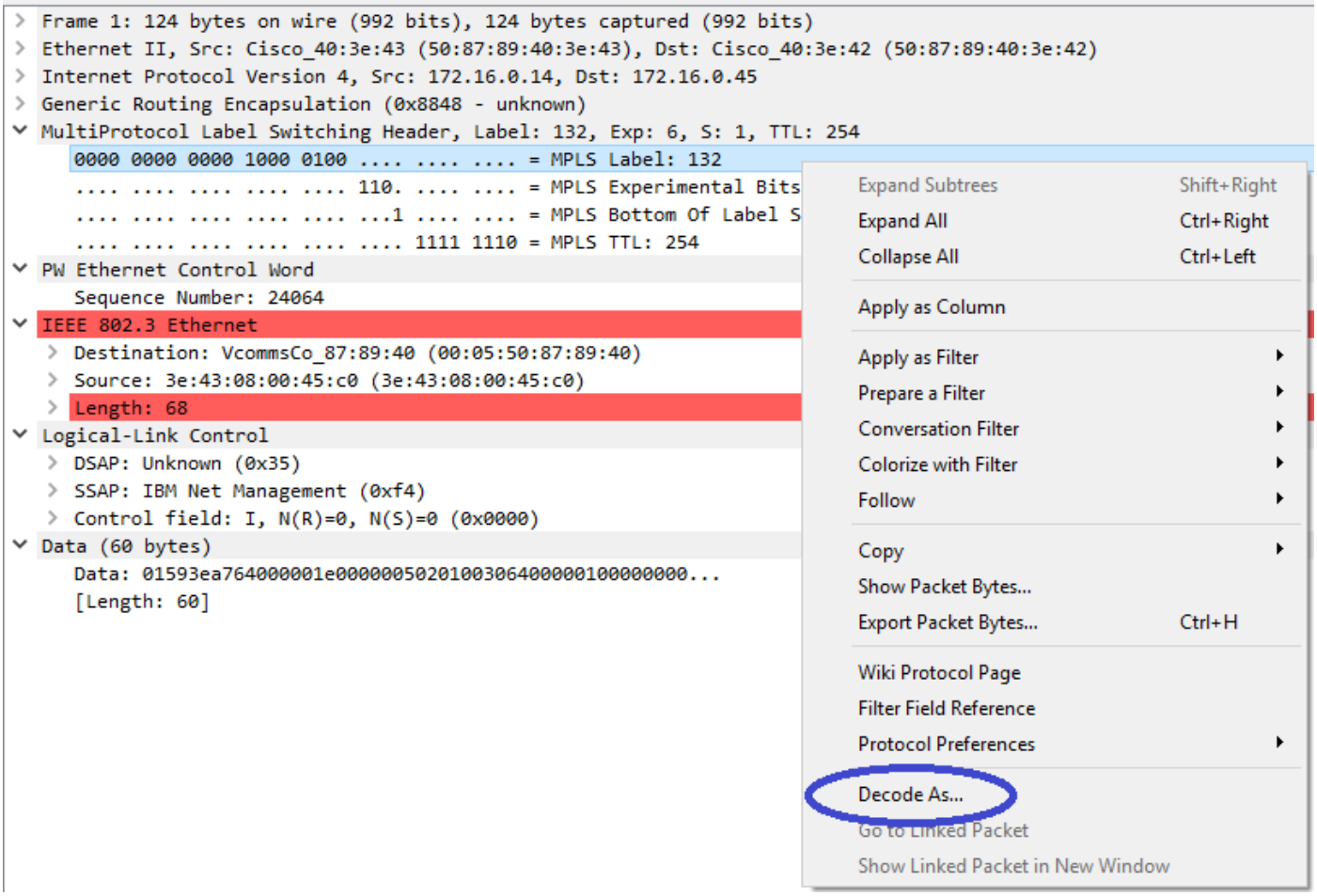
作為解碼過程的第一步，只顯示攜帶OTV擴展VLAN 100內容的OTV封裝資料包。使用的過濾器是mpls.label == 132，代表VLAN 100。

附註：要顯示通過OTV擴展的特定VLAN的OTV封裝資料包，請使用以下Wireshark顯示過濾器：mpls.label == <<vlan number extended over OTV> + 32>



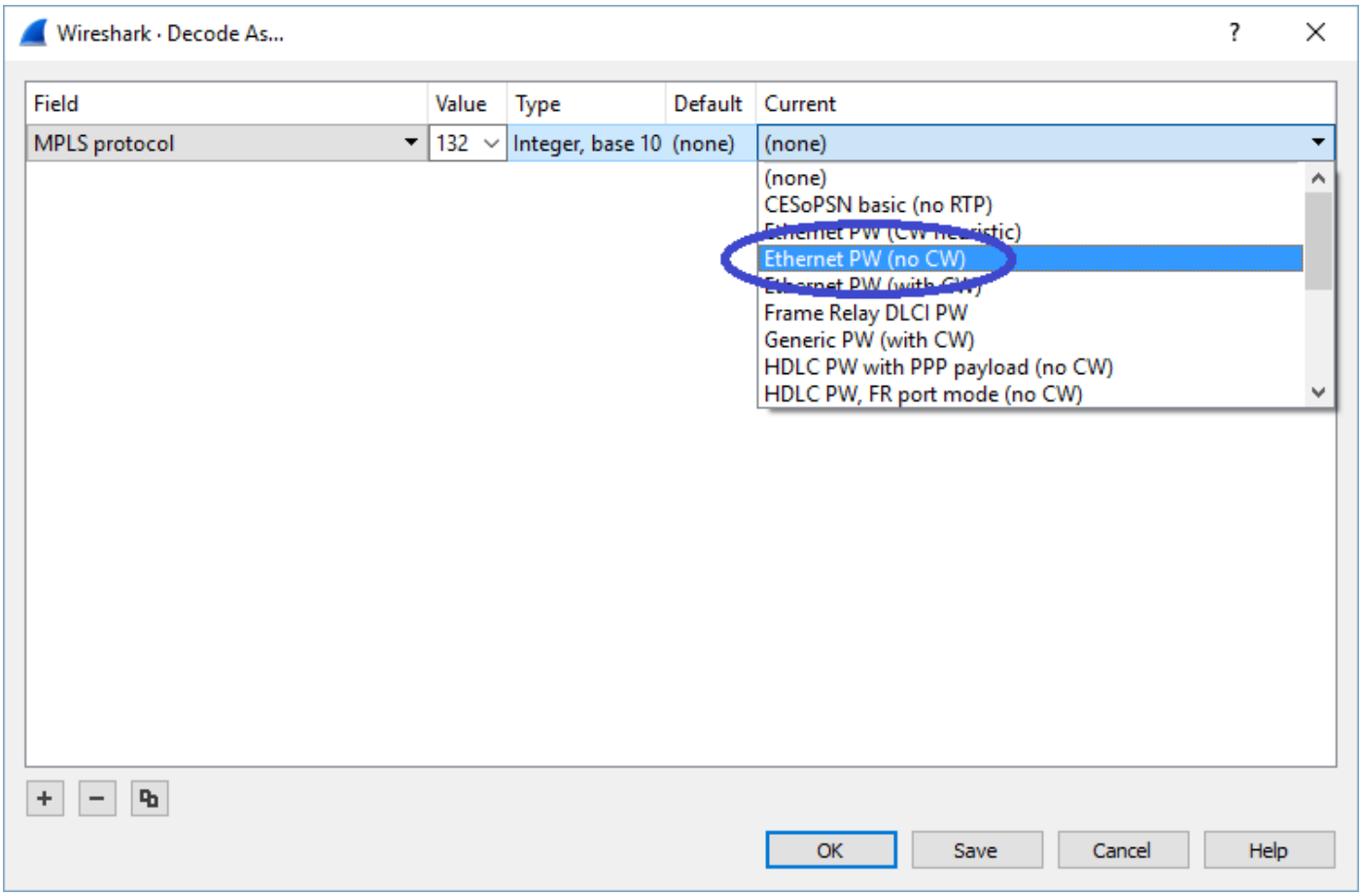
顯示Vlan 100的OTV封裝資料包，通過OTV擴展

預設情況下，Wireshark將MPLS L2VPN資料包內容的前四個位元組解釋為控制字。需要針對OTV封裝的資料包更正此問題。為此，按一下右鍵任何資料包的MPLS標簽欄位，並選擇*解碼為*..... 選項。



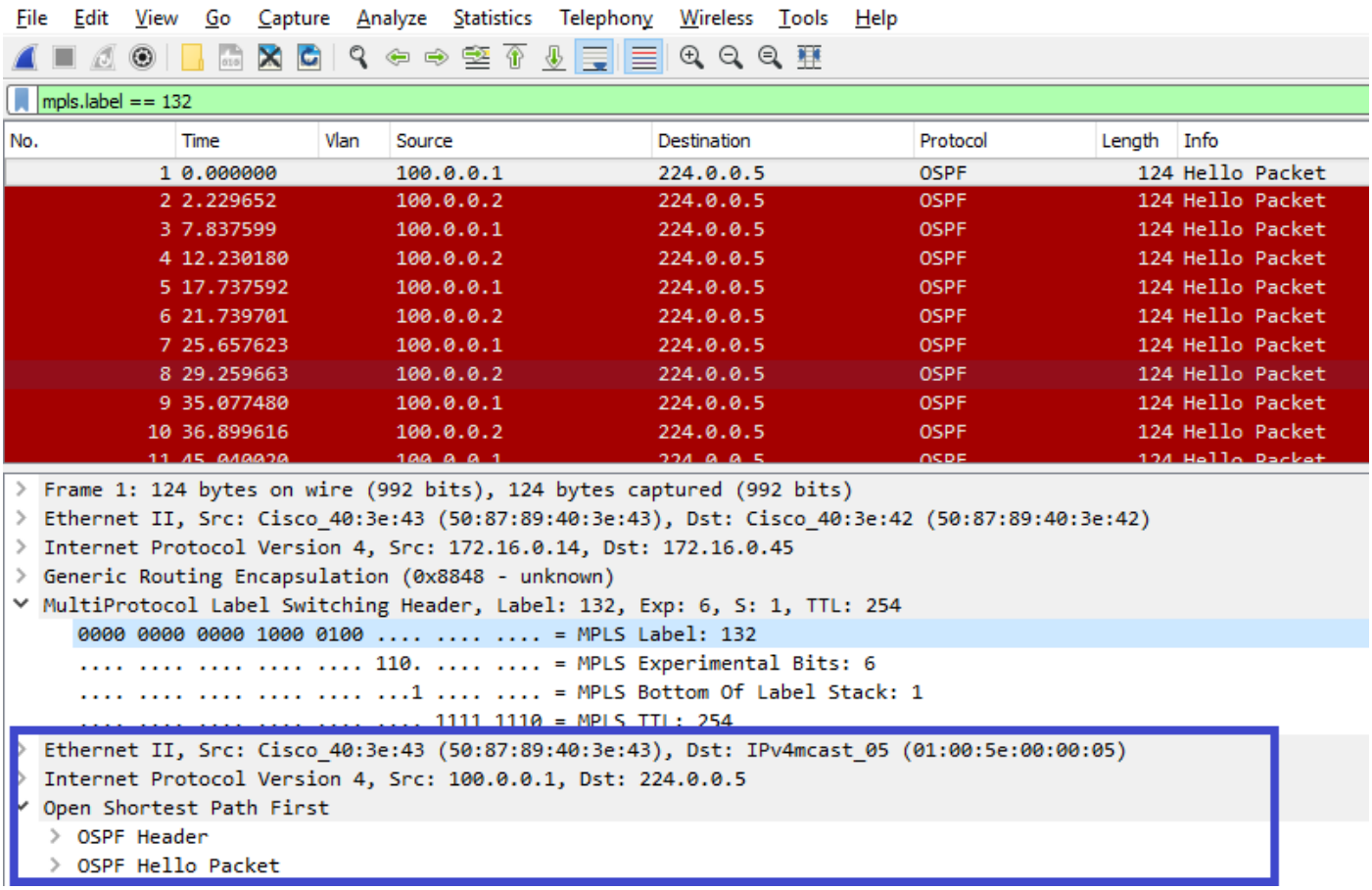
按一下右鍵MPLS標簽欄位，然後選擇「解碼為.....」選項

下一步是通知Wireshark封裝的內容沒有控制字。



選擇「無CW」選項

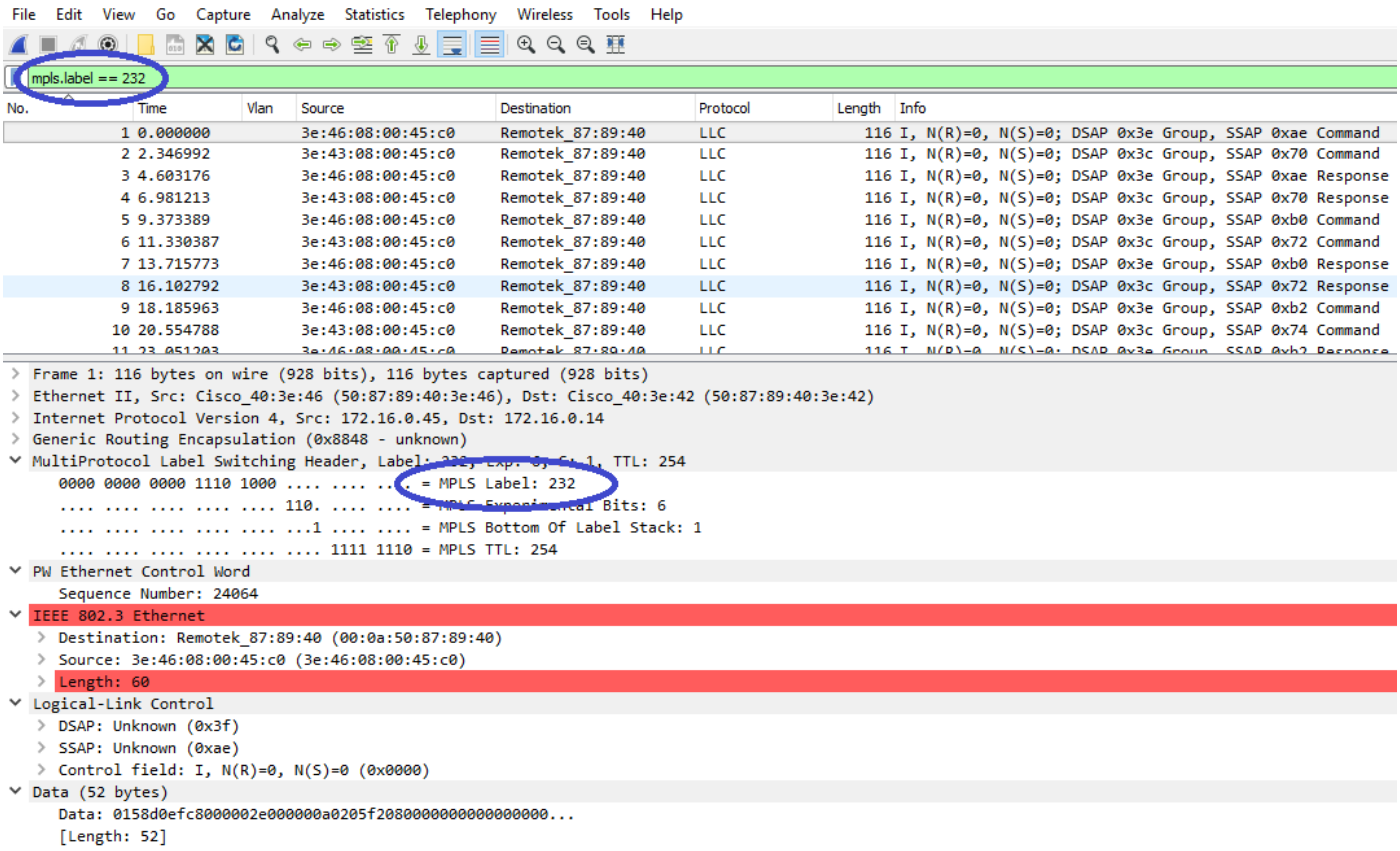
通過按一下「確定」按鈕提交此更改後，Wireshark分析工具將正確顯示OTV封裝資料包的內容。



Wireshark正確顯示OTV封裝資料包的內容

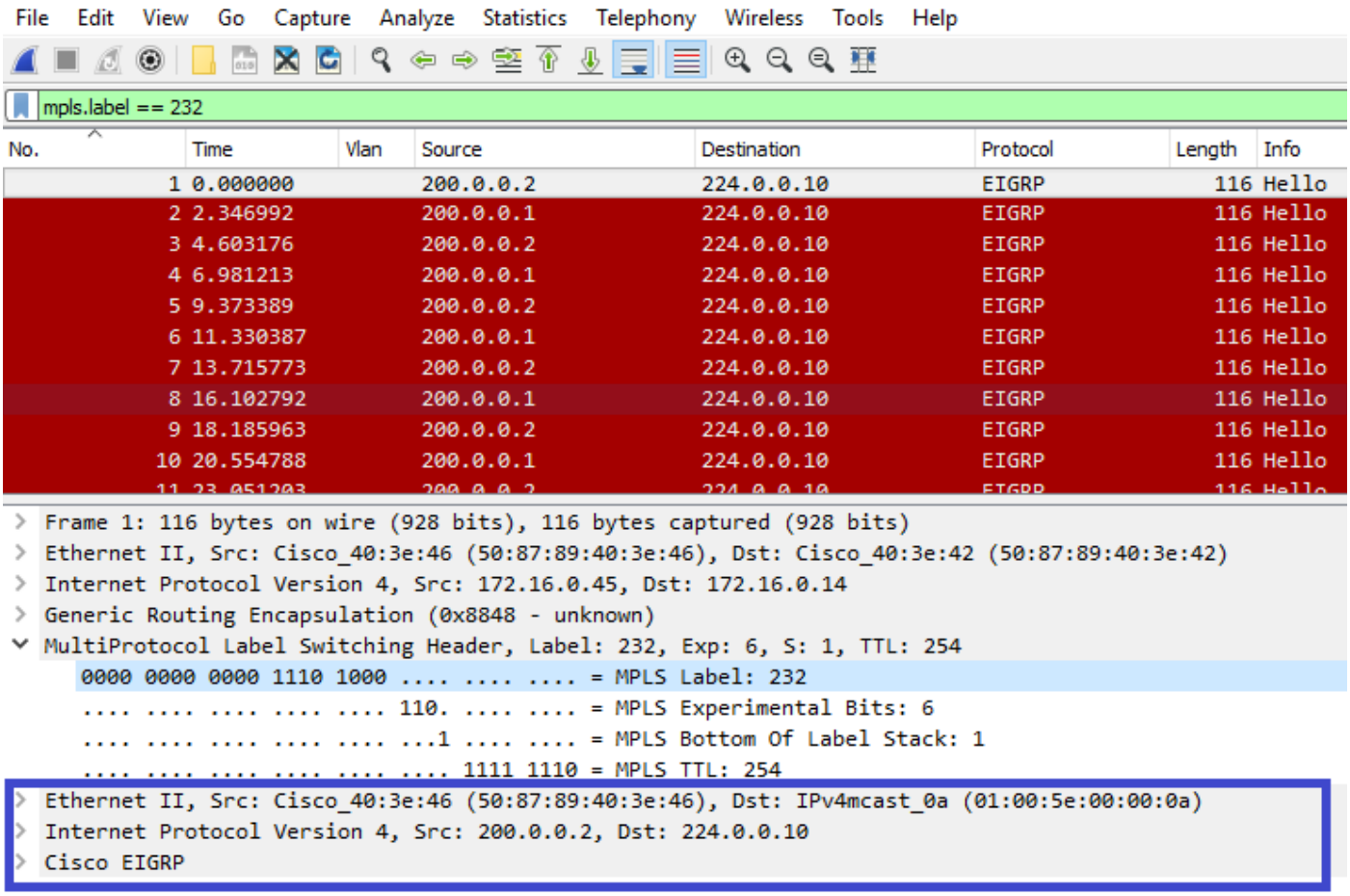
解碼Vlan 200中的資料包

以上步驟適用於通過OTV擴展的任何VLAN。例如，使用Wireshark過濾器只顯示vlan 200的資料包，我們會在分析工具中獲得以下輸出。



顯示VLAN 200的資料包，通過OTV擴展

一旦指示Wireshark不將MPLS資料包的前幾個位元組解釋為PW控制字，解碼過程就可以成功完成。



WIreshark將Vlan 200流量正確顯示為EIGRP資料包

使用Editcap刪除OTV報頭

通常，Wireshark安裝隨附命令列資料包編輯工具*Editcap*。此工具可以從捕獲的資料包中永久刪除OTV開銷。這允許在Wireshark圖形使用者介面(GUI)中輕鬆顯示和分析捕獲的資料包，而無需手動調整Wireshark的解析行為。

在Windows平台上運行Editcap

在Windows作業系統上，*editcap.exe*預設安裝在c:\Program Files\Wireshark>目錄中。

使用*-C* 標誌運行此工具，以刪除OTV開銷並將結果儲存到*.pcap*檔案中。

```
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>
```

在Mac OS平台上運行Editcap

在Mac OS作業系統上，可在/usr/local/bin資料夾中使用editcap。

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

通過使用*編輯*工具，則會丟失作為MPLS報頭一部分編碼的VLAN資訊，而MPLS報頭又是OTV填充碼的一部分。如果僅需要分析特定Vlan的流量，請記住，使用「mpls.label == <<vlan number extended over OTV> + 32>」Wireshark GUI過濾器之前，使用*Editcap*工具刪除OTV報頭。

結論

排除Cisco OTV解決方案故障需要從控制平面操作和資料平面封裝的角度很好地瞭解技術。通過有效應用這些知識，Wireshark等免費資料包分析工具在OTV資料包分析中非常強大。除了各種資料包顯示選項，典型的Wireshark安裝還提供了資料包編輯工具，可以簡化資料包分析。這樣，故障排除可以側重於資料包內容中與特定故障排除會話最相關的部分。