请使用Wireshark排除故障OTV解决方案

目录

简介

本文展示使用Wireshark、一著名的免费软件数据包捕获和分析工具，在排除故障思科OTV解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- 重叠传输虚拟化(OTV)在连结系列交换机
- 基础多协议标签交换(MPLS) Layer2虚拟私有Netwoks (VPN)
- Wireshark，一个自由和开放源信息包分析程序(https://www.wireshark.org)

使用的组件

本文档中的信息根据连结7000系列交换机平台。

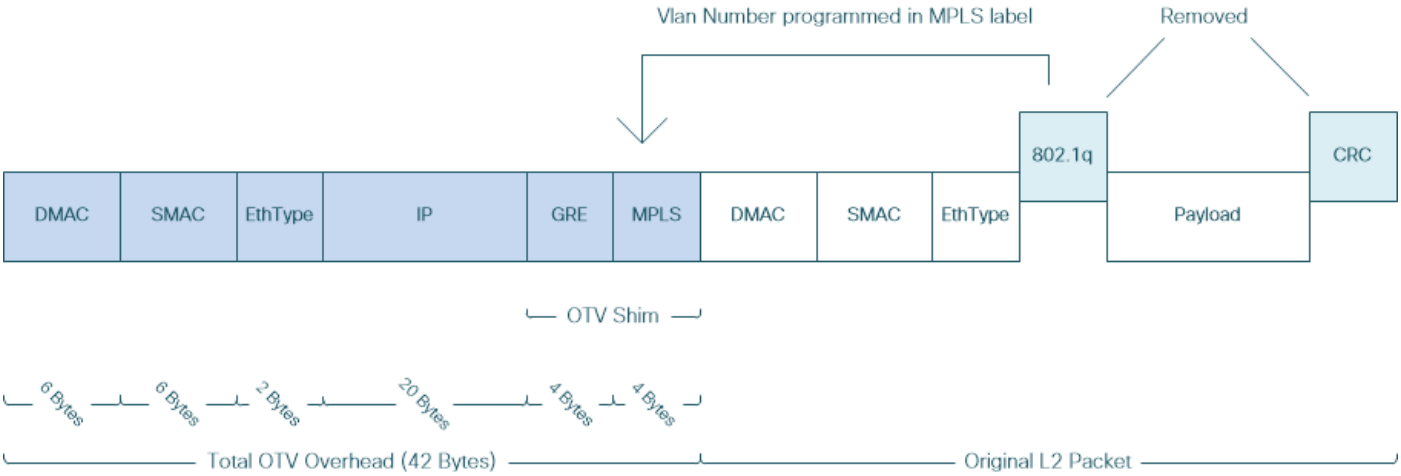
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题说明

当排除故障在VPN环境时的网络问题，其中一个技术包括封装数据包捕获和分析。然而，在思科OTV网络环境此方法与某一挑战回面。常用的数据包分析工具，类似Wireshark，一个自由和开放源信息包分析程序，可能不正确地解释OTV被封装的流量内容。因此费力应急方案，例如封装的数据的提取从OTV数据包的，通常要求顺利地执行数据分析。

OTV数据包格式

OTV封装由42个字节增加数据包的整体MTU大小。这是OTV边缘设备的操作的结果从原始第2层帧删除CRC和802.1Q字段并且添加OTV填充码(也包含VLAN和重叠ID信息)和外部IP报头。



在MPLS L2VPN解决方案，在衬底网络的设备没有正确地解码足够的信息MPLS数据包有效负载。一般，这不是问题，因为在MPLS核心网络的信息包转发执行根据标签，因此MPLS数据包内容的一详细分析在衬底网络的没有要求。

然而这提出一挑战OTV数据包数据分析是否为排除故障并且/或者监控目的要求。

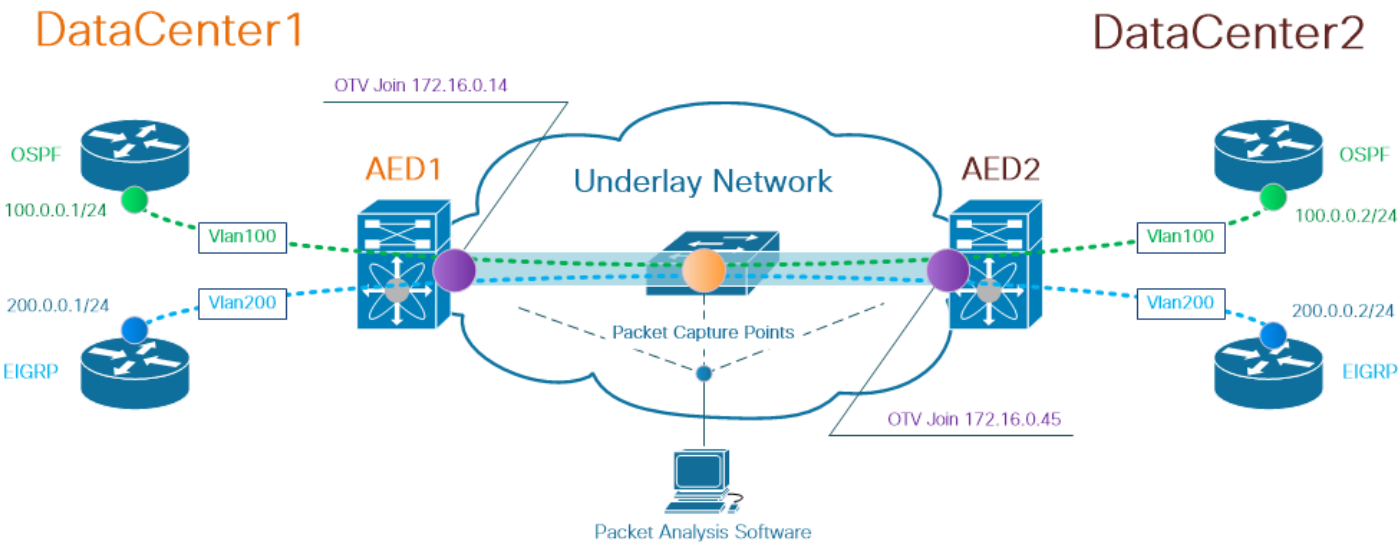
数据包分析工具，例如Wireshark，尝试解码通过应用正常MPLS数据包解析规则跟随MPLS报头的数据包数据。然而，因为它可能没有关于控制字协商结果的信息，通常将进行在MPLS L2VPN首端和尾端路由器之间，数据包分析工具落回到默认解析行为并且应用它对跟随MPLS报头的数据包数据。

> **Note**:在MPLS L2VPN解决方案，例如在MPLS (原子)的所有传输， pseudowire终端协商使用控制字参数。 控制字是一个可选4字节字段查找在MPLS标签栈和Layer2有效负载之间在pseudowire数据包。控制字传播通用的和Layer2有效负载特定信息。如果C位设置到1，广播服务商边缘盼望控制字是存在发信号的pseudowire的每pseudowire数据包。如果C位设置到0，控制字没有预计存在。

结果，解析行为的默认Wireshark可能不解释OTV数据包内容正确地，因而更加复杂OTV网络进行的故障排除流程。

拓扑

下列是简单OTV网络的网络图。VLAN 100和VLAN 200建立的路由器在两DataCenters、DataCenter1和DataCenter2之间的OSPF和EIGRP邻接，分别。数据中心互连(DCI)用在N7k交换机，表示在图表作为AED1和AED2之间的OTV通道实现。



Note: 思科OTV解决方案使用授权边缘设备(AED)角色的概念，分配到在特定的站点封装并且解封装OTV流量的网络设备。

在隧道解决方案经常看到的挑战是验证特定类型重叠数据包(IGP、FHRP等等)是否使它到在衬底网络的某些点。OSPF和EIGRP使用得重叠流量为例。

数据包捕获

有多种方式执行数据包捕获在网络。一个选项是使用思科交换端口分析器(SPAN)功能、联机在思科Catalyst和思科连结交换平台。

作为故障排除流程一部分，多点的数据包捕获可能需要执行。OTV加入接口和接口在衬底网络可以使用作为SPAN数据包捕获点。

解决方案

Wireshark默认解析引擎可能曲解OTV被封装的重叠数据包的最初的少数字节，好象他们Pseudowire仿真边缘对边缘(PWE3)控制字的部分，典型地用于在MPLS分组交换网络的MPLS L2VPNs。

Note:MPLS Pseudowire仿真边缘对边缘(PWE3)控制字被称为在其余的*控制字*本文。

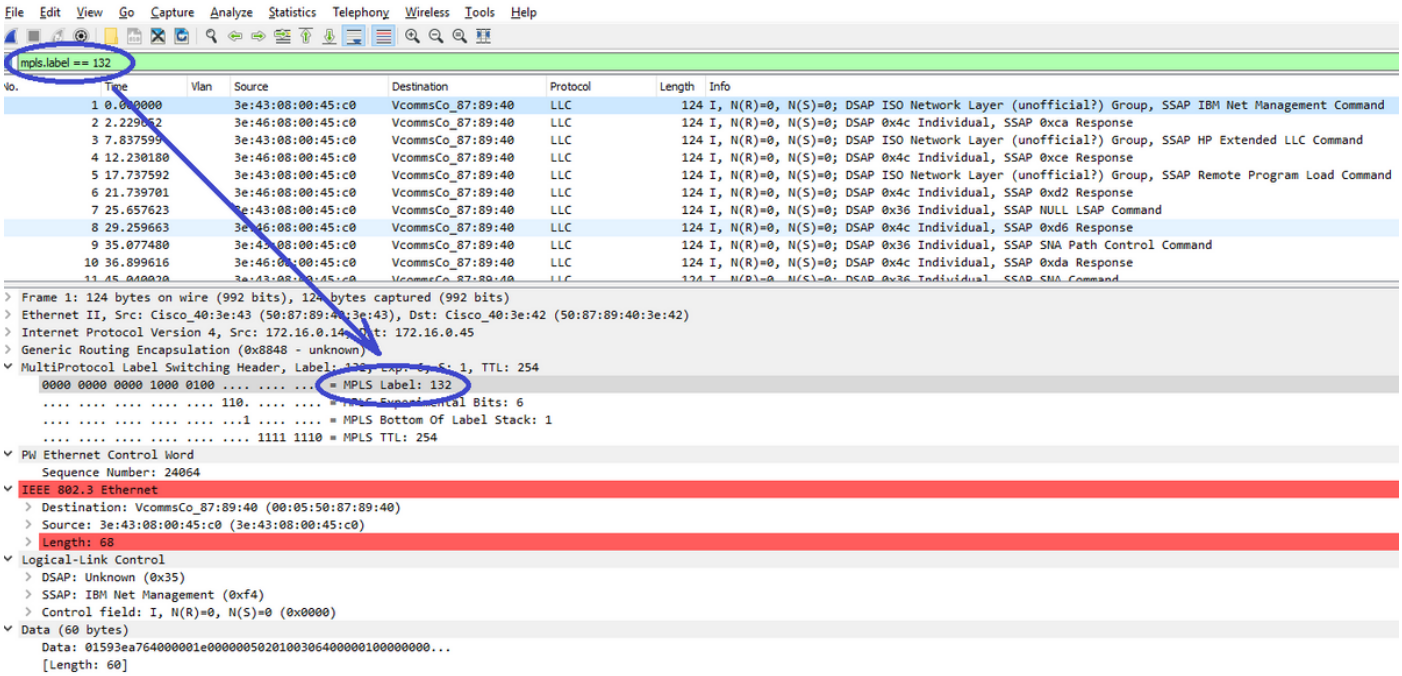
要保证Wireshark数据包分析工具正确地解释OTV被封装的数据包内容，手工的调整对数据包解码进程是需要的。

Note:用于OTV报头的MPLS标签等于重叠VLAN号+ 32。

在VLAN 100的解码数据包

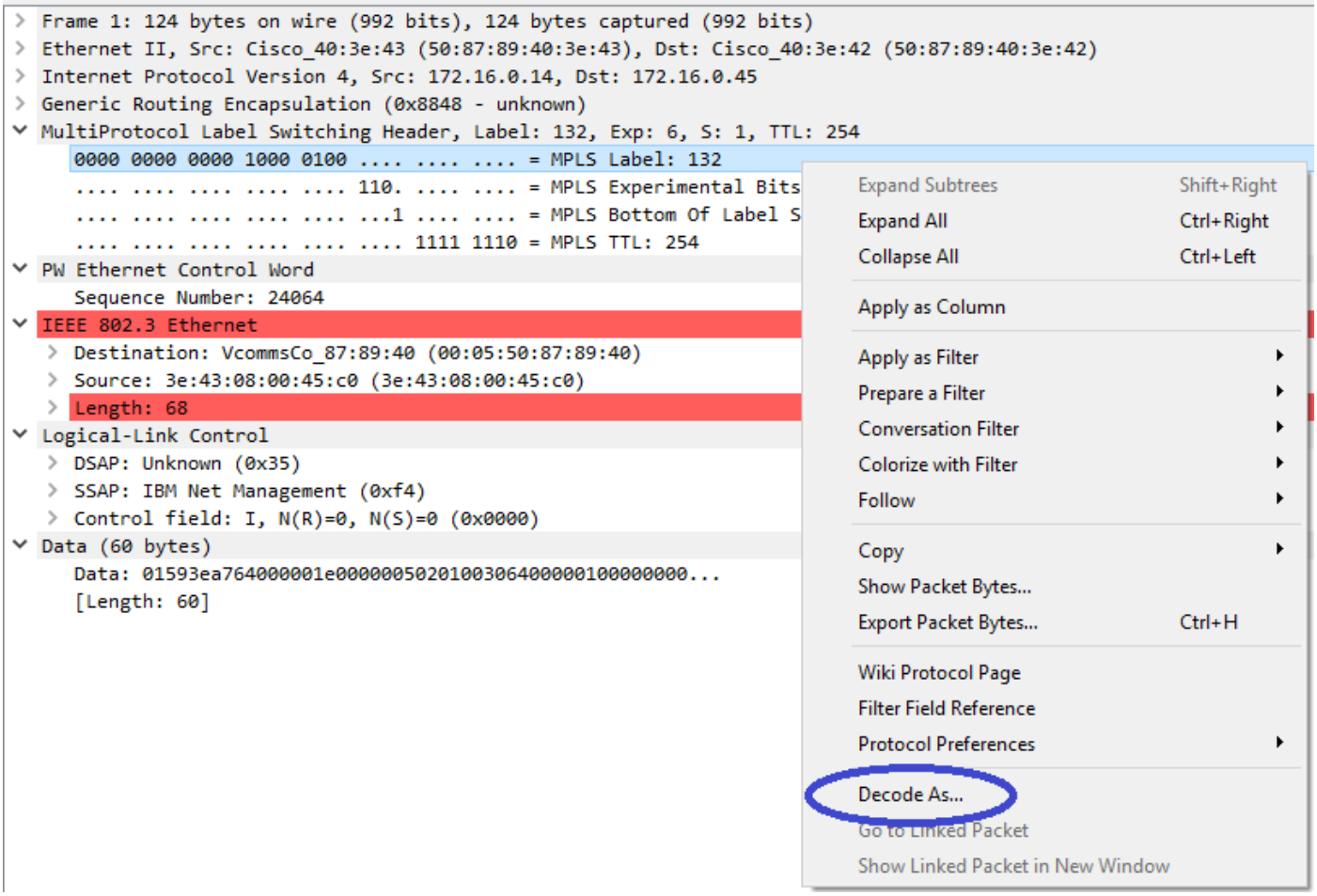
首先解码进程，请显示运载OTV已扩展VLAN 100内容仅的OTV被封装的数据包。使用的过滤器是mpls.label == 132，代表VLAN 100。

Note:要显示OTV封装在OTV被扩展的特定VLAN的数据包，使用以下Wireshark显示过滤器：mpls.label == <<vlan编号延伸在OTV> + 32>



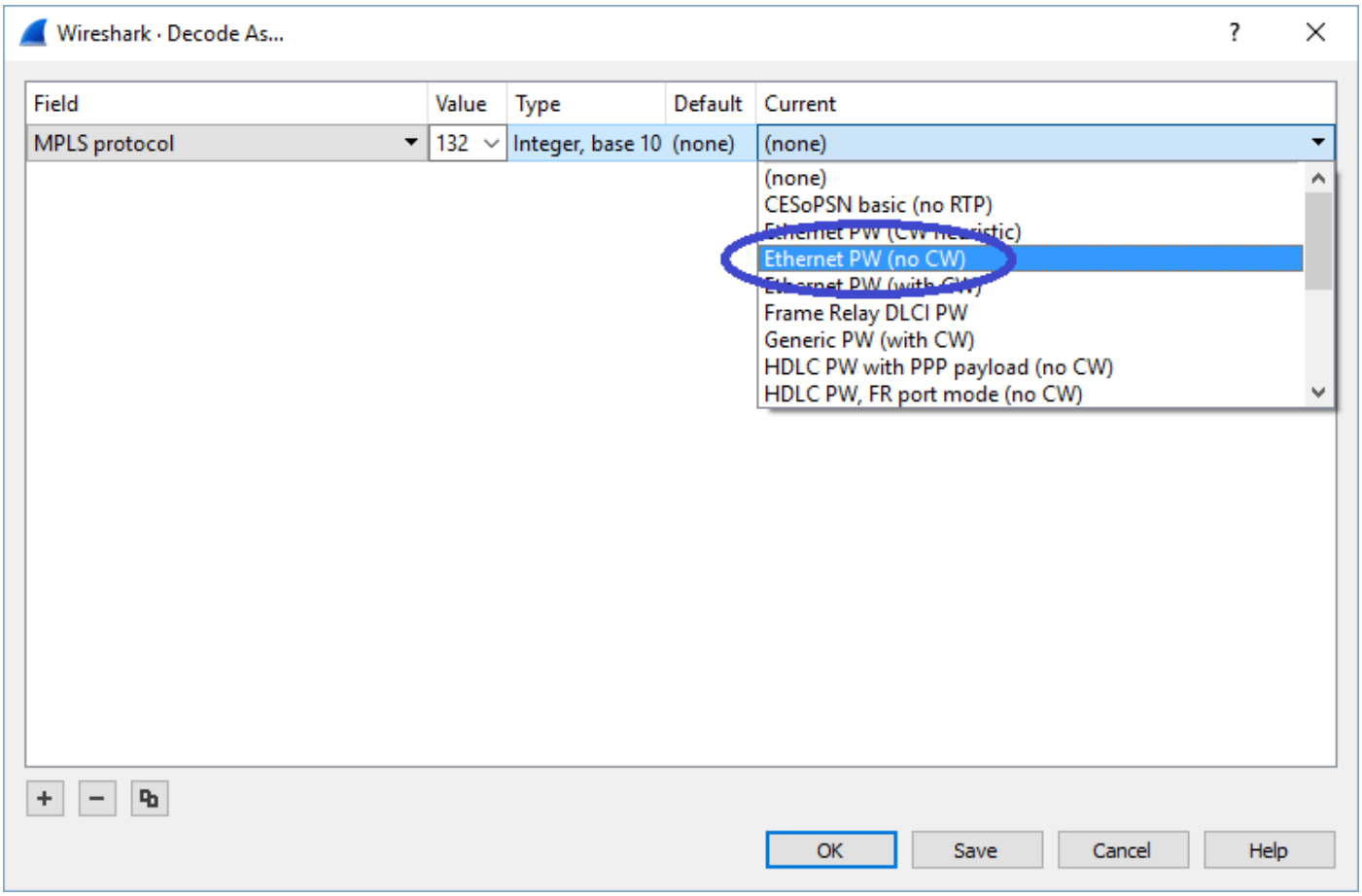
显示VLAN 100的OTV被封装的数据包，被扩展在OTV

默认情况下Wireshark解释MPLS L2VPN数据包内容的前四个字节作为控制字。这需要为OTV被封装的数据包被更正。要执行此，在的MPLS标签字段的右键单击任何数据包，和选择*解码作为*...选项。



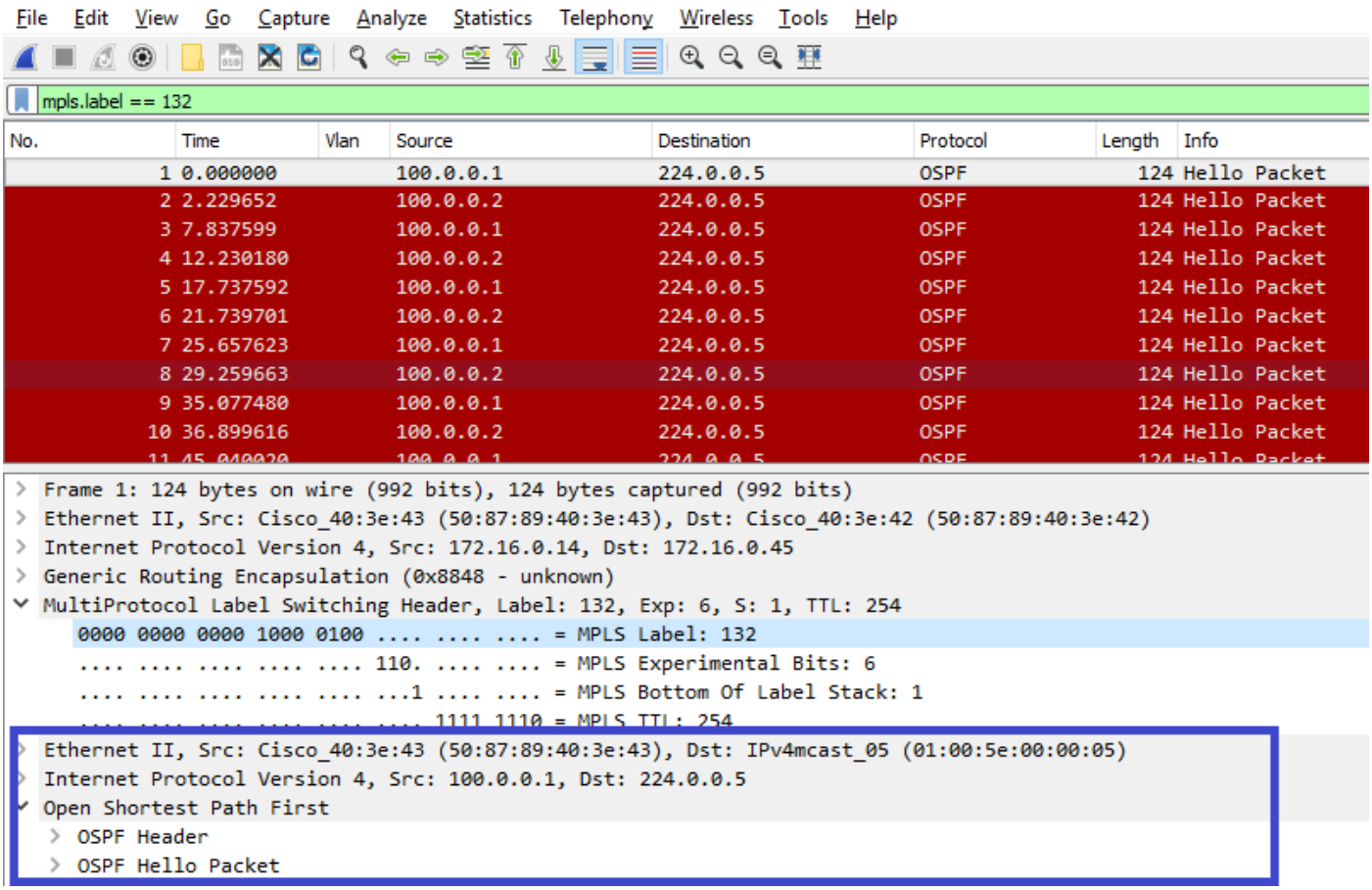
用鼠标右键单击在MPLS标签字段并且选择解码作为...选项

下一步是告诉Wireshark被封装的内容没有控制字。



选择"no CW"选项

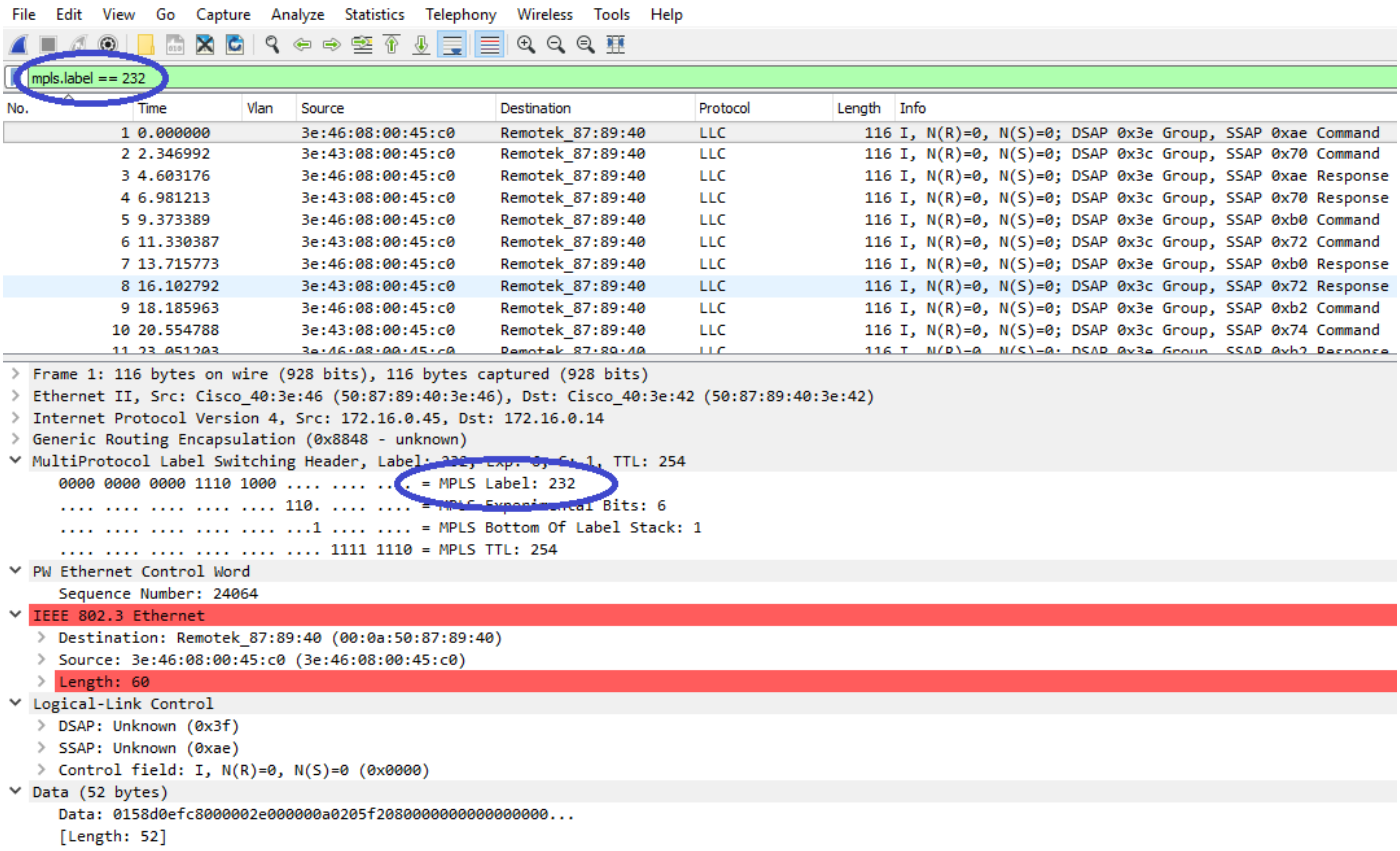
一旦此更改通过单击提交OK按钮， Wireshark分析工具将正确地显示OTV被封装的数据包内容。



正确Wireshark OTV被封装的数据包显示内容

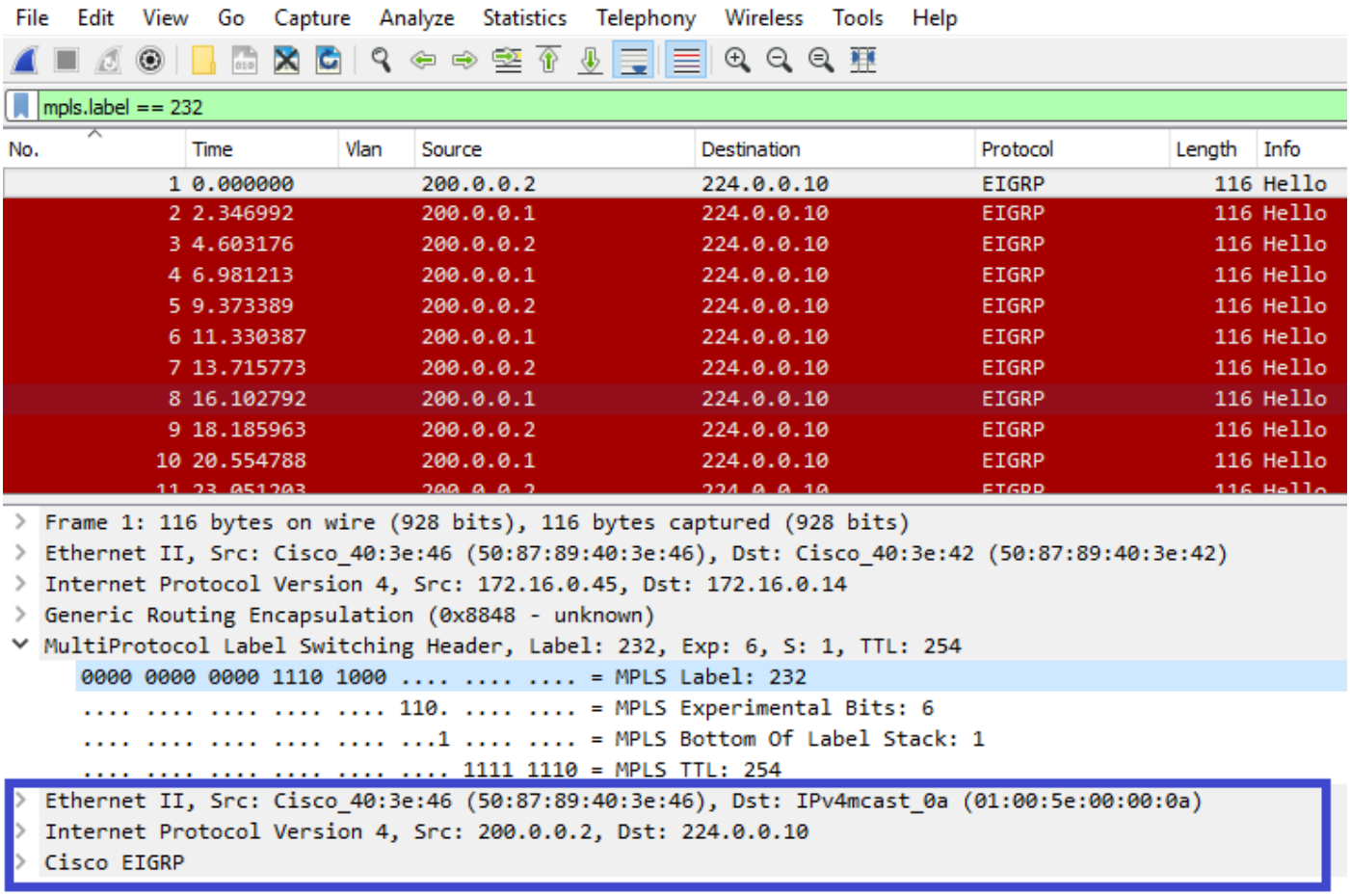
在VLAN 200的解码数据包

在步骤上为在OTV被扩展的所有VLAN请是可适用的。例如，使用显示Wireshark的过滤器仅数据包VLAN 200，我们在分析工具获得以下输出。



显示VLAN的200数据包，被扩展在OTV

一旦Wireshark被指示不解释MPLS数据包最初的少数字节作为PW控制字，请解码进程能成功地完成。



Wireshark正确地显示VLAN 200流量作为EIGRP数据包

请使用Editcap去除OTV报头

一般， Wireshark安装附有编辑工具呼叫的*Editcap的*line命令数据包。此工具能从获取数据包永久性删除OTV开销。这允许容易获取数据包显示和分析在Wireshark图形用户界面(GUI)的，不用需要手工调节Wireshark的解析行为。

运行在Windows平台的Editcap

默认情况下在Windows操作系统上， *editcap.exe*在c:\Program Files\Wireshark >目录安装。

运行此工具以-取消OTV开销和保存在.*pcap*文件的结果的*C*标志。

```
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>
```

运行在Mac OS平台的Editcap

在Mac OS操作系统上， editcap是可用的在/usr/local/bin文件夹。

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

通过删除OTV报头从获取数据包withEditcaptool，一个丢失作为MPLS报头一部分，编码，反过来是OTV填充码的零件的VLAN信息。切记使用‘mpls.label == <<vlan编号被扩展在OTV> + 32>' Wireshark GUI过滤器在删除与Editcaptool的OTV报头前，*如果仅流量分析特定VLAN要求。*

结论

排除故障思科OTV解决方案要求一好了解技术，从控制层面操作和数据层面封装方面。有效地应用知识，免费软件数据包分析工具例如Wireshark能证明非常强大在OTV数据包分析。除多种数据包显示选项之外，典型的Wireshark安装提供编辑能简化数据包分析的工具的数据包。这允许集中的故障排除在与特定的故障排除过程是最相关的数据包内容的部分。