使用Wireshark排除OTV解决方案故障

目录

简介
先决条件
要求
使用的组件
问题说明
OTV数据包格式
拓扑
数据包捕获
解决方案
解码VLAN 100中的数据包
解码VLAN 200中的数据包
使用Editcap删除OTV报头
在Windows平台上运行Editcap
在Mac OS平台上运行Editcap
结论

简介

本文档演示了Wireshark（一种众所周知的免费软件数据包捕获和分析工具）在排除Cisco OTV解决方案故障时的使用。

先决条件

要求

Cisco 建议您了解以下主题：

- Nexus系列交换机上的重叠传输虚拟化(OTV)
- 多协议标签交换(MPLS)第2层虚拟专用网络(VPN)基础知识
- Wireshark，免费的开源数据包分析器(https://www.wireshark.org)

使用的组件

本文档中的信息基于 Nexus 7000 系列交换机平台。

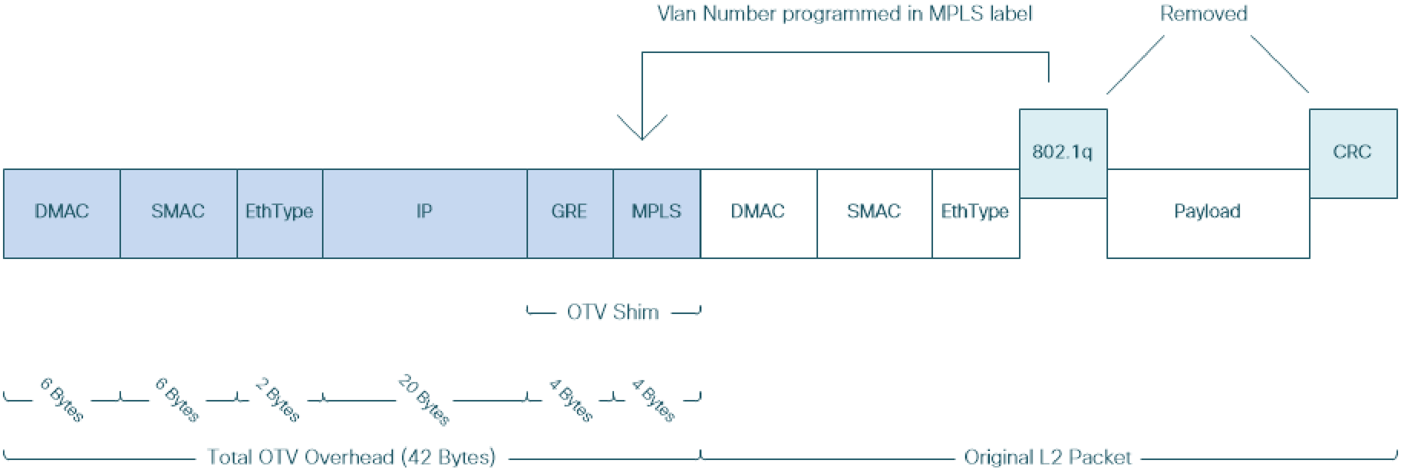
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题说明

在排除VPN环境中的网络故障时，其中一项技术涉及捕获和分析封装的数据包。但是，在Cisco OTV网络环境中，此方法遇到了一定挑战。常用的数据包分析工具，如Wireshark、 a 免费和开源数据包分析器， 可能无法正确解释OTV封装流量的内容。因此，通常需要费时的解决方法，例如从OTV数据包中提取封装的数据，才能成功执行数据分析。

OTV数据包格式

OTV封装将数据包的总MTU大小增加42字节。这是OTV边缘设备操作的结果，该设备从原始第2层帧中删除CRC和802.1Q字段，并添加OTV填充码（还包含VLAN和重叠ID信息）和外部IP报头。



在MPLS L2VPN解决方案中，底层网络中的设备没有足够的信息来正确解码MPLS数据包负载。通常，这不是问题，因为MPLS核心网络中的数据包转发是基于标签执行的，因此不需要深入分析底层网络中的MPLS数据包的内容。

但是，如果为了进行故障排除和/或监控目的而需要对OTV数据包进行数据分析，则这会带来挑战。

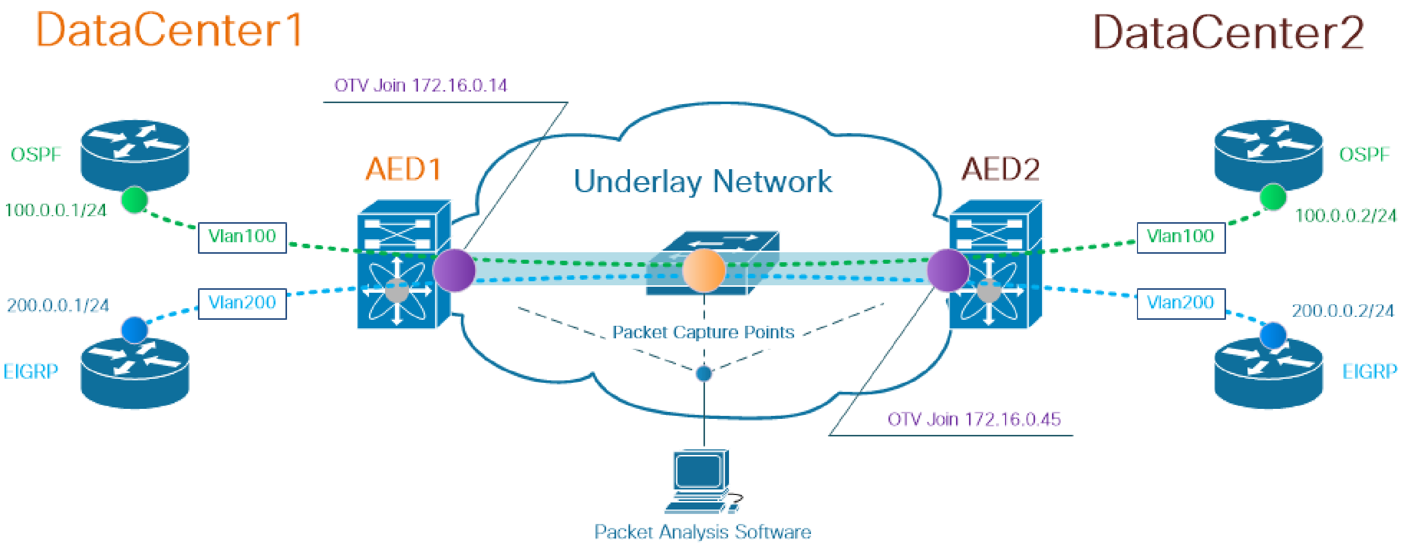
数据包分析工具（如Wireshark）尝试通过应用常规MPLS数据包解析规则来解码MPLS报头后面的数据包数据。但是，由于它可能没有有关控制字协商结果的信息，因此数据包分析工具会回退到默认解析行为并将其应用于MPLS报头之后的数据包数据。

> **注意**：在MPLS L2VPN解决方案(如MPLS上的任何传输(ATOM))中，伪线端点协商使用控制字参数。控制字是位于伪线数据包中MPLS标签堆栈和第2层负载之间的可选4字节字段。控制字传送通用信息和第2层负载特定信息。如果C位设置为1，则通告提供商边缘(PE)期望控制字存在于正在发出信号的伪线上的每个伪线数据包中。如果C位设置为0，则不会显示任何控制字。

因此，默认的Wireshark解析行为可能无法正确解释OTV数据包的内容，从而使OTV网络的故障排除过程更加复杂。

拓扑

以下是简单OTV网络的网络图。Vlan 100和Vlan 200中的路由器分别在两个数据中心（数据中心1和数据中心2）之间建立OSPF和EIGRP邻接关系。数据中心互联(DCI)在N7k交换机之间通过OTV隧道实现，如图所示为AED1和AED2。



> **注意**：Cisco OTV解决方案使用授权边缘设备(AED)角色的概念，该角色分配给网络设备，用于封装和解封特定站点的OTV流量。

隧道解决方案中经常遇到的挑战是验证特定类型的重叠数据包（IGP、FHRP等）是否使其到达底层网络中的特定点。OSPF和EIGRP重叠流量就是一个示例。

数据包捕获

在网络中执行数据包捕获有多种方法。一个选项是使用思科交换端口分析器(SPAN)功能，该功能可在Cisco Catalyst和Cisco Nexus交换平台上使用。

在故障排除过程中，可能需要执行多个点的数据包捕获。底层网络中的OTV加入接口和接口可用作SPAN数据包捕获点。

解决方案

Wireshark默认解析引擎可能会误解OTV封装的重叠数据包的前几个字节，就像它们是Pseudowire Emulation Edge-to-Edge(PWE3)Control Word的一部分一样,MPLS L2VPN通常在MPLS分组交换网络中使用。

> **注意**：MPLS伪线仿真边到边(PWE3)控制字在本文档*的*其余部分称为控制字。

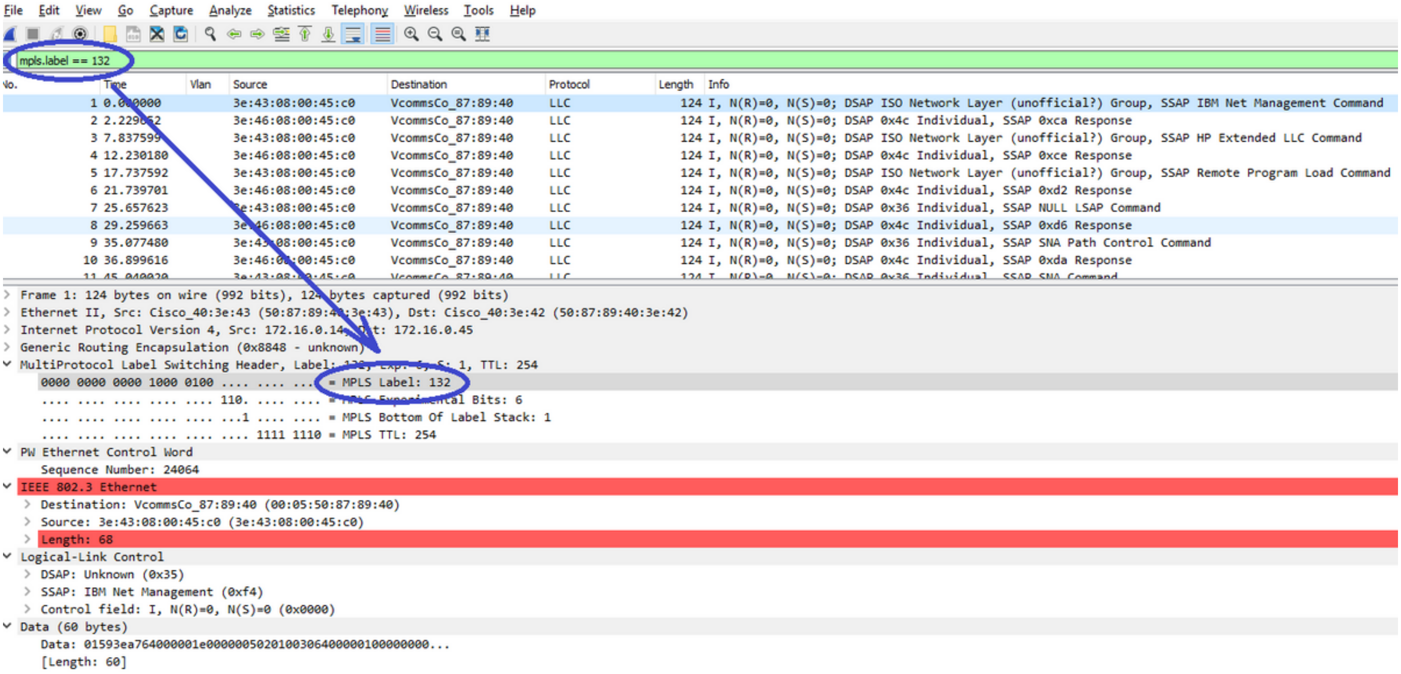
为了确保Wireshark数据包分析工具正确解释OTV封装数据包的内容，需要手动调整数据包解码过程。

> **注意**：OTV报头中使用的MPLS标签等于重叠VLAN编号+ 32。

解码VLAN 100中的数据包

作为解码过程的第一步，只显示承载OTV扩展VLAN 100内容的OTV封装数据包。使用的过滤器是mpls.label == 132，表示VLAN 100。

注意：要显示通过OTV扩展的特定VLAN的OTV封装数据包，请使用以下Wireshark显示过滤器：mpls.label == <<vlan number extended over OTV> + 32>


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

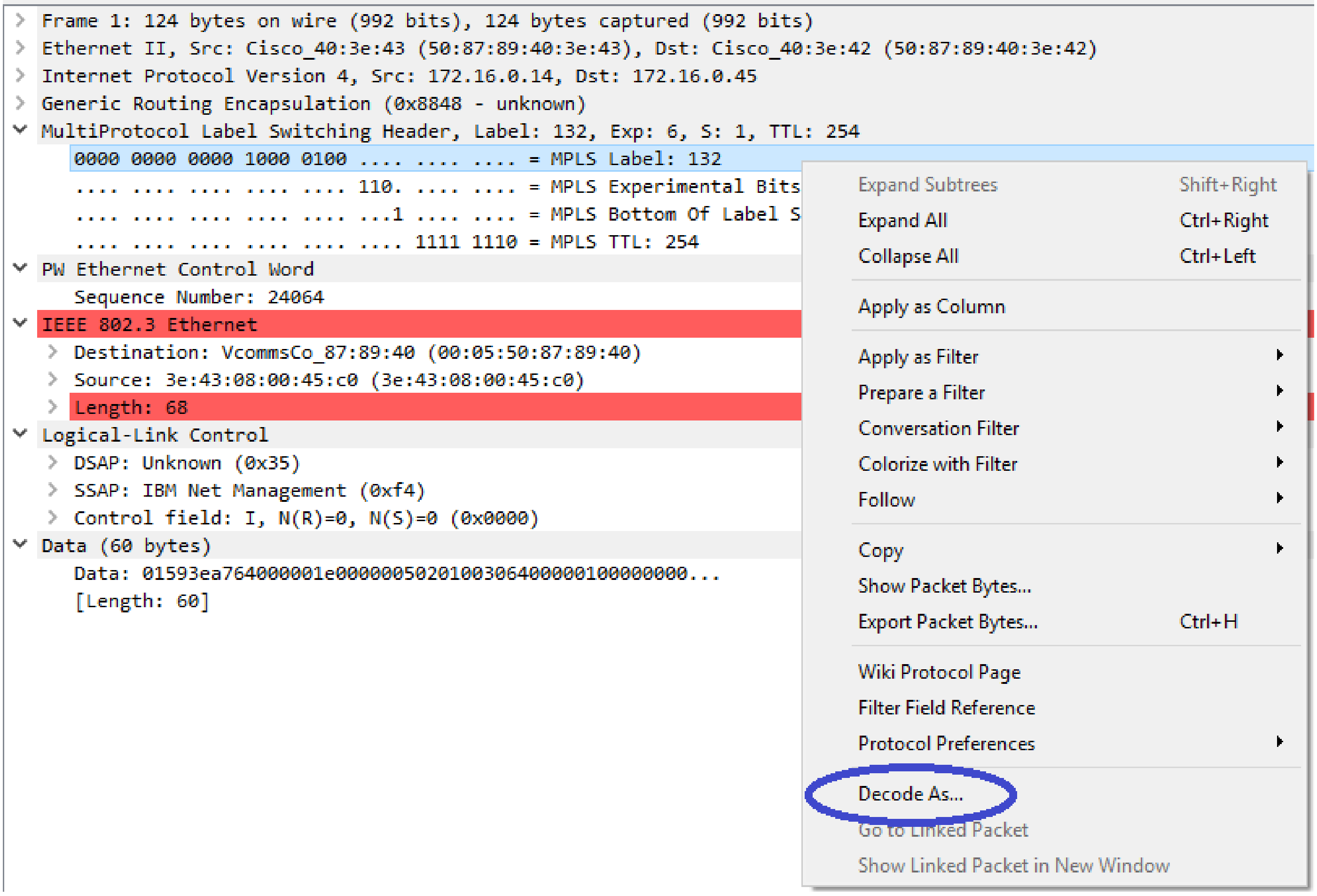
```
mpls.label == 132

No.  Time        Vlan  Source              Destination        Protocol  Length  Info
   1 0.000000          3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP IBM Net Management Command
   2 2.229652          3e:46:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xca Response
   3 7.837599          3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP HP Extended LLC Command
   4 12.230180         3e:46:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xce Response
   5 17.737592         3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP Remote Program Load Command
   6 21.739701         3e:46:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xd2 Response
   7 25.657623         3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x36 Individual, SSAP NULL LSAP Command
   8 29.259663         3e:46:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xd6 Response
   9 35.077480         3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x36 Individual, SSAP SNA Path Control Command
  10 36.899616         3e:46:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xda Response
  11 45.040020         3e:43:08:00:45:c0   VcommsCo_87:89:40  LLC       124 I, N(R)=0, N(S)=0; DSAP 0x36 Individual, SSAP SNA Command

> Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)
> Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45
> Generic Routing Encapsulation (0x8848 - unknown)
v MultiProtocol Label Switching Header, Label: 132, Exp: 6, S: 1, TTL: 254
    0000 0000 0000 1000 0100 .... .... .... = MPLS Label: 132
    .... .... .... .... .... 110. .... .... = MPLS Experimental Bits: 6
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
v PW Ethernet Control Word
    Sequence Number: 24064
v IEEE 802.3 Ethernet
  > Destination: VcommsCo_87:89:40 (00:05:50:87:89:40)
  > Source: 3e:43:08:00:45:c0 (3e:43:08:00:45:c0)
  > Length: 68
v Logical-Link Control
  > DSAP: Unknown (0x35)
  > SSAP: IBM Net Management (0xf4)
  > Control field: I, N(R)=0, N(S)=0 (0x0000)
v Data (60 bytes)
    Data: 01593ea764000001e00000050201003064000001000000000...
    [Length: 60]
```

显示OTV封装的Vlan 100数据包，通过OTV扩展

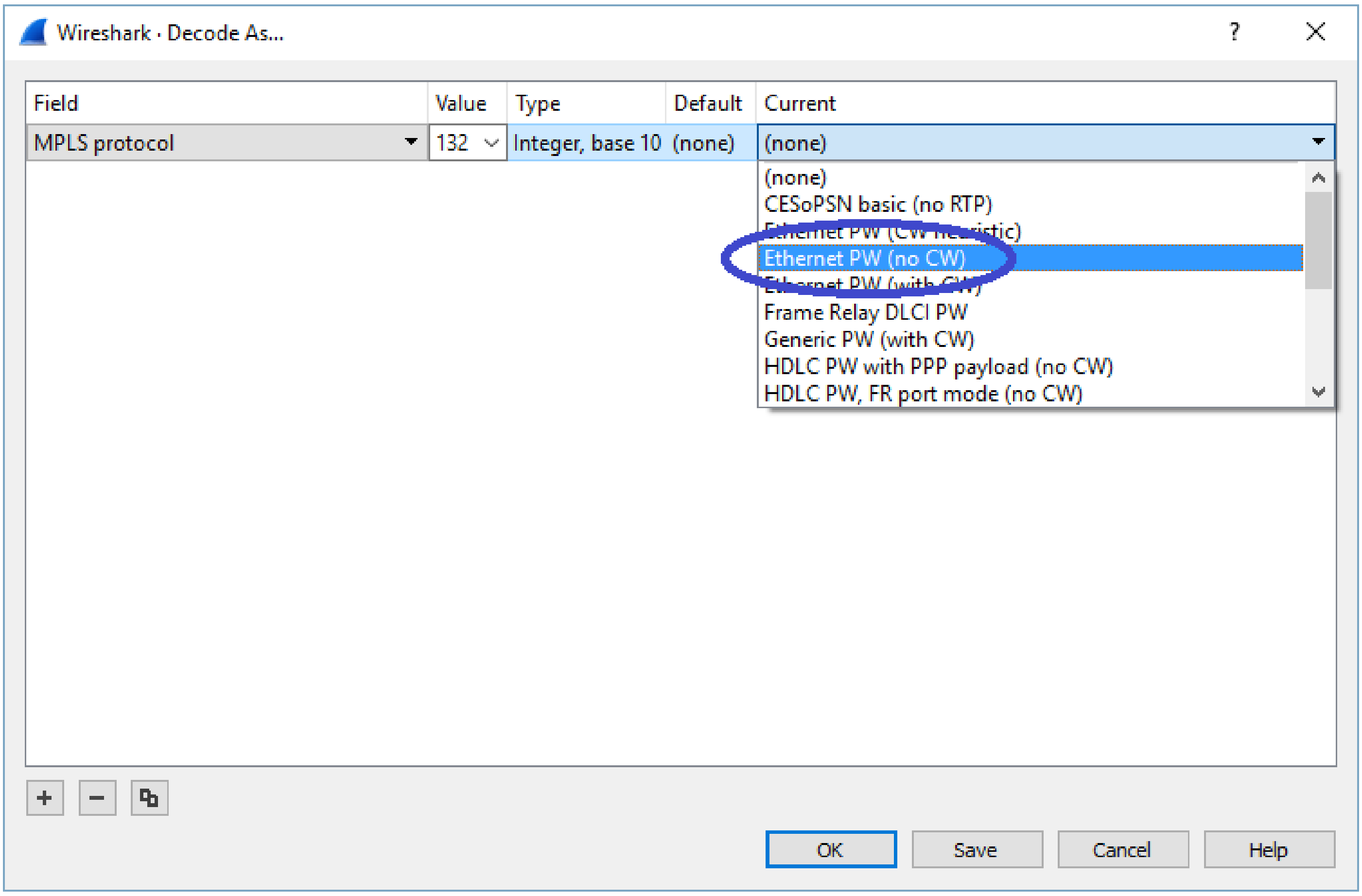
默认情况下，Wireshark将MPLS L2VPN数据包内容的前四个字节解释为控制字。这需要对OTV封装的数据包进行纠正。为此，请右键单击任何数据包的MPLS标签字段，然后选择“解码为……”(*Decode As...)* 选项.



```
> Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)
> Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45
> Generic Routing Encapsulation (0x8848 - unknown)
v MultiProtocol Label Switching Header, Label: 132, Exp: 6, S: 1, TTL: 254
    0000 0000 0000 1000 0100 .... .... .... = MPLS Label: 132
    .... .... .... .... .... 110. .... .... = MPLS Experimental Bits
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label S
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
v PW Ethernet Control Word
    Sequence Number: 24064
v IEEE 802.3 Ethernet
  > Destination: VcommsCo_87:89:40 (00:05:50:87:89:40)
  > Source: 3e:43:08:00:45:c0 (3e:43:08:00:45:c0)
  > Length: 68
v Logical-Link Control
  > DSAP: Unknown (0x35)
  > SSAP: IBM Net Management (0xf4)
  > Control field: I, N(R)=0, N(S)=0 (0x0000)
v Data (60 bytes)
    Data: 01593ea764000001e00000050201003064000001000000000...
    [Length: 60]
```

右键点击MPLS标签字段，然后选择解码为……选项

下一步是告诉Wireshark，封装的内容没有控制字。

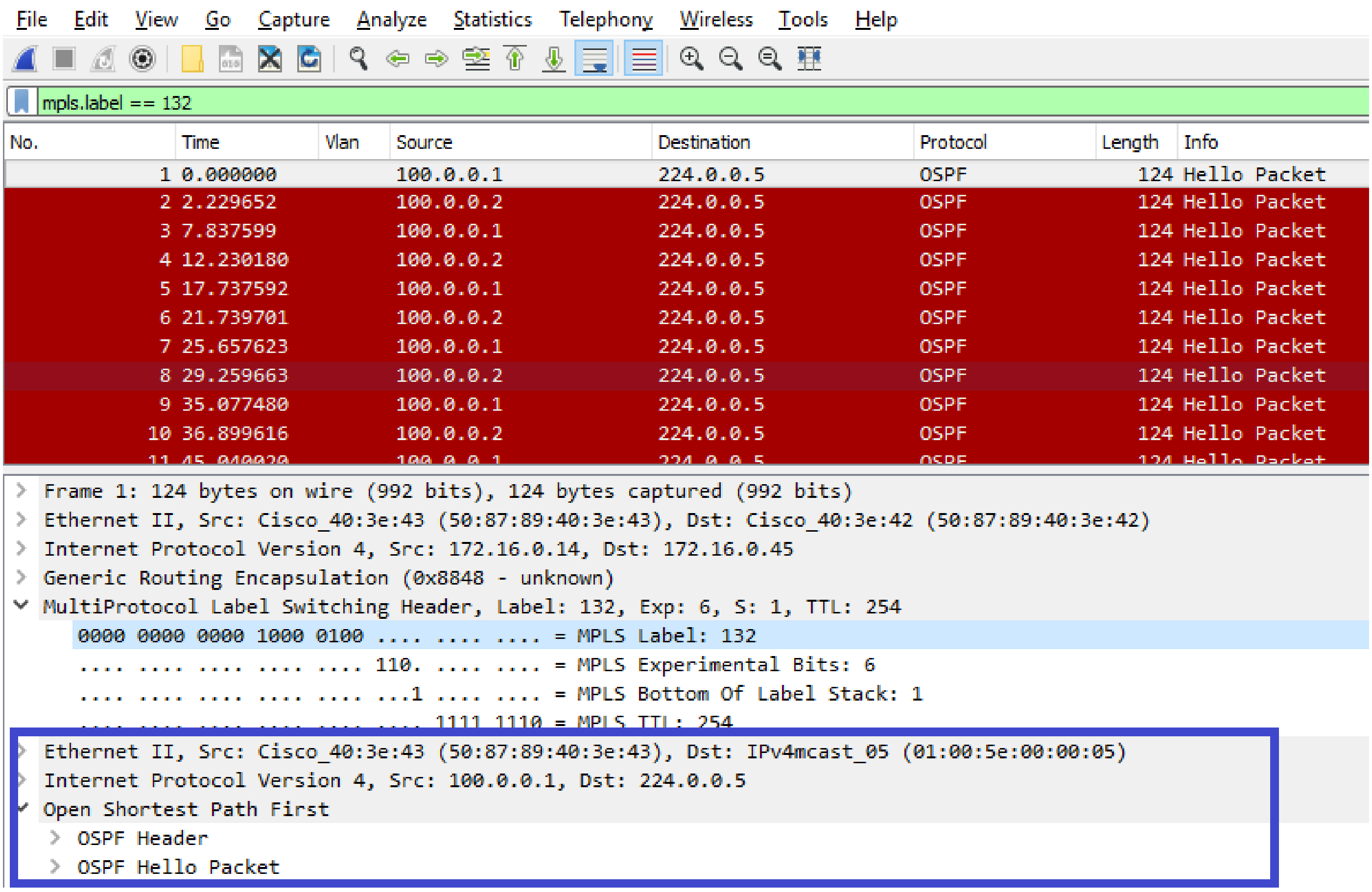


Field	Value	Type	Default	Current
MPLS protocol	132	Integer, base 10	(none)	(none)

(none)
CESoPSN basic (no RTP)
Ethernet PW (CW heuristic)
Ethernet PW (no CW)
Ethernet PW (with CW)
Frame Relay DLCI PW
Generic PW (with CW)
HDLC PW with PPP payload (no CW)
HDLC PW, FR port mode (no CW)

选择“无CW”选项

通过单击“确定”按钮提交此更改后，Wireshark分析工具将正确显示OTV封装数据包的内容。



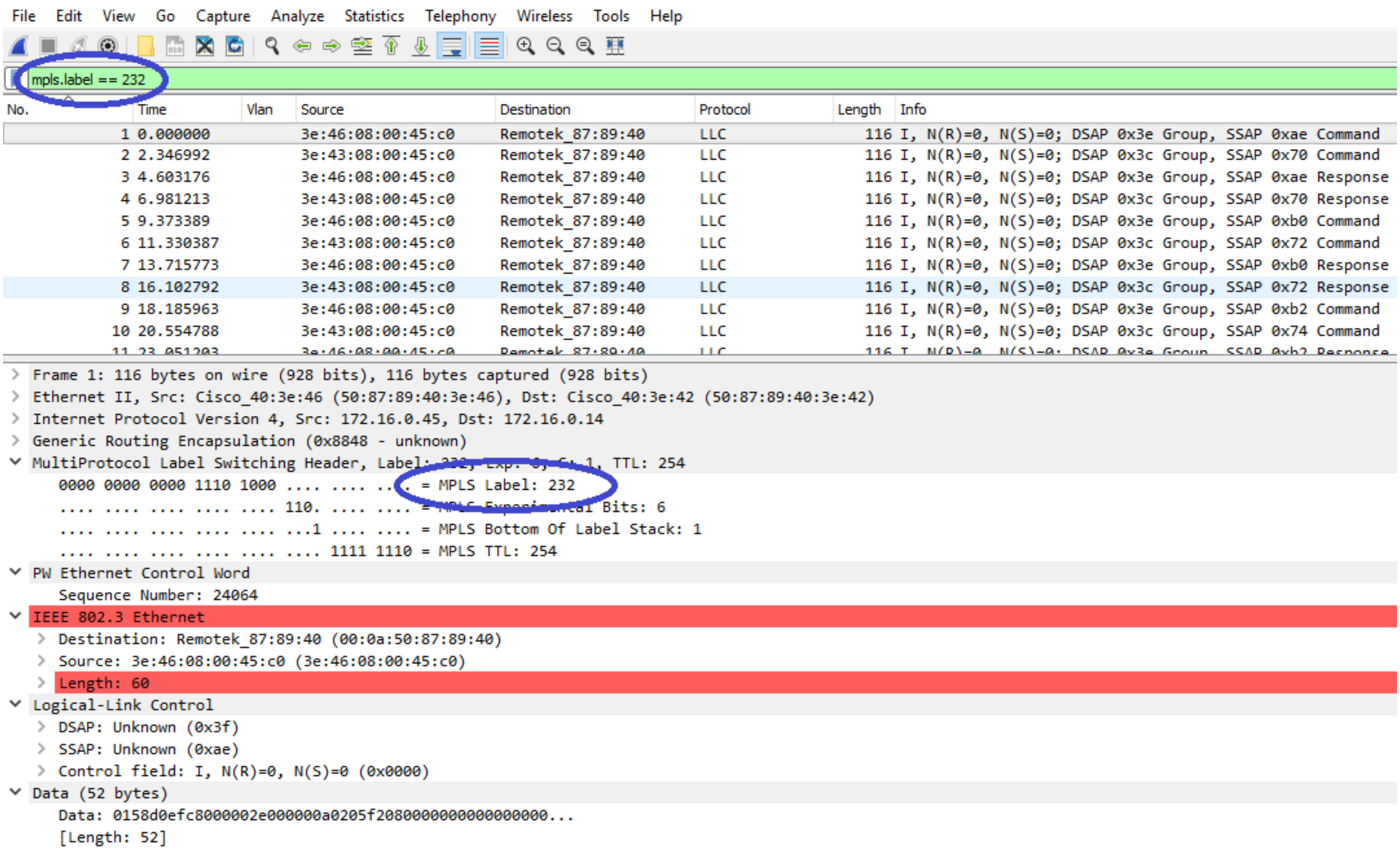
mpls.label == 132

No.	Time	Vlan	Source	Destination	Protocol	Length	Info
1	0.000000		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet
2	2.229652		100.0.0.2	224.0.0.5	OSPF	124	Hello Packet
3	7.837599		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet
4	12.230180		100.0.0.2	224.0.0.5	OSPF	124	Hello Packet
5	17.737592		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet
6	21.739701		100.0.0.2	224.0.0.5	OSPF	124	Hello Packet
7	25.657623		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet
8	29.259663		100.0.0.2	224.0.0.5	OSPF	124	Hello Packet
9	35.077480		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet
10	36.899616		100.0.0.2	224.0.0.5	OSPF	124	Hello Packet
11	45.040020		100.0.0.1	224.0.0.5	OSPF	124	Hello Packet

```
> Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)
> Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45
> Generic Routing Encapsulation (0x8848 - unknown)
v MultiProtocol Label Switching Header, Label: 132, Exp: 6, S: 1, TTL: 254
    0000 0000 0000 1000 0100 .... .... .... = MPLS Label: 132
    .... .... .... .... .... 110. .... .... = MPLS Experimental Bits: 6
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
> Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
> Internet Protocol Version 4, Src: 100.0.0.1, Dst: 224.0.0.5
v Open Shortest Path First
  > OSPF Header
  > OSPF Hello Packet
```

解码VLAN 200中的数据包

以上步骤适用于通过OTV扩展的任何vlan。例如，使用Wireshark过滤器仅显示vlan 200的数据包，我们在分析工具中得到以下输出。



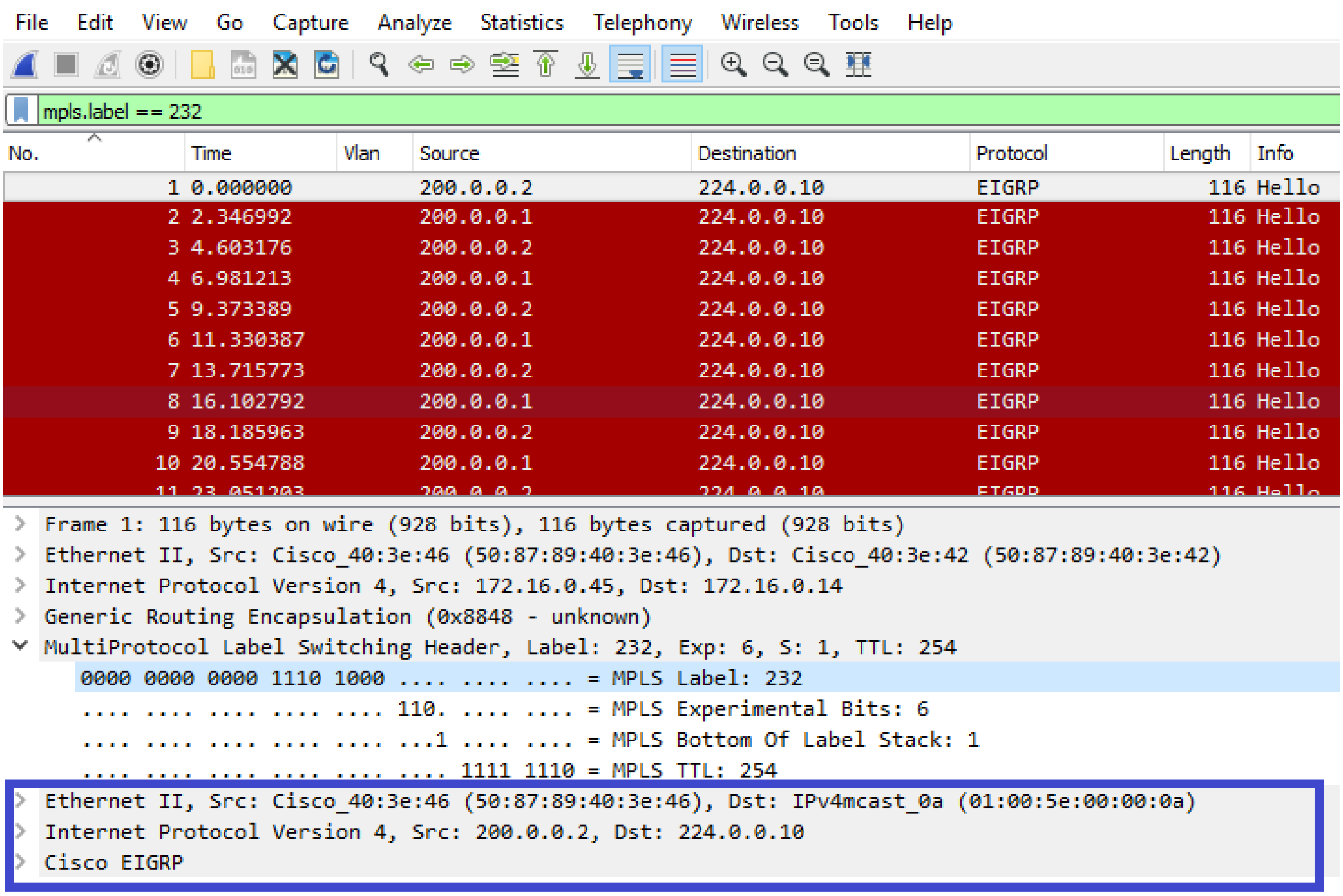
mpls.label == 232

```
No.    Time       Vlan  Source             Destination        Protocol  Length  Info
     1 0.000000         3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xae Command
     2 2.346992         3e:43:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x70 Command
     3 4.603176         3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xae Response
     4 6.981213         3e:43:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x70 Response
     5 9.373389         3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb0 Command
     6 11.330387        3e:43:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x72 Command
     7 13.715773        3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb0 Response
     8 16.102792        3e:43:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x72 Response
     9 18.185963        3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb2 Command
    10 20.554788        3e:43:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x74 Command
    11 23.051203        3e:46:08:00:45:c0  Remotek_87:89:40   LLC          116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb2 Response
```

```
> Frame 1: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Ethernet II, Src: Cisco_40:3e:46 (50:87:89:40:3e:46), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)
> Internet Protocol Version 4, Src: 172.16.0.45, Dst: 172.16.0.14
> Generic Routing Encapsulation (0x8848 - unknown)
v MultiProtocol Label Switching Header, Label: 232, Exp: 6, S: 1, TTL: 254
    0000 0000 0000 1110 1000 .... .... .... = MPLS Label: 232
    .... .... .... .... .... 110. .... .... = MPLS Experimental Bits: 6
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
v PW Ethernet Control Word
    Sequence Number: 24064
v IEEE 802.3 Ethernet
  > Destination: Remotek_87:89:40 (00:0a:50:87:89:40)
  > Source: 3e:46:08:00:45:c0 (3e:46:08:00:45:c0)
  > Length: 60
v Logical-Link Control
  > DSAP: Unknown (0x3f)
  > SSAP: Unknown (0xae)
  > Control field: I, N(R)=0, N(S)=0 (0x0000)
v Data (52 bytes)
    Data: 0158d0efc8000002e000000a0205f2080000000000000000...
    [Length: 52]
```

显示OTV上扩展的VLAN 200的数据包

一旦Wireshark被指示不将MPLS数据包的前几个字节解释为PW控制字，解码过程就可以成功完成。



mpls.label == 232

No.	Time	Vlan	Source	Destination	Protocol	Length	Info
1	0.000000		200.0.0.2	224.0.0.10	EIGRP	116	Hello
2	2.346992		200.0.0.1	224.0.0.10	EIGRP	116	Hello
3	4.603176		200.0.0.2	224.0.0.10	EIGRP	116	Hello
4	6.981213		200.0.0.1	224.0.0.10	EIGRP	116	Hello
5	9.373389		200.0.0.2	224.0.0.10	EIGRP	116	Hello
6	11.330387		200.0.0.1	224.0.0.10	EIGRP	116	Hello
7	13.715773		200.0.0.2	224.0.0.10	EIGRP	116	Hello
8	16.102792		200.0.0.1	224.0.0.10	EIGRP	116	Hello
9	18.185963		200.0.0.2	224.0.0.10	EIGRP	116	Hello
10	20.554788		200.0.0.1	224.0.0.10	EIGRP	116	Hello
11	23.051203		200.0.0.2	224.0.0.10	EIGRP	116	Hello

```
> Frame 1: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Ethernet II, Src: Cisco_40:3e:46 (50:87:89:40:3e:46), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)
> Internet Protocol Version 4, Src: 172.16.0.45, Dst: 172.16.0.14
> Generic Routing Encapsulation (0x8848 - unknown)
v MultiProtocol Label Switching Header, Label: 232, Exp: 6, S: 1, TTL: 254
      0000 0000 0000 1110 1000 .... .... .... = MPLS Label: 232
      .... .... .... .... .... 110. .... .... = MPLS Experimental Bits: 6
      .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
      .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
> Ethernet II, Src: Cisco_40:3e:46 (50:87:89:40:3e:46), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
> Internet Protocol Version 4, Src: 200.0.0.2, Dst: 224.0.0.10
> Cisco EIGRP
```

WIreshark将Vlan 200流量正确显示为EIGRP数据包

使用Editcap删除OTV报头

通常，Wireshark安装附带一个名为Editcap的命令行数据包编辑*工具*。此工具可永久消除捕获数据包的OTV开销。这样，在Wireshark图形用户界面(GUI)中可以轻松显示和分析捕获的数据包，而无需手动调整Wireshark的解析行为。

在Windows平台上运行Editcap

在Windows操作系统上，*editcap.exe*默认安装在c:\Program Files\Wireshark>目录中。

使用 — C标志运行此工具以删除OTV开销并将结果保存*到.pcap*文件。

```
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平台上运行Editcap

在Mac OS操作系统上，editcap位于/usr/local/bin文件夹中。

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

通过从捕获的数据包中删除OTV报头，*编辑*工具，丢失作为MPLS报头一部分编码的VLAN信息，而MPLS报头又是OTV填充码的一部分。如果仅需要分析特定Vlan的流量，请记住在使用*Editcap*工具删除OTV报头之前，使用“mpls.label == <<vlan number extended over OTV> + 32>” Wireshark GUI过滤器。

结论

对Cisco OTV解决方案进行故障排除需要从控制平面操作和数据平面封装角度充分了解该技术。Wireshark等免费软件数据包分析工具可以有效地应用知识，在OTV数据包分析中证明非常强大。除了各种数据包显示选项外，典型的Wireshark安装还提供了数据包编辑工具，可简化数据包分析。这样，故障排除就可以专注于与特定故障排除会话最相关的数据包内容部分。