

Usar o Wireshark para Solucionar Problemas de Soluções OTV

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descrição do problema](#)

[Formato de pacote OTV](#)

[Topologia](#)

[Captura do pacote](#)

[Solução](#)

[Decodificar pacotes na VLAN 100](#)

[Decodificar pacotes na VLAN 200](#)

[Usar Editcap para remover o cabeçalho OTV](#)

[Executar Editcap na Plataforma Windows](#)

[Execute a Editcap na plataforma Mac OS](#)

[Conclusão](#)

Introduction

Este documento demonstra o uso do Wireshark, uma ferramenta de análise e captura de pacotes freeware bem conhecida, na solução de problemas do Cisco OTV.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Overlay Transport Virtualization (OTV) em switches Nexus Series
- Conceitos básicos de VPNs (Virtual Private Networks, Redes virtuais privadas) de camada 2 de MPLS (Multiprotocol Label Switching)
- Wireshark, um analisador de pacotes de código aberto e livre (<https://www.wireshark.org>)

Componentes Utilizados

As informações neste documento são baseadas na plataforma do Nexus 7000 Series Switch.

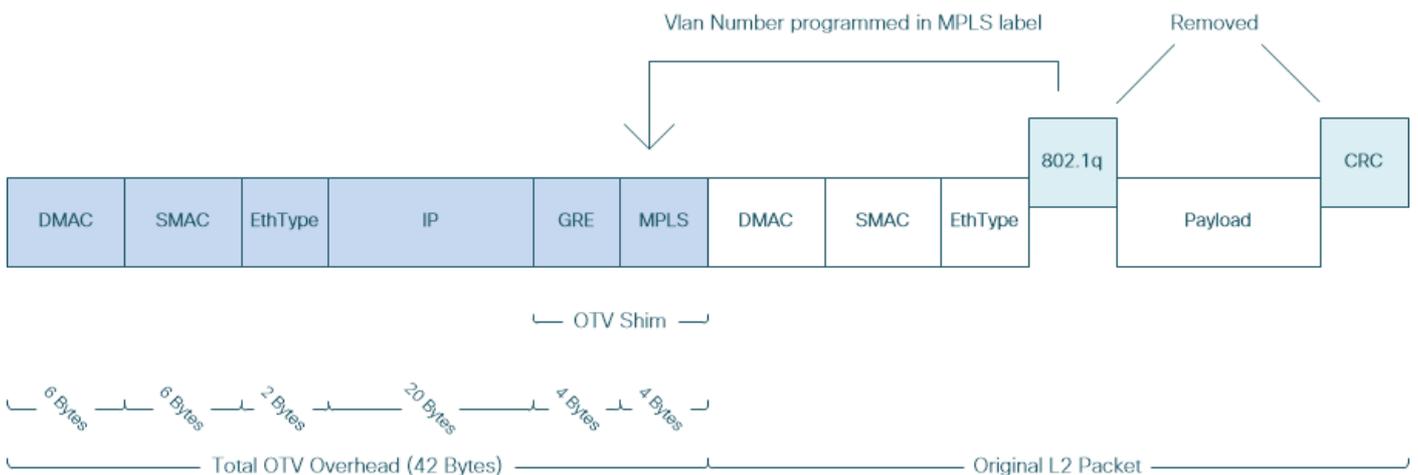
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Descrição do problema

Ao Troubleshoot problemas de rede em ambientes VPN, uma das técnicas envolve a captura e a análise de pacotes encapsulados. No entanto, em ambientes de rede Cisco OTV, essa abordagem é enfrentada com um certo desafio. As ferramentas de análise de pacotes mais usadas, como o Wireshark, a analisador de pacotes de código aberto e livre, pode não interpretar corretamente o conteúdo do tráfego encapsulado de OTV. Dessa forma, soluções laboriosas, como a extração de dados encapsulados de um pacote OTV, geralmente são necessárias para executar com sucesso a análise de dados.

Formato de pacote OTV

O encapsulamento de OTV aumenta o tamanho total de MTU do pacote em 42 bytes. Esse é o resultado da operação do dispositivo de borda de OTV que remove os campos CRC e 802.1Q do quadro original da Camada 2 e adiciona um cabeçalho OTV (contendo também informações de VLAN e de ID de sobreposição) e um cabeçalho IP externo.



Nas soluções L2VPN MPLS, os dispositivos na rede subjacente não têm informações suficientes para decodificar corretamente o payload do pacote MPLS. Normalmente, isso não é um problema, pois o encaminhamento de pacotes em uma rede central MPLS é realizado com base em rótulos, portanto, não é necessária uma análise detalhada do conteúdo dos pacotes MPLS na rede de base.

No entanto, isso apresenta um desafio se a análise de dados de pacotes OTV for necessária para fins de solução de problemas e/ou monitoramento.

Ferramentas de análise de pacotes, como o Wireshark, tentam decodificar dados de pacote que seguem o cabeçalho MPLS aplicando regras de análise de pacote MPLS regulares. No entanto, como ele pode não ter informações sobre os resultados da negociação do Control Word, que normalmente seria executada entre os roteadores de front-end de L2VPN MPLS e de fim da rede, as ferramentas de análise de pacote retornam ao comportamento de análise padrão e o aplicam aos dados de pacote que seguem o cabeçalho MPLS.

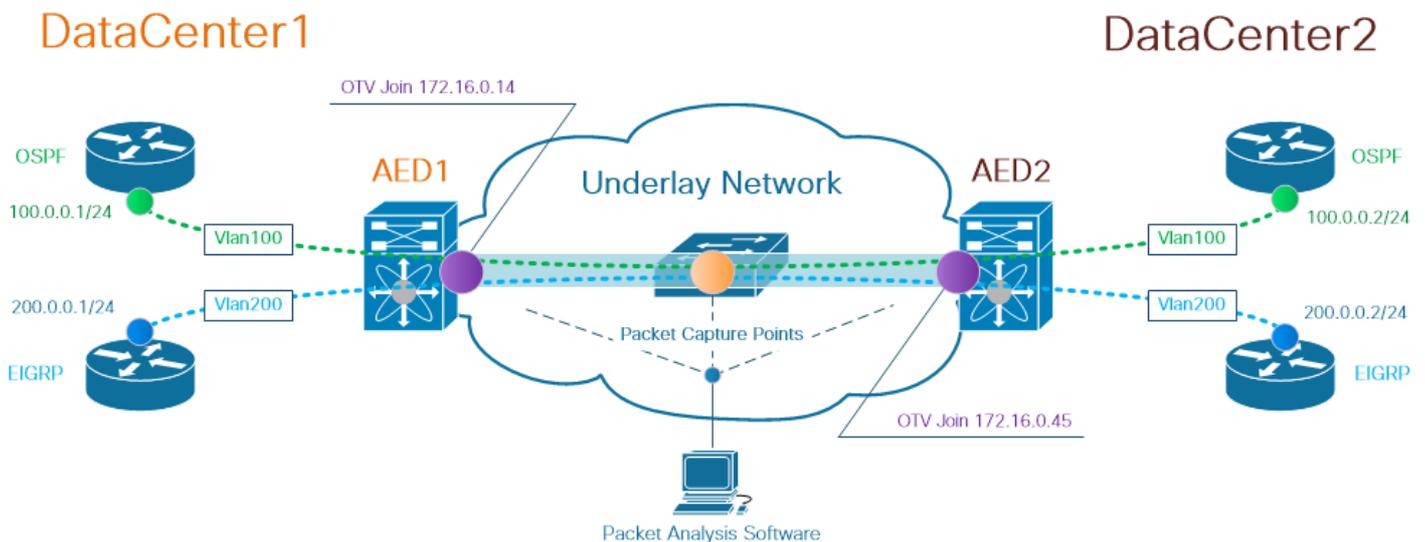
Note: Em soluções L2VPN MPLS, como Any Transport Over MPLS (ATOM), terminais pseudowire negociam o uso do parâmetro Control Word. Uma palavra de controle é um campo opcional de 4 bytes localizado entre a pilha de rótulos MPLS e o payload da Camada

2 no pacote pseudowire. A palavra de controle transporta informações genéricas e específicas de payload da Camada 2. Se o bit C estiver definido como 1, o borda do provedor de publicidade (PE) espera que a palavra de controle esteja presente em cada pacote de pseudônimo no pseudônimo que está sendo sinalizado. Se o bit C for definido como 0, nenhuma palavra de controle será esperada.

Como resultado, o comportamento padrão de análise do Wireshark pode não interpretar corretamente o conteúdo dos pacotes OTV, tornando o processo de solução de problemas da rede OTV mais complexo.

Topologia

A seguir está um diagrama de rede de uma rede OTV simples. Os roteadores na Vlan 100 e na Vlan 200 estabelecem adjacências de OSPF e EIGRP entre dois Data Centers, DataCenter1 e DataCenter2, respectivamente. A interconexão de data center (DCI) é implementada com túnel OTV entre switches N7k, mostrada no diagrama como AED1 e AED2.



Observação: a solução Cisco OTV usa o conceito da função de dispositivo de borda autoritativo (AED), atribuída ao dispositivo de rede que encapsula e desencapsula o tráfego de OTV em um site específico.

O desafio frequentemente visto nas soluções de tunelamento é verificar se um tipo específico de pacotes de sobreposição (IGP, FHRP, etc.) o faz chegar a certos pontos na rede de sobreposição. O tráfego de sobreposição OSPF e EIGRP é usado como exemplo.

Captura do pacote

Há várias maneiras de executar uma captura de pacotes na rede. Uma opção é usar o recurso Cisco Switched Port Analyzer (SPAN), disponível nas plataformas de switching Cisco Catalyst e Cisco Nexus.

Como parte do processo de solução de problemas, as capturas de pacotes em vários pontos podem precisar ser realizadas. As interfaces e interfaces OTV Join na rede de base podem ser usadas como ponto de captura de pacotes SPAN.

Solução

O mecanismo de análise padrão do Wireshark pode interpretar incorretamente os primeiros bytes de pacotes de sobreposição encapsulados de OTV como se eles fizessem parte do Pseudowire Emulation Edge-to-Edge (PWE3) Control Word, que é tipicamente usado em L2VPNs de MPLS sobre uma rede comutada de pacotes MPLS.

Note: A palavra de controle de Emulação de Pseudowire Edge-to-Edge (PWE3) MPLS é chamada de *palavra de controle* no restante deste documento.

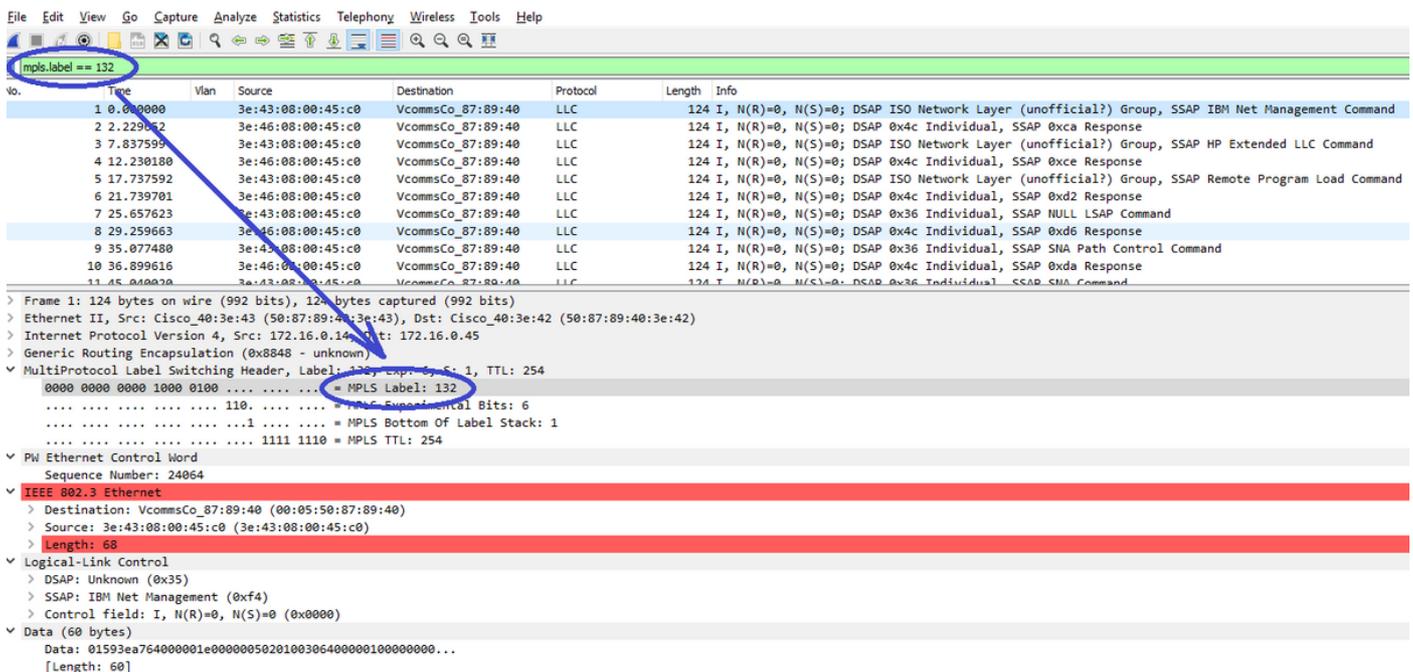
Para garantir que a ferramenta de análise de pacotes Wireshark interprete corretamente o conteúdo dos pacotes encapsulados de OTV, é necessário ajuste manual no processo de decodificação de pacotes.

Note: O rótulo MPLS usado no cabeçalho OTV é igual ao número da vlan sobreposta + 32.

Decodificar pacotes na VLAN 100

Como primeira etapa do processo de decodificação, exiba somente pacotes encapsulados de OTV que transportam conteúdo da vlan 100 estendida de OTV. O filtro usado é `mpls.label == 132`, que representa a vlan 100.

Note: Para exibir pacotes encapsulados de OTV para uma vlan específica estendida sobre OTV, use o seguinte filtro de exibição do Wireshark: `mpls.label == <<vlan number extended over OTV> + 32`



The screenshot shows the Wireshark interface with the filter `mpls.label == 132` applied. The packet list pane shows several packets, with the first one selected. The packet details pane shows the following structure:

- 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)
- MultiProtocol Label Switching Header, Label: 132, Exp: 0, 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
- PW Ethernet Control Word
 - Sequence Number: 24064
- 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
- Logical-Link Control
 - DSAP: Unknown (0x35)
 - SSAP: IBM Net Management (0xf4)
 - Control field: I, N(R)=0, N(S)=0 (0x0000)
- Data (60 bytes)
 - Data: 01593ea764000001e0000005020100306400000100000000...
 - [Length: 60]

Exibir pacotes encapsulados de OTV para Vlan 100, estendidos sobre OTV

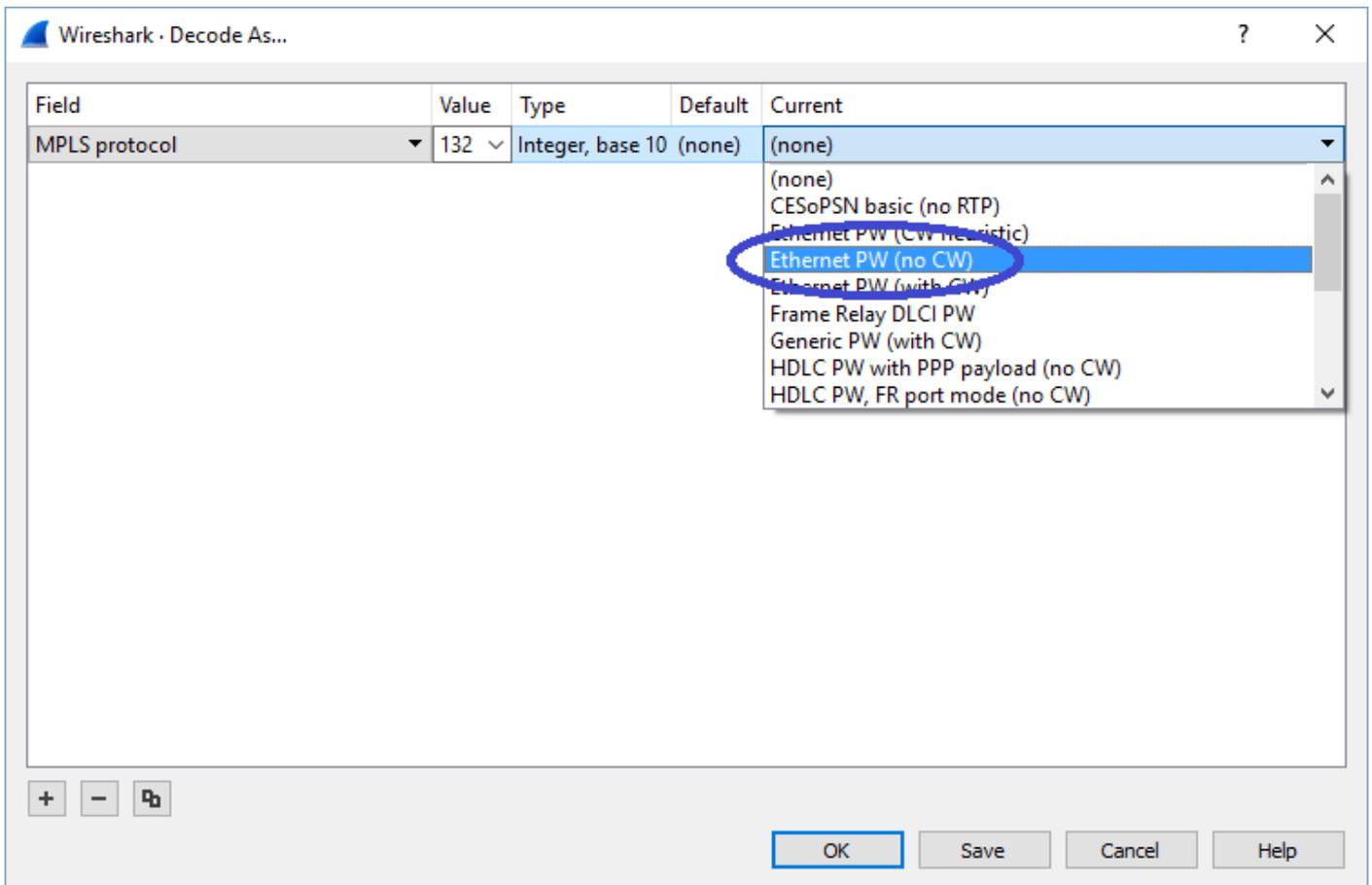
Por padrão, o Wireshark interpreta os primeiros quatro bytes do conteúdo dos pacotes L2VPN MPLS como Control Word. Isso precisa ser corrigido para pacotes encapsulados de OTV. Para fazer isso, clique com o botão direito do mouse no campo de rótulo MPLS de qualquer um dos

pacotes e escolha *Decodificar como...* opção.

The screenshot shows the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet details pane is expanded to show the MultiProtocol Label Switching Header (MPLS). The MPLS header fields are: Label: 132, Exp: 6, S: 1, TTL: 254. The context menu is open over the MPLS header, and the 'Decode As...' option is circled in blue. The menu items are: Expand Subtrees (Shift+Right), Expand All (Ctrl+Right), Collapse All (Ctrl+Left), Apply as Column, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize with Filter, Follow, Copy, Show Packet Bytes..., Export Packet Bytes... (Ctrl+H), Wiki Protocol Page, Filter Field Reference, Protocol Preferences, Decode As... (circled), Go to Linked Packet, and Show Linked Packet in New Window.

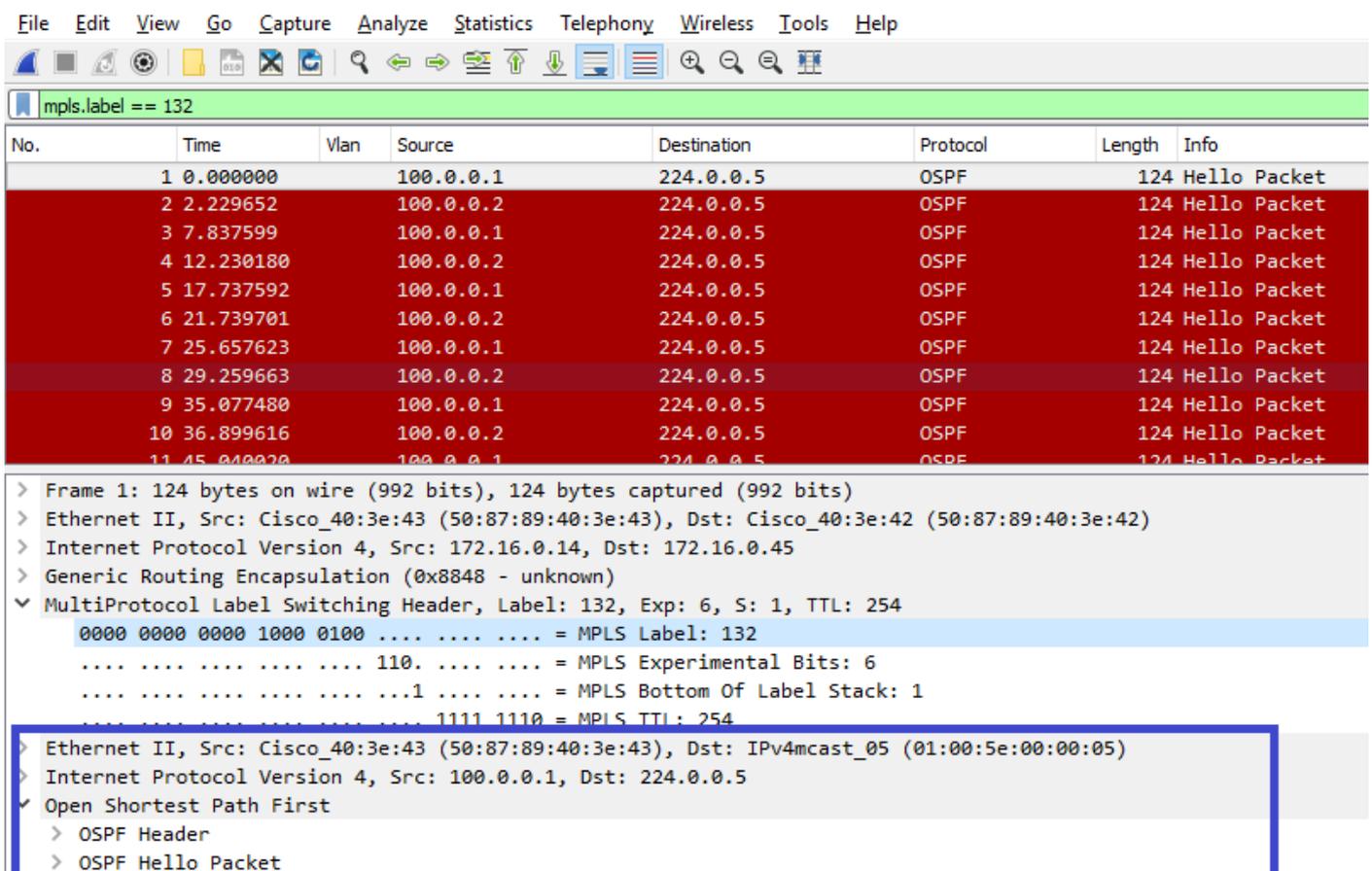
Clique com o botão direito do mouse no campo Rótulo MPLS e escolha *Decodificar como...* opção

A próxima etapa é informar ao Wireshark que o conteúdo encapsulado não tem o Control Word.



Escolha a opção "sem CW"

Depois que essa alteração for enviada clicando no botão OK, a ferramenta de análise do Wireshark exibirá corretamente o conteúdo dos pacotes encapsulados de OTV.



O Wireshark exibe corretamente o conteúdo dos pacotes encapsulados de OTV

Decodificar pacotes na VLAN 200

As etapas acima se aplicam a qualquer vlan estendida sobre OTV. Por exemplo, usando o filtro do Wireshark para exibir somente pacotes da vlan 200, obtemos a seguinte saída na ferramenta de análise.

The screenshot shows the Wireshark interface with a capture filter 'mpls.label == 232' applied. The packet list pane shows several packets, with packet 8 selected. The packet details pane for packet 8 is expanded to show the following structure:

- 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)
- MultiProtocol Label Switching Header, Label: 232, Exp: 0, 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
- PW Ethernet Control Word
 - Sequence Number: 24064
- 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
- Logical-Link Control
 - DSAP: Unknown (0x3f)
 - SSAP: Unknown (0xae)
 - Control field: I, N(R)=0, N(S)=0 (0x0000)
- Data (52 bytes)
 - Data: 0158d0efc8000002e00000a0205f20800000000000000...
 - [Length: 52]

Exibir pacotes para a vlan 200, estendida sobre OTV

Depois que o Wireshark for instruído a não interpretar os primeiros bytes do pacote MPLS como Palavra de Controle PW, o processo de decodificação poderá ser concluído com êxito.

The screenshot shows the Wireshark interface with a capture filter 'mpls.label == 232'. The packet list pane displays 11 packets, all of which are EIGRP Hello messages. The packet details pane for the selected packet (Frame 1) shows the following structure:

- 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)
- 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

O Wireshark exibe corretamente o tráfego da Vlan 200 como pacotes EIGRP

Usar Editcap para remover o cabeçalho OTV

Geralmente, as instalações do Wireshark vêm com uma ferramenta de edição de pacotes de linha de comando chamada *Editcap*. Essa ferramenta pode remover permanentemente a sobrecarga de OTV dos pacotes capturados. Isso permite fácil exibição e análise de pacotes capturados na Interface Gráfica do Usuário (GUI - Graphical User Interface) do Wireshark, sem a necessidade de ajustar manualmente o comportamento de análise do Wireshark.

Executar Editcap na Plataforma Windows

No sistema operacional Windows, o *editcap.exe* é instalado por padrão no diretório `c:\Program Files\Wireshark>`.

Execute esta ferramenta com flag `-C` para remover a sobrecarga de OTV e salvar o resultado em um arquivo *.pcap*.

```
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>
```

Execute a Editcap na plataforma Mac OS

No sistema operacional Mac OS, o *editcap* está disponível na pasta `/usr/local/bin`.

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

Removendo o cabeçalho OTV de pacotes capturados com *Edição* ferramenta, uma perde as informações de Vlan, que são codificadas como parte do cabeçalho MPLS, que, por sua vez, faz parte do calço OTV. Lembre-se de usar o filtro da GUI do Wireshark 'mpls.label == <<vlan number extended over OTV> + 32>' antes de remover o cabeçalho do OTV com a ferramenta *Editcap*, se a análise do tráfego de uma VLAN específica for necessária.

Conclusão

A solução de problemas das soluções Cisco OTV exige uma boa compreensão da tecnologia, tanto da perspectiva da operação do plano de controle quanto do encapsulamento do plano de dados. Aplicando com eficiência o conhecimento, as ferramentas de análise de pacotes freeware, como o Wireshark, podem ser muito eficientes na análise de pacotes OTV. Além de várias opções de exibição de pacotes, a instalação típica do Wireshark oferece uma ferramenta de edição de pacotes que pode simplificar a análise de pacotes. Isso permite que a solução de problemas se concentre nas partes do conteúdo do pacote mais relevantes para uma sessão de solução de problemas específica.