Utilice Wireshark para solucionar problemas de soluciones de OTV

Contenido

Introducción

Este documento demuestra el uso de Wireshark, una herramienta de análisis y captura de paquetes gratuita muy conocida, en la solución de solución de problemas de Cisco OTV.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Overlay Transport Virtualization (OTV) en switches Nexus Series
- Aspectos básicos de las redes privadas virtuales (VPN) de capa 2 de switching de etiquetas multiprotocolo (MPLS)
- Wireshark, un analizador de paquetes libre y de código abierto (https://www.wireshark.org)

Componentes Utilizados

La información de este documento se basa en la plataforma de switches Nexus serie 7000.

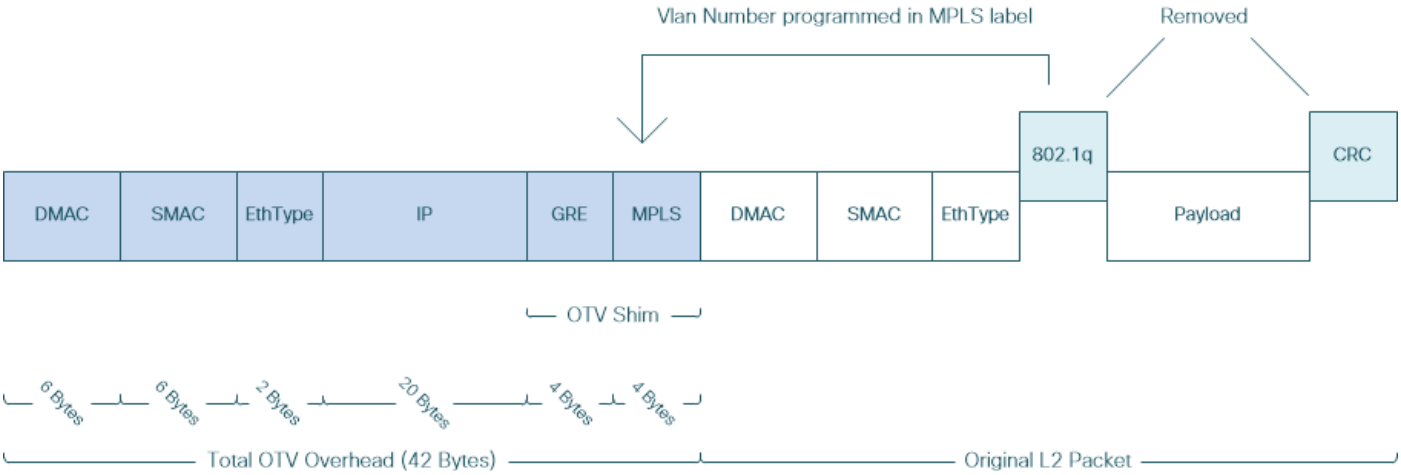
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Descripción de problemas

Al resolver problemas de red en entornos VPN, una de las técnicas implica la captura y el análisis de paquetes encapsulados. Sin embargo, en los entornos de red de Cisco OTV, este enfoque se enfrenta a un cierto desafío. Herramientas de análisis de paquetes utilizadas habitualmente, como Wireshark, a analizador de paquetes de código abierto y libre, puede no interpretar correctamente el contenido del tráfico encapsulado en OTV. Por lo tanto, las soluciones alternativas laboriosas, como la extracción de datos encapsulados de un paquete OTV, suelen ser necesarias para realizar con éxito un análisis de datos.

Formato de paquete OTV

La encapsulación OTV aumenta el tamaño de MTU total del paquete en 42 bytes. Esto es el resultado de la operación del dispositivo OTV Edge que elimina el CRC y los campos 802.1Q de la trama original de Capa 2 y agrega un Shim OTV (que también contiene la información de VLAN y Overlay ID) y un encabezado IP externo.



En las soluciones L2VPN MPLS, los dispositivos de la red subyacente no tienen suficiente información para decodificar correctamente la carga útil del paquete MPLS. Normalmente, esto no es un problema, ya que el reenvío de paquetes en una red de núcleo MPLS se realiza en base a las etiquetas, por lo tanto, no se requiere un análisis en profundidad del contenido de los paquetes MPLS en la red subyacente.

Sin embargo, esto presenta un desafío si se requiere el análisis de datos de los paquetes OTV para la resolución de problemas y/o el monitoreo.

Las herramientas de análisis de paquetes, como Wireshark, intentan decodificar los datos de paquetes que siguen el encabezado MPLS aplicando reglas de análisis de paquetes MPLS regulares. Sin embargo, dado que puede no tener información sobre los resultados de la negociación de Control Word, que normalmente se realizaría entre los routers de cabecera y de cola MPLS L2VPN, las herramientas de análisis de paquetes vuelven al comportamiento de análisis predeterminado y lo aplican a los datos de paquetes que siguen al encabezado MPLS.

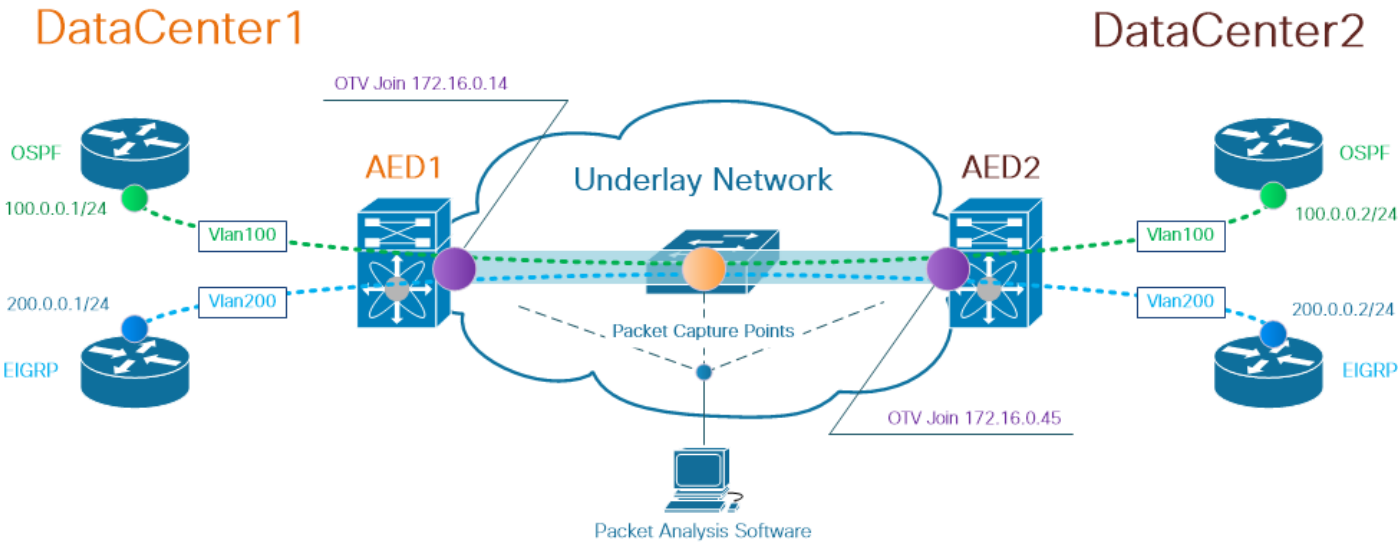
> **Nota:** En las soluciones L2VPN MPLS, como Any Transport Over MPLS (ATOM), los terminales de pseudowire negocian el uso del parámetro de Control Word. Una palabra de control es un campo opcional de 4 bytes ubicado entre la pila de etiquetas MPLS y la carga

útil de Capa 2 en el paquete pseudowire. La palabra de control transporta información genérica y específica de la carga útil de Capa 2. Si el bit C se establece en 1, el Borde del proveedor de publicidad (PE) espera que la palabra de control esté presente en cada paquete de pseudowire en el pseudowire que se está señalizando. Si el bit C está configurado en 0, no se espera que ninguna palabra de control esté presente.

Como resultado, es posible que el comportamiento predeterminado del análisis de Wireshark no interprete correctamente el contenido de los paquetes OTV, lo que hace que el proceso de resolución de problemas de la red OTV sea más complejo.

Topología

El siguiente es un diagrama de red de una red OTV simple. Los routers en Vlan 100 y Vlan 200 establecen adyacencias OSPF y EIGRP entre dos DataCenters, DataCenter1 y DataCenter2, respectivamente. DataCenter Interconnect (DCI) se implementa con un túnel OTV entre los switches N7k, que se muestra en el diagrama como AED1 y AED2.



Nota: la solución Cisco OTV utiliza el concepto de función de dispositivo de extremo autorizado (AED), asignado a un dispositivo de red que encapsula y desencapsula el tráfico de OTV en un sitio determinado.

El desafío que a menudo se observa en las soluciones de tunelización es verificar si un tipo particular de paquetes superpuestos (IGP, FHRP, etc.) llega a ciertos puntos en la red subyacente. El tráfico superpuesto OSPF y EIGRP se utiliza como ejemplo.

Captura de paquete

Hay varias maneras de realizar una captura de paquetes en la red. Una opción es utilizar la función Cisco Switched Port Analyzer (SPAN), disponible en las plataformas de switching Cisco Catalyst y Cisco Nexus.

Como parte del proceso de resolución de problemas, es posible que sea necesario realizar capturas de paquetes en varios puntos. Las interfaces de unión de OTV y las interfaces en la red subyacente se pueden utilizar como punto de captura de paquetes SPAN.

Solución

El motor de análisis predeterminado de Wireshark puede interpretar erróneamente los primeros bytes de los paquetes superpuestos encapsulados por OTV como si formaran parte de la Palabra de control Pseudowire Emulation Edge-to-Edge (PWE3), que normalmente se utiliza en MPLS L2VPNs en una red conmutada por paquetes MPLS.

> **Nota:** En el resto de este documento, se denomina palabra de control de emulación de extremo a extremo de Pseudowire MPLS (PWE3) como *palabra de control*.

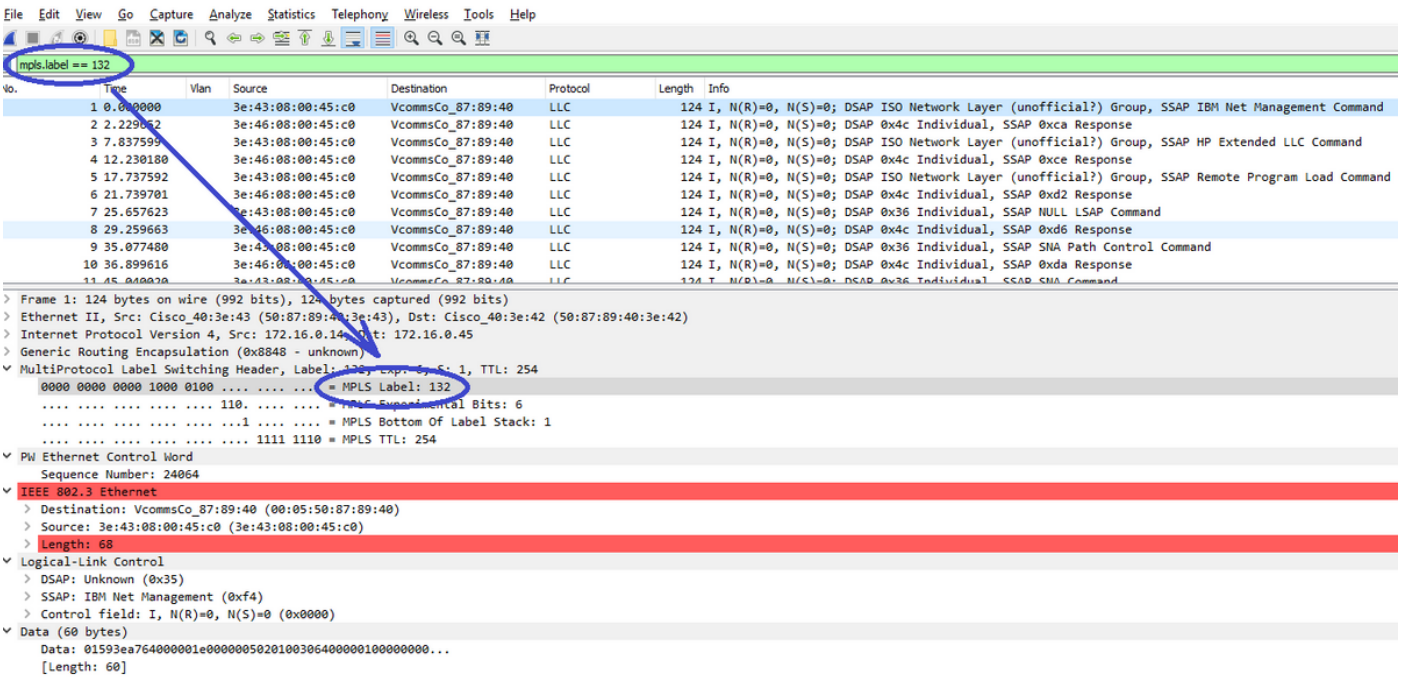
Para garantizar que la herramienta de análisis de paquetes Wireshark interpreta correctamente el contenido de los paquetes encapsulados por OTV, se necesita un ajuste manual del proceso de descodificación de paquetes.

> **Nota:** La etiqueta MPLS utilizada en el encabezado OTV es igual al número vlan superpuesto + 32.

Decodificar paquetes en Vlan 100

Como primer paso del proceso de descodificación, muestre solamente los paquetes encapsulados por OTV que llevan contenido de la vlan 100 extendida por OTV. El filtro utilizado es mpls.label == 132, que representa vlan 100.

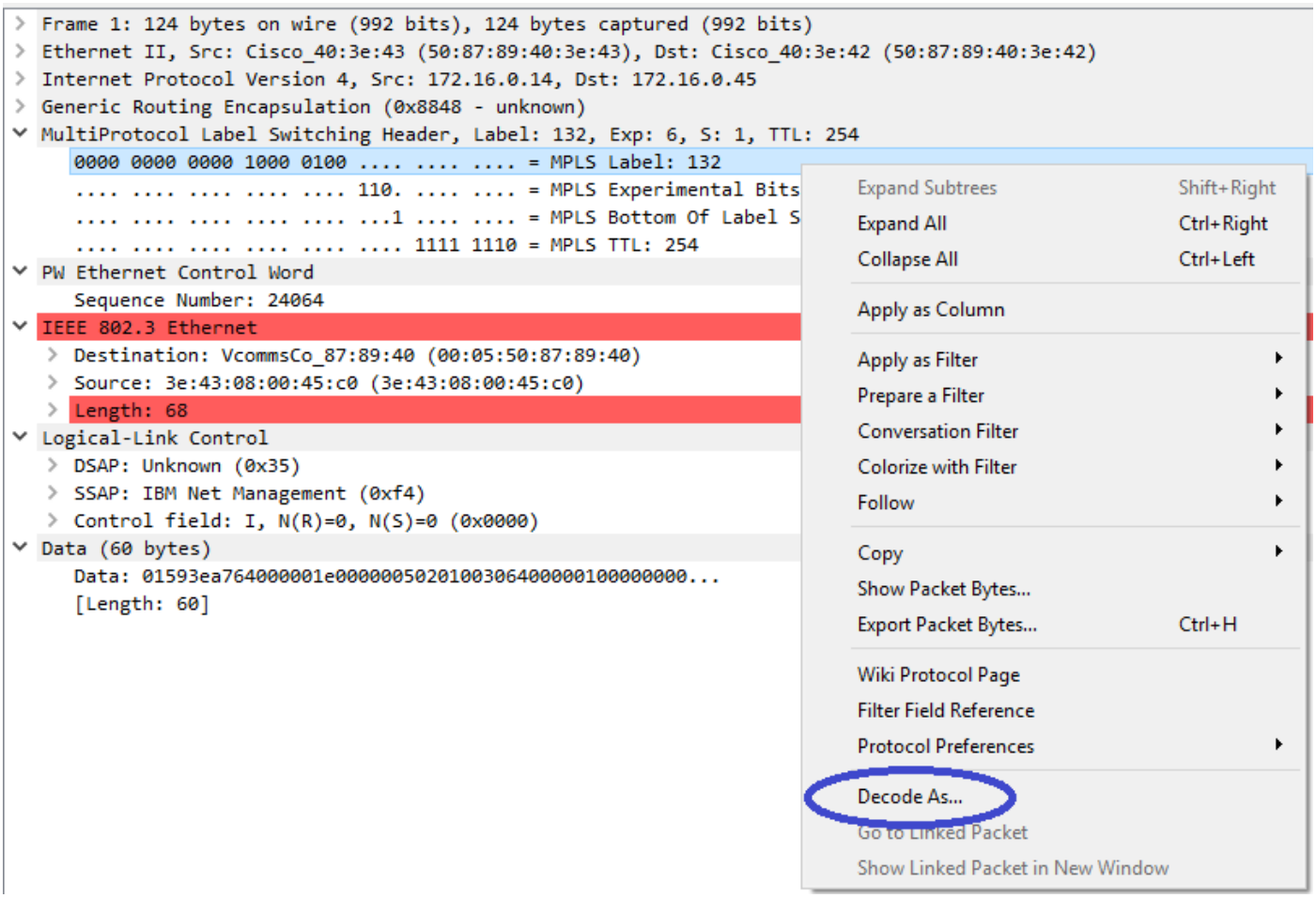
> **Nota:** Para mostrar los paquetes encapsulados por OTV para una vlan determinada extendida sobre OTV, utilice el siguiente filtro de visualización de Wireshark: mpls.label == <<vlan number extended over OTV> + 32>



Mostrar paquetes encapsulados OTV para Vlan 100, extendidos sobre OTV

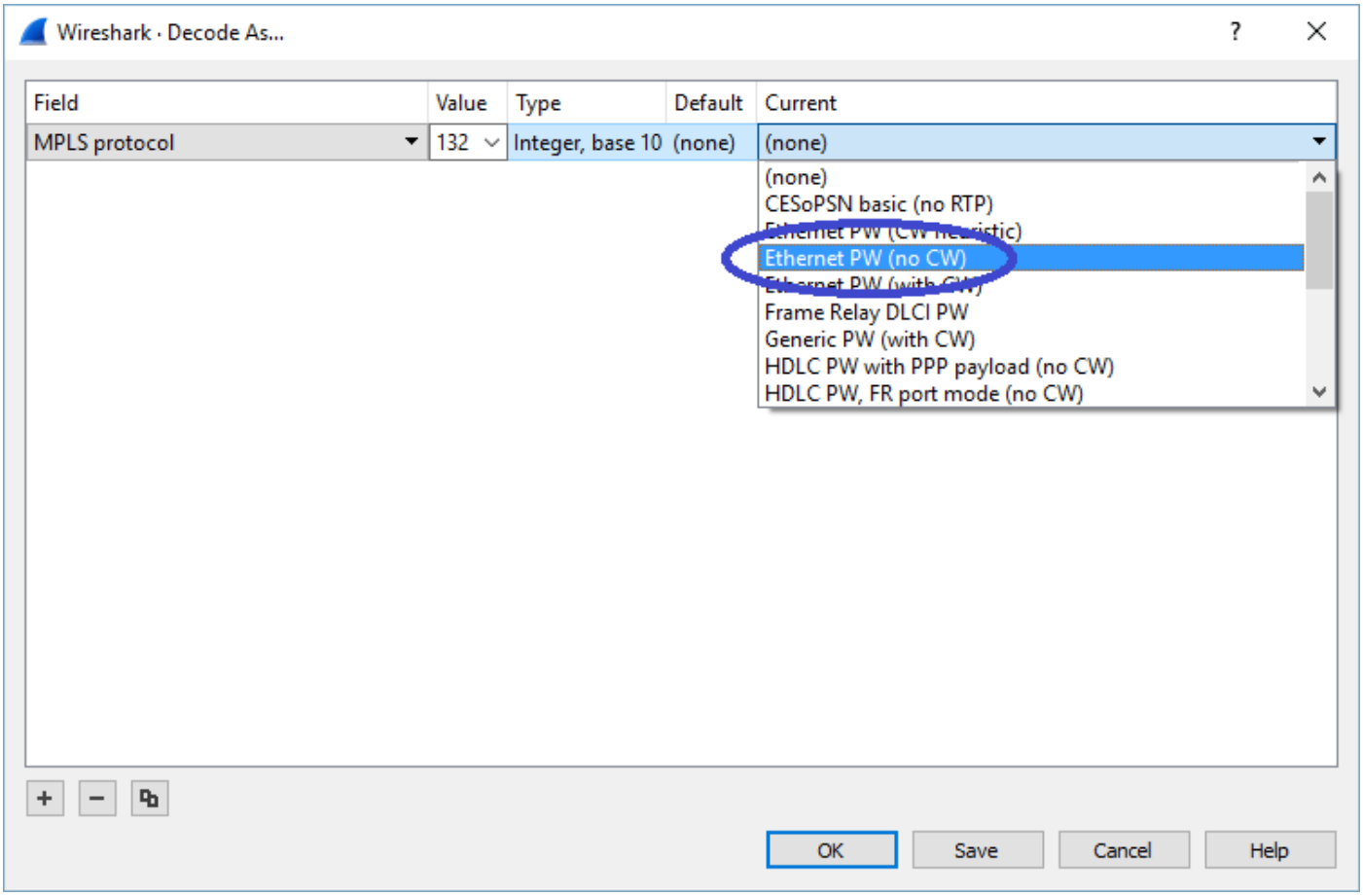
De forma predeterminada, Wireshark interpreta los primeros cuatro bytes del contenido de los paquetes L2VPN MPLS como Palabra de control. Esto debe corregirse para los paquetes

encapsulados por OTV. Para ello, haga clic con el botón derecho en el campo de etiqueta MPLS de cualquiera de los paquetes y elija *Decodificar como...* opción.



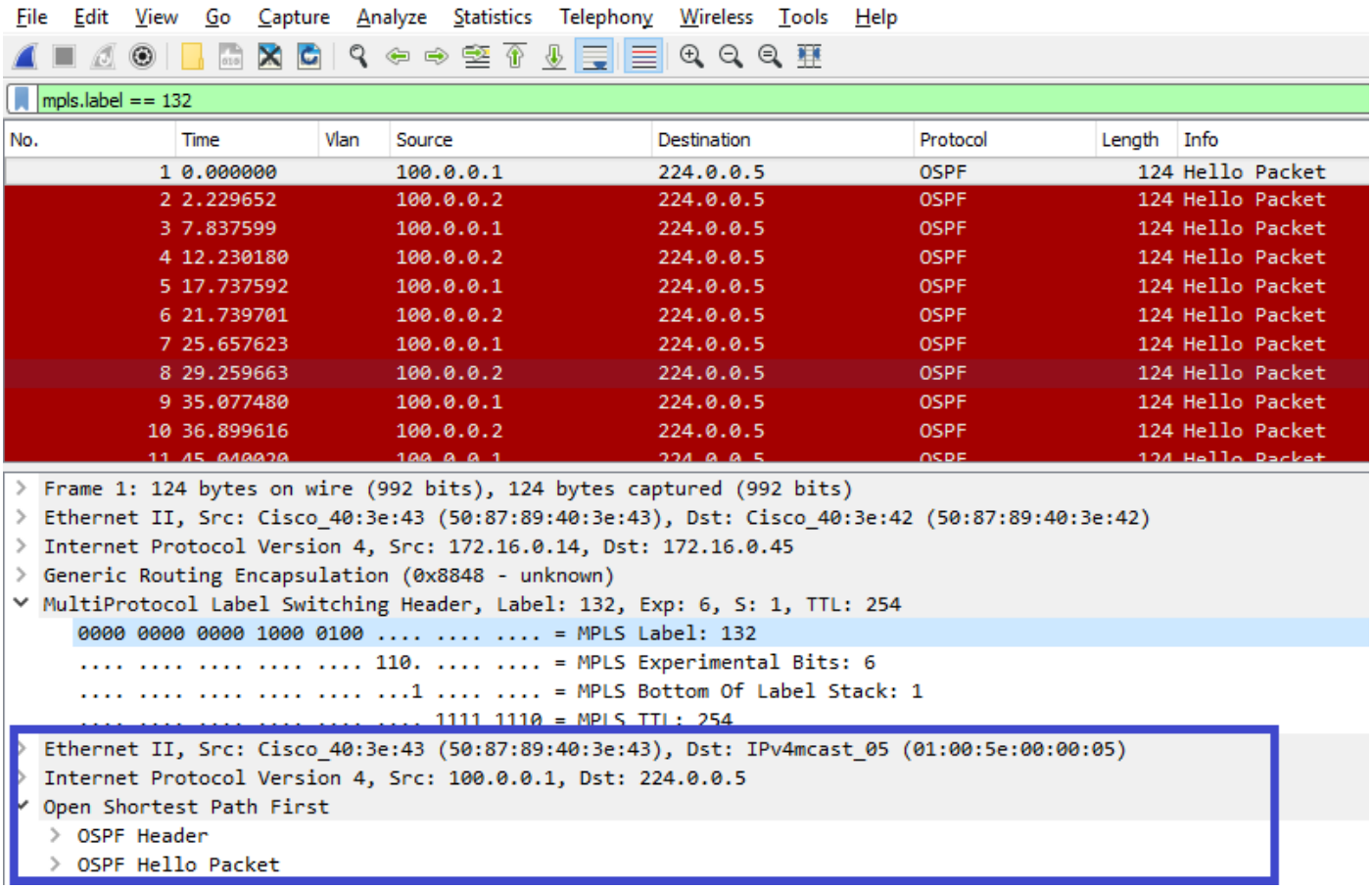
Haga clic con el botón derecho en el campo de etiqueta MPLS y elija Decodificar como... opción

El siguiente paso es decirle a Wireshark que el contenido encapsulado no tiene palabra de control.



Elija la opción "sin CW"

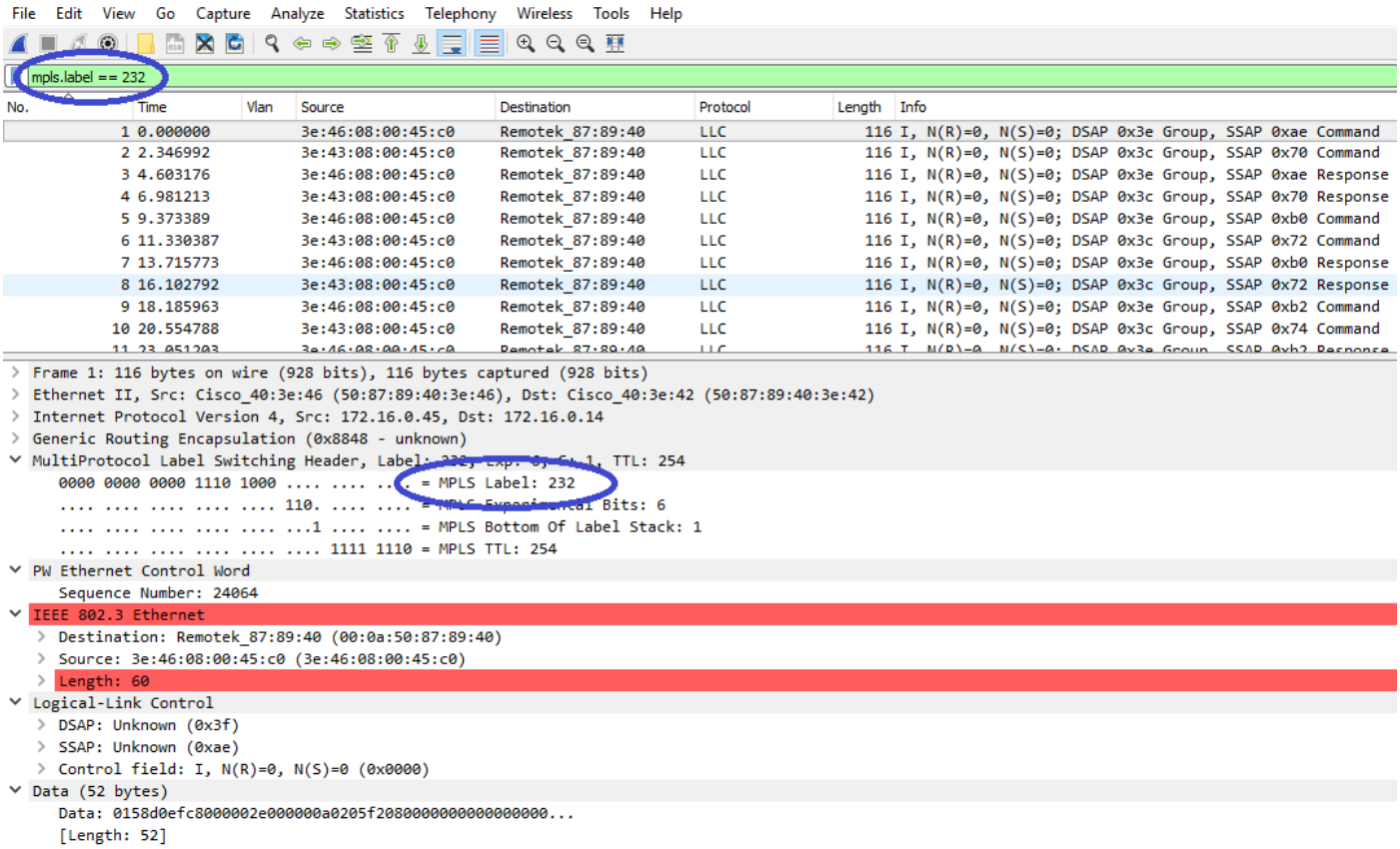
Una vez enviado este cambio haciendo clic en el botón OK (Aceptar), la herramienta de análisis Wireshark mostrará correctamente el contenido de los paquetes encapsulados en OTV.



Wireshark muestra correctamente el contenido de los paquetes encapsulados por OTV

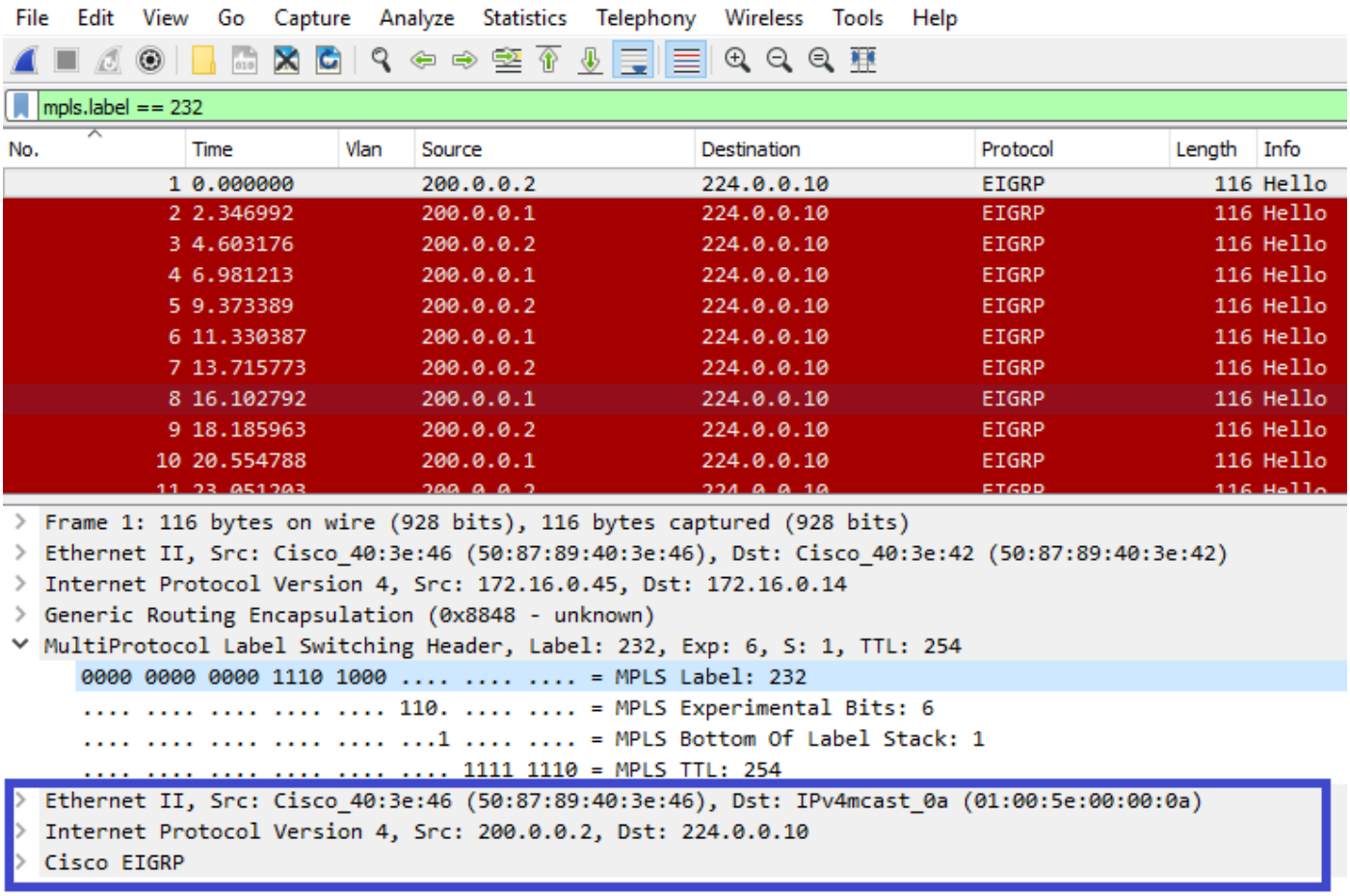
Decodificar paquetes en Vlan 200

Los pasos anteriores son aplicables para cualquier vlan extendida sobre OTV. Por ejemplo, al utilizar el filtro Wireshark para mostrar sólo los paquetes de vlan 200, obtenemos el siguiente resultado en la herramienta de análisis.



Mostrar paquetes para vlan 200, extendidos sobre OTV

Una vez que se indica a Wireshark que no interprete los primeros bytes del paquete MPLS como Palabra de control PW, el proceso de descodificación puede completarse correctamente.



WIreshark muestra correctamente el tráfico Vlan 200 como paquetes EIGRP

Utilizar Editcap para eliminar el encabezado de OTV

Normalmente, las instalaciones de Wireshark vienen con una herramienta de edición de paquetes de línea de comandos llamada *Editcap*. Esta herramienta puede eliminar permanentemente la sobrecarga de OTV de los paquetes capturados. Esto permite una visualización y análisis sencillos de los paquetes capturados en la interfaz gráfica de usuario (GUI) de Wireshark, sin necesidad de ajustar manualmente el comportamiento de análisis de Wireshark.

Ejecutar Editcap en la plataforma de Windows

En el sistema operativo Windows, *editcap.exe* se instala de forma predeterminada en el directorio c:\Program Files\Wireshark>.

Ejecute esta herramienta con el indicador *-C* para quitar la sobrecarga de OTV y guardar el resultado en un archivo *.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>
```

Ejecutar Editcap en la plataforma Mac OS

En el sistema operativo Mac OS, editcap está disponible en la carpeta /usr/local/bin.

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

Al eliminar el encabezado OTV de los paquetes capturados con*Editcap*herramienta, se pierde la información de VLAN que se codifica como parte del encabezado MPLS, que a su vez forma parte de OTV shim. Recuerde utilizar el filtro de GUI de Wireshark 'mpls.label == <<vlan number extended over OTV> + 32>' antes de eliminar el encabezado OTV con la herramienta *Editcap*, si se requiere el análisis del tráfico solamente de una VLAN en particular.

Conclusión

La solución de problemas de las soluciones de Cisco OTV requiere una buena comprensión de la tecnología, tanto desde el punto de vista del funcionamiento del plano de control como de la perspectiva de la encapsulación del plano de datos. Aplicando de manera eficaz el conocimiento, las herramientas de análisis de paquetes freeware como Wireshark pueden resultar muy potentes en el análisis de paquetes OTV. Además de las diversas opciones de visualización de paquetes, la instalación típica de Wireshark ofrece una herramienta de edición de paquetes que puede simplificar el análisis de paquetes. Esto permite que la resolución de problemas se centre en las partes del contenido del paquete que son más relevantes para una sesión de troubleshooting en particular.