Utiliser Wireshark pour dépanner les solutions OTV

Contenu

Introduction

Ce document présente l'utilisation de Wireshark, un outil d'analyse et de capture de paquets gratuits bien connu, pour le dépannage de la solution Cisco OTV.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Virtualisation du transport de superposition (OTV) sur les commutateurs de la gamme Nexus
- Notions de base sur les réseaux privés virtuels (VPN) de couche 2 de la commutation multiprotocole par étiquette (MPLS)
- Wireshark, un analyseur de paquets libre et open source (https://www.wireshark.org)

Components Used

Les informations de ce document sont basées sur la plate-forme de commutation Nexus 7000.

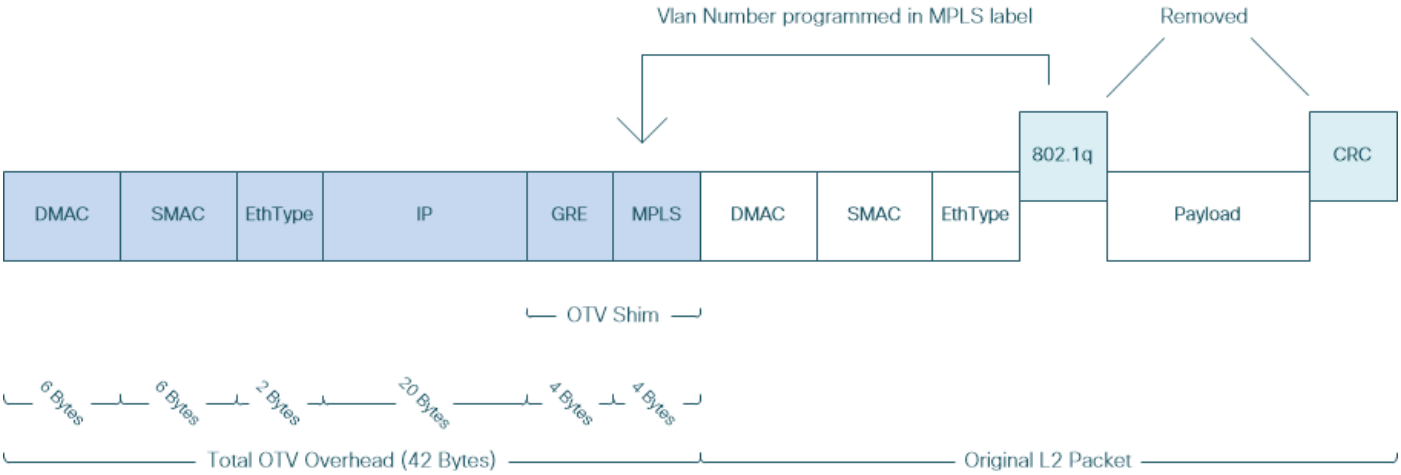
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Description du problème

Lors du dépannage de problèmes réseau dans des environnements VPN, l'une des techniques consiste à capturer et à analyser des paquets encapsulés. Cependant, dans les environnements de réseau Cisco OTV, cette approche est confrontée à un certain défi. Outils d'analyse de paquets couramment utilisés, tels que Wireshark, a analyseur de paquets gratuit et open source, peut ne pas interpréter correctement le contenu du trafic encapsulé OTV. Par conséquent, des solutions de contournement laborieuses, telles que l'extraction de données encapsulées à partir d'un paquet OTV, sont généralement nécessaires pour effectuer avec succès l'analyse des données.

Format de paquet OTV

L'encapsulation OTV augmente la taille MTU globale du paquet de 42 octets. Ceci est le résultat du fonctionnement du périphérique Edge OTV qui supprime le CRC et les champs 802.1Q de la trame de couche 2 d'origine et ajoute un Shim OTV (contenant également les informations VLAN et Overlay ID) et un en-tête IP externe.



Dans les solutions MPLS L2VPN, les périphériques du réseau sous-jacent ne disposent pas d'informations suffisantes pour décoder correctement la charge utile des paquets MPLS. En règle générale, ce n'est pas un problème, car le transfert de paquets dans un réseau principal MPLS est effectué sur la base d'étiquettes. Par conséquent, il n'est pas nécessaire d'effectuer une analyse approfondie du contenu des paquets MPLS dans le réseau sous-jacent.

Cependant, cela pose un problème si l'analyse des données des paquets OTV est requise pour le dépannage et/ou la surveillance.

Les outils d'analyse de paquets, tels que Wireshark, tentent de décoder les données de paquets qui suivent l'en-tête MPLS en appliquant des règles d'analyse de paquets MPLS régulières. Cependant, comme il ne dispose peut-être pas d'informations sur les résultats de la négociation Control Word, qui serait normalement effectuée entre les routeurs de tête de réseau L2VPN MPLS et les routeurs de bout en bout, les outils d'analyse de paquets reviennent au comportement d'analyse par défaut et l'appliquent aux données de paquets qui suivent l'en-tête MPLS.

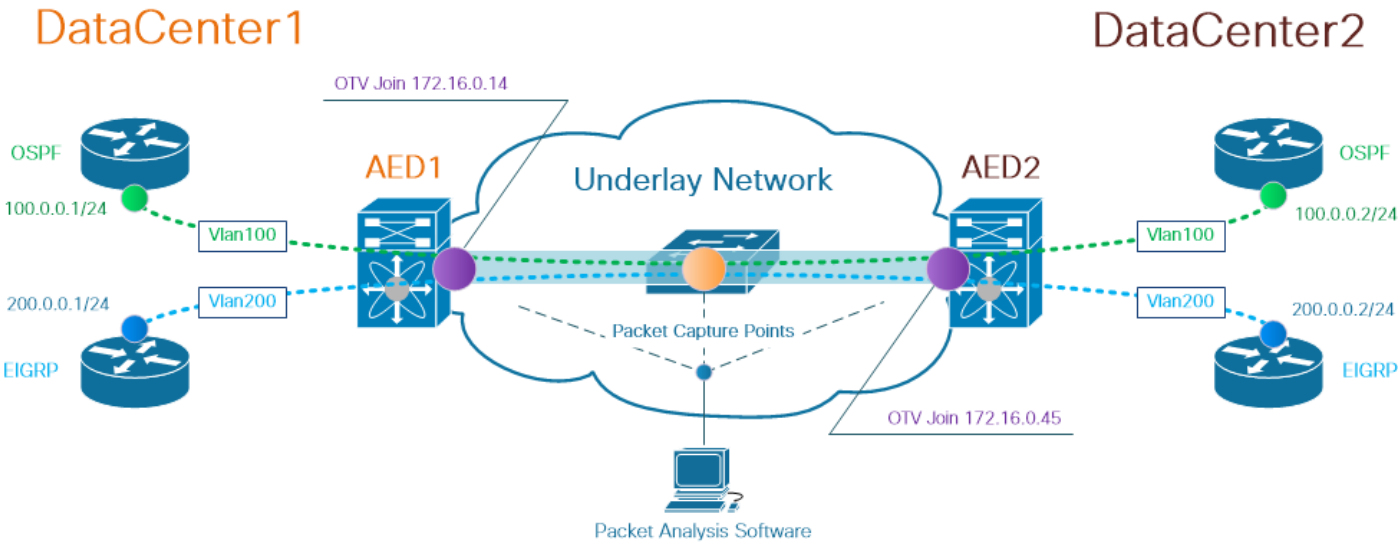
> **Note**: Dans les solutions L2VPN MPLS, telles que Any Transport Over MPLS (ATOM), les terminaux pseudowire négocient l'utilisation du paramètre Control Word. Un mot de contrôle est un champ facultatif de 4 octets situé entre la pile d'étiquettes MPLS et la charge utile de

couche 2 dans le paquet pseudowire. Le mot de contrôle transporte des informations génériques et spécifiques à la charge utile de couche 2. Si le bit C est défini sur 1, le périphérique du fournisseur de publicité (PE) s'attend à ce que le mot de contrôle soit présent dans chaque paquet de pseudocâble sur le pseudocâble qui est signalé. Si le bit C est défini sur 0, aucun mot de contrôle ne doit être présent.

Par conséquent, le comportement d'analyse Wireshark par défaut peut ne pas interpréter correctement le contenu des paquets OTV, rendant ainsi le processus de dépannage du réseau OTV plus complexe.

Topologie

Voici un schéma de réseau d'un réseau OTV simple. Les routeurs des VLAN 100 et 200 établissent des contiguïtés OSPF et EIGRP entre deux data centers, DataCenter1 et DataCenter2, respectivement. L'interconnexion de data center (DCI) est mise en oeuvre avec un tunnel OTV entre les commutateurs N7k, représenté sur le schéma sous la forme AED1 et AED2.



Remarque : la solution Cisco OTV utilise le concept de rôle AED (Authoritative Edge Device), attribué à un périphérique réseau qui encapsule et décapsule le trafic OTV sur un site particulier.

Le défi souvent relevé dans les solutions de tunnellisation consiste à vérifier si un type particulier de paquets de superposition (IGP, FHRP, etc.) le fait à certains points du réseau de sous-couche. Le trafic de superposition OSPF et EIGRP est utilisé comme exemple.

Capture de paquets

Il existe plusieurs façons d'effectuer une capture de paquets dans le réseau. Une option consiste à utiliser la fonctionnalité SPAN (Switched Port Analyzer) de Cisco, disponible sur les plates-formes de commutation Cisco Catalyst et Cisco Nexus.

Dans le cadre du processus de dépannage, il peut être nécessaire d'effectuer des captures de paquets à plusieurs points. Les interfaces et interfaces de jointure OTV du réseau de sous-couche peuvent être utilisées comme point de capture de paquets SPAN.

Solution

Le moteur d'analyse par défaut de Wireshark peut mal interpréter les premiers octets d'un paquet de superposition encapsulé OTV comme s'ils faisaient partie d'un mot de contrôle PowerEdge à Edge (PWE3) d'émulation Pseudowire, généralement utilisé dans les VPN L2VPN MPLS sur un réseau à commutation de paquets MPLS.

> **Note**: Le mot de contrôle MPLS Pseudowire Emulation Edge-to-Edge (PWE3) est appelé *Control Word* dans le reste de ce document.

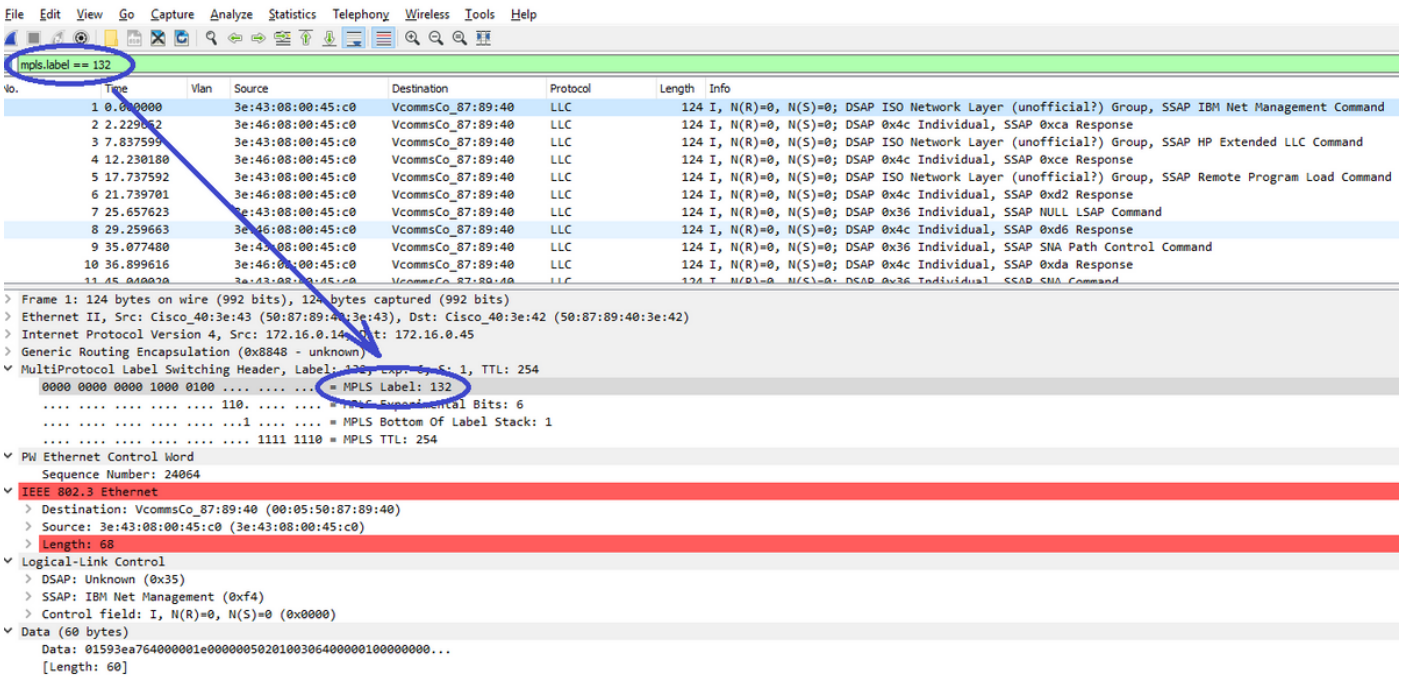
Pour s'assurer que l'outil d'analyse de paquets Wireshark interprète correctement le contenu des paquets encapsulés OTV, un ajustement manuel du processus de décodage de paquets est nécessaire.

> **Note**: L'étiquette MPLS utilisée dans l'en-tête OTV est égale au numéro de VLAN de superposition + 32.

Décoder les paquets dans Vlan 100

Comme première étape du processus de décodage, affichez uniquement les paquets encapsulés OTV qui transportent le contenu du VLAN 100 étendu OTV. Le filtre utilisé est mpls.label == 132, qui représente le vlan 100.

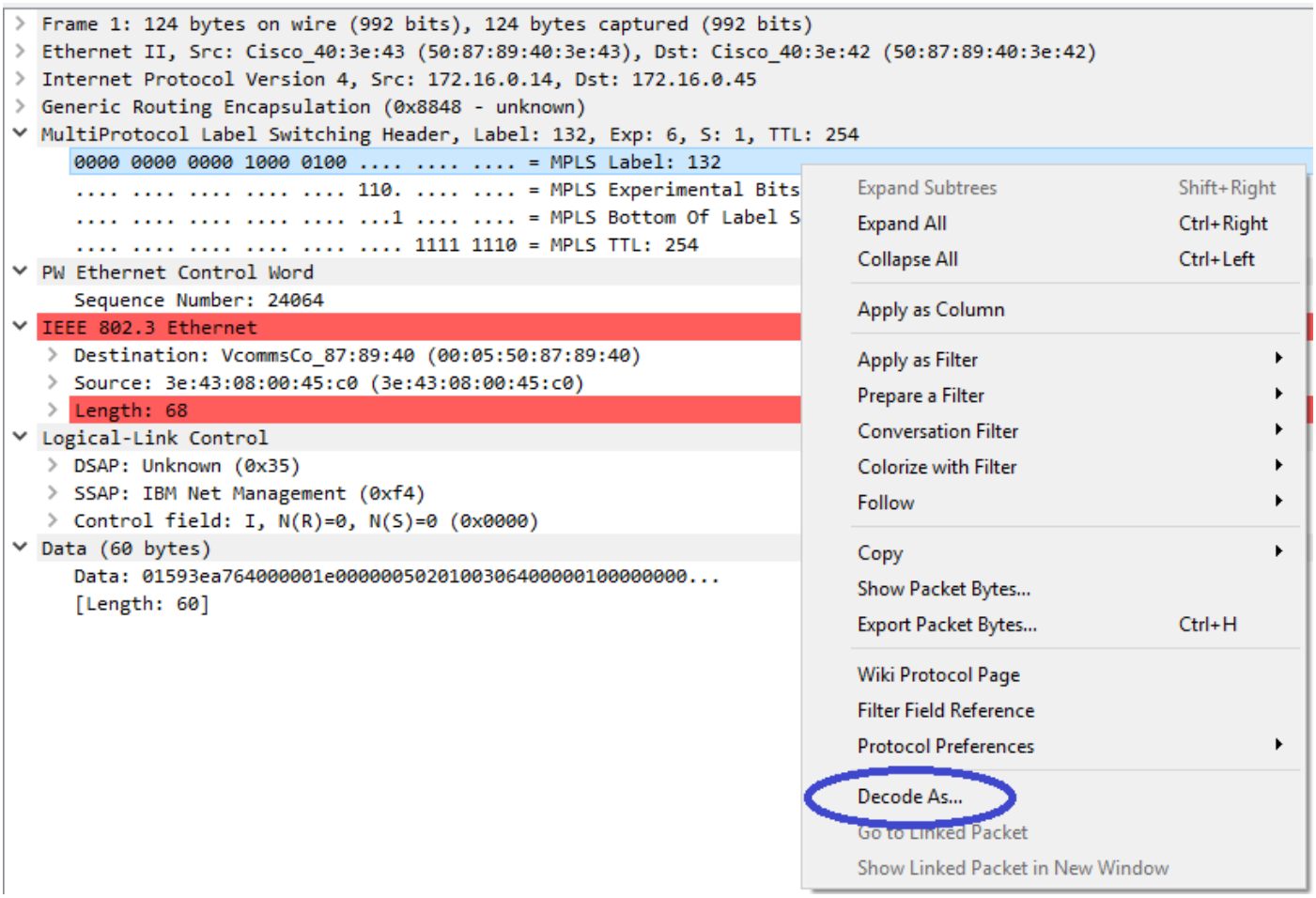
> **Note**: Pour afficher les paquets encapsulés OTV pour un VLAN particulier étendu sur OTV, utilisez le filtre d'affichage Wireshark suivant : mpls.label == « numéro de VLAN étendu sur OTV> + 32>



Afficher les paquets encapsulés OTV pour Vlan 100, étendus sur OTV

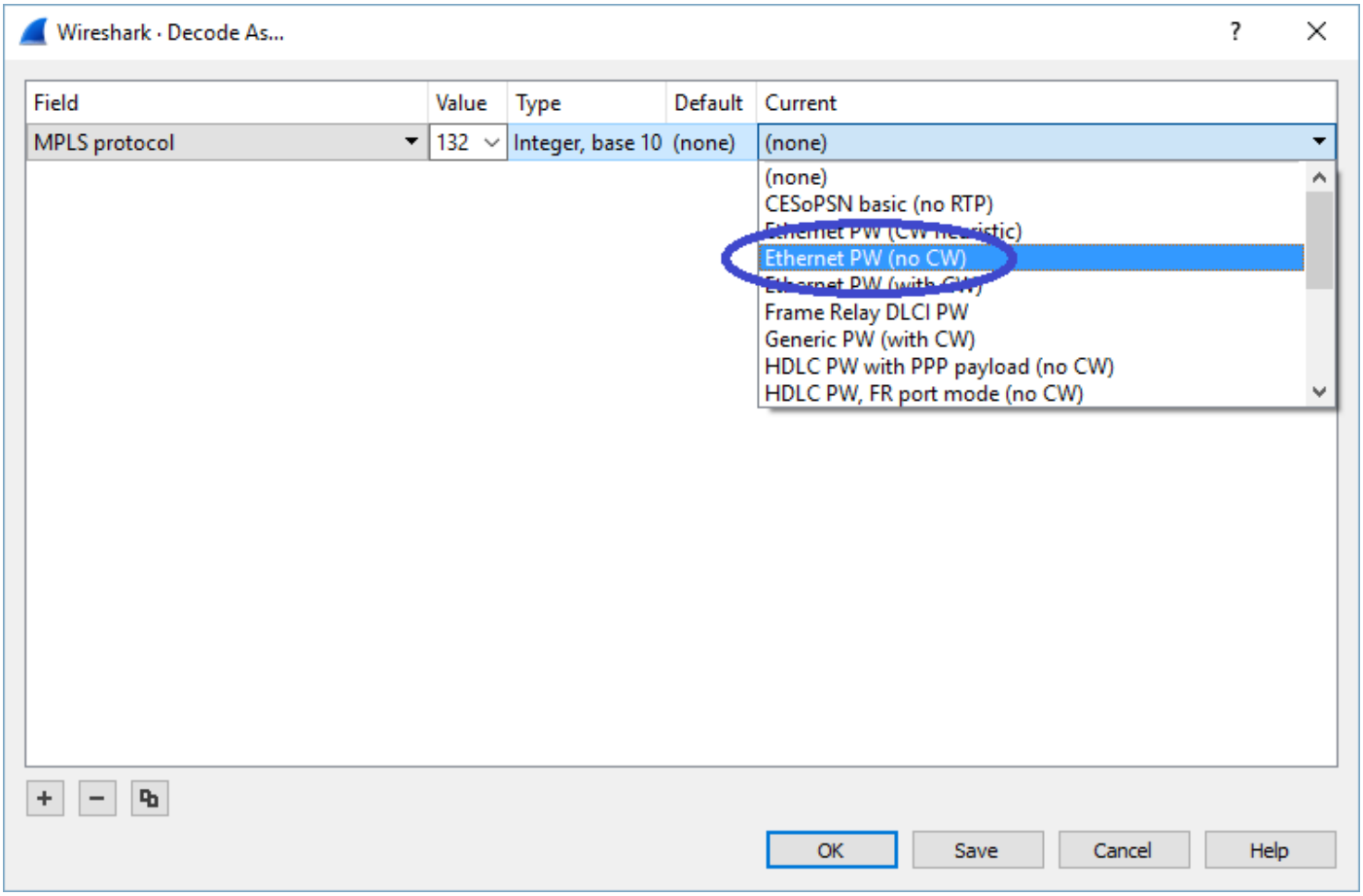
Par défaut, Wireshark interprète les quatre premiers octets du contenu des paquets MPLS L2VPN comme Control Word. Ceci doit être corrigé pour les paquets encapsulés OTV. Pour ce faire,

cliquez avec le bouton droit sur le champ d'étiquette MPLS de l'un des paquets, puis choisissez *Décoder sous...* option.



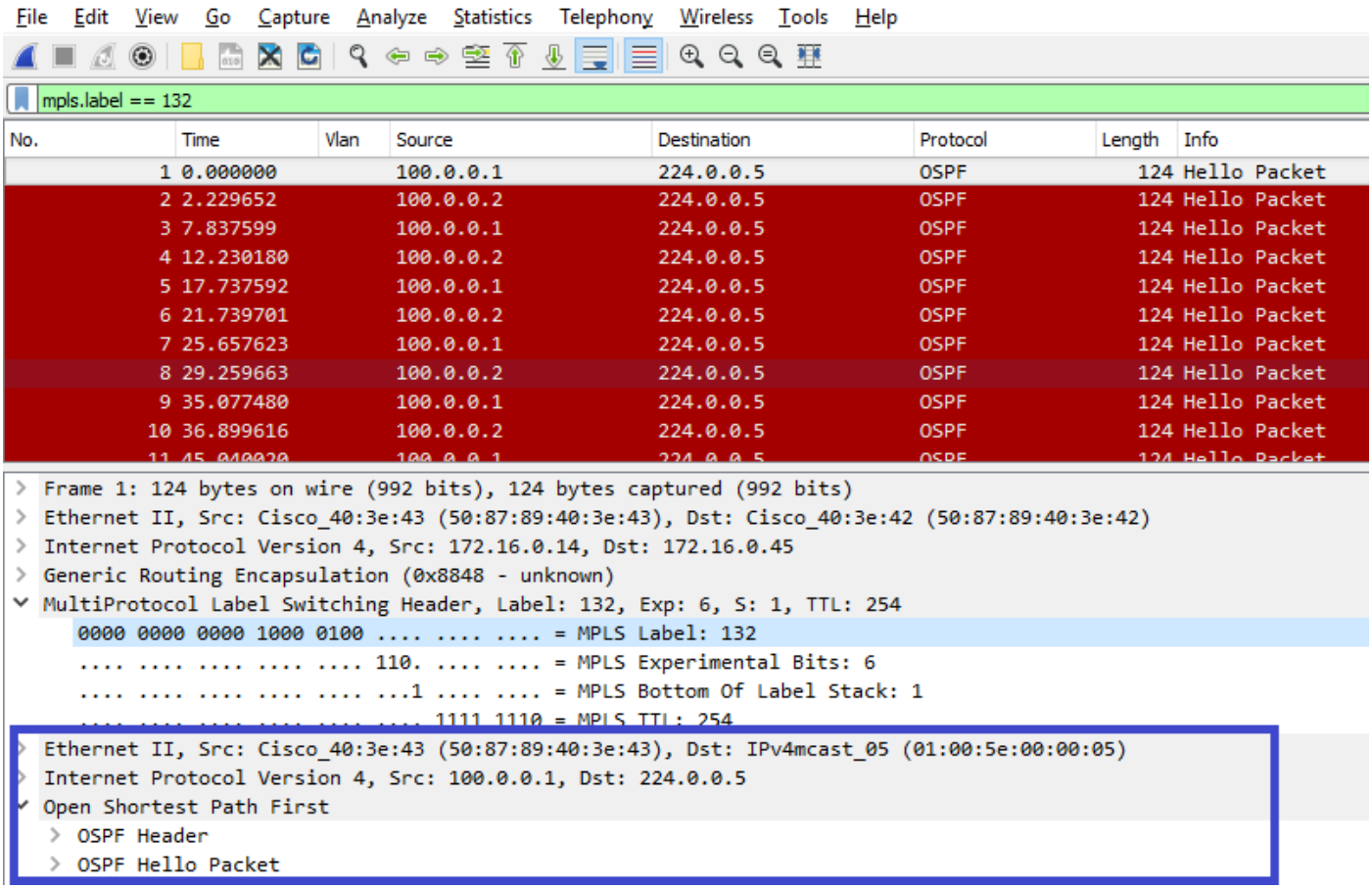
Cliquez avec le bouton droit sur le champ d'étiquette MPLS et choisissez Décoder en tant que... option

L'étape suivante consiste à indiquer à Wireshark que le contenu encapsulé n'a pas de mot de contrôle.



Sélectionnez l'option « pas de PV ».

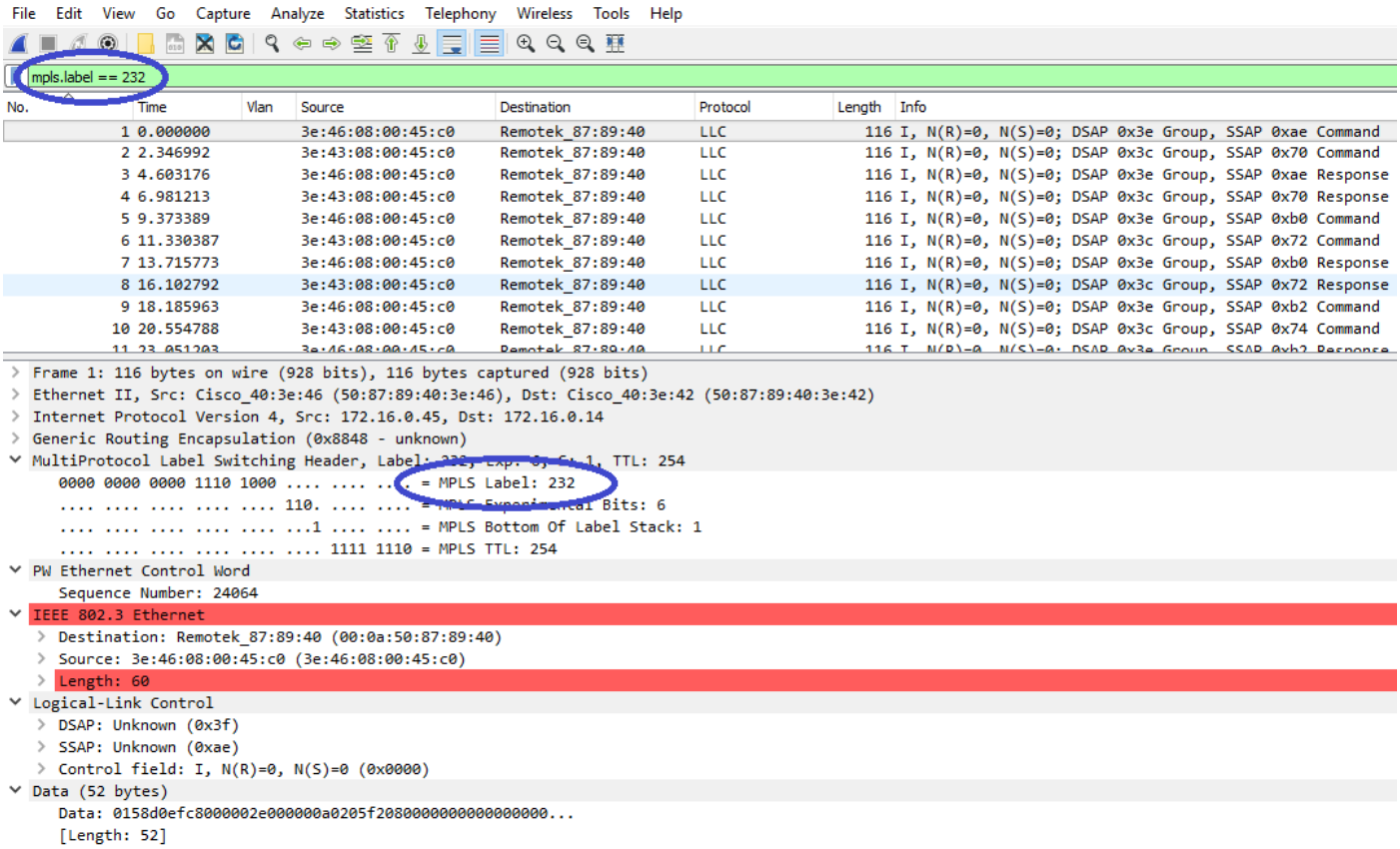
Une fois cette modification envoyée en cliquant sur OK, l'outil d'analyse Wireshark affiche correctement le contenu des paquets encapsulés OTV.



Wireshark affiche correctement le contenu des paquets encapsulés OTV

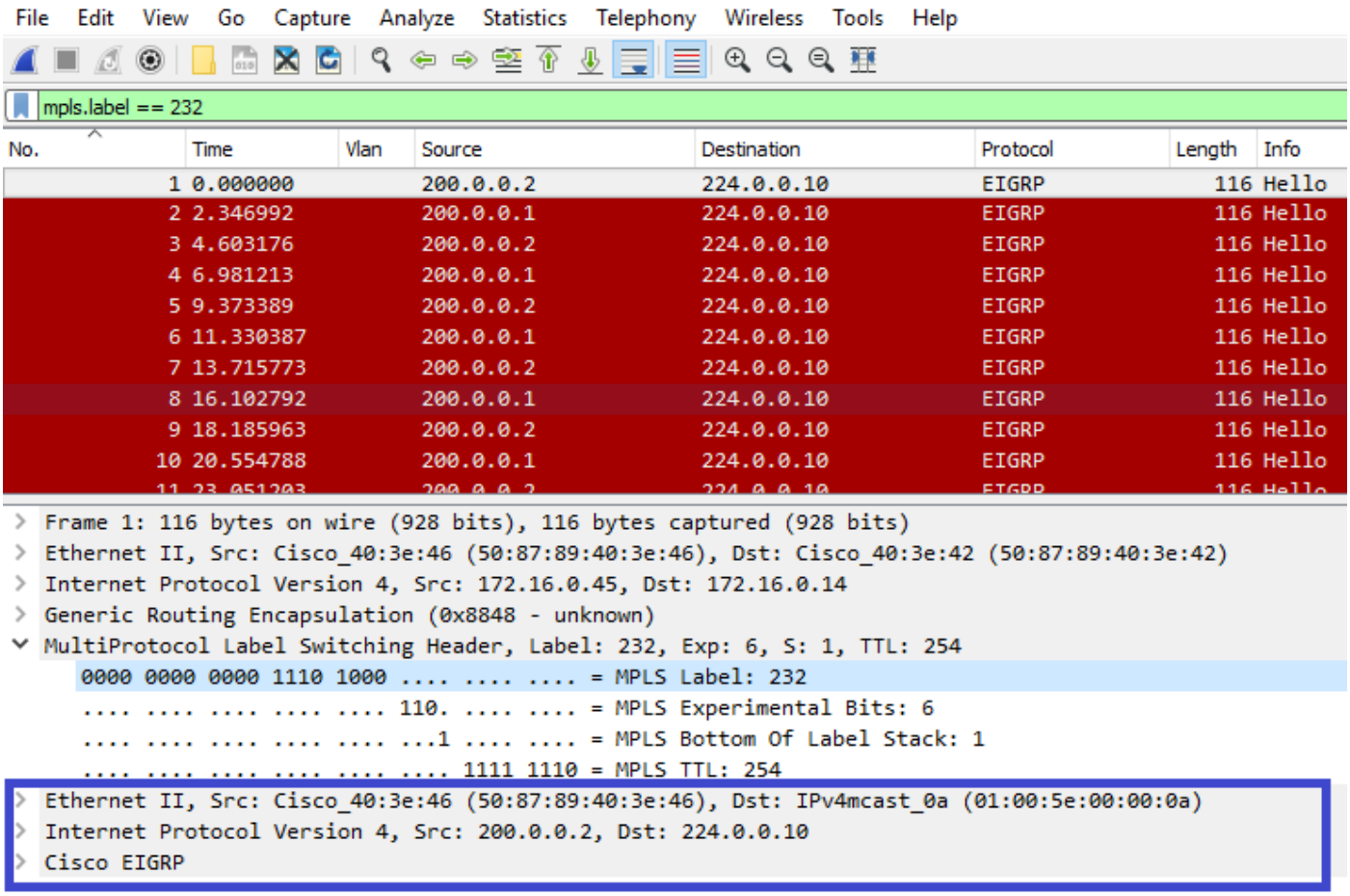
Décoder les paquets dans Vlan 200

Les étapes ci-dessus s'appliquent à tout VLAN étendu sur OTV. Par exemple, en utilisant le filtre Wireshark pour afficher uniquement les paquets de vlan 200, nous obtenons le résultat suivant dans l'outil d'analyse.



Afficher les paquets pour le VLAN 200, étendu sur OTV

Une fois que Wireshark a reçu l'instruction de ne pas interpréter les premiers octets du paquet MPLS comme PW Control Word, le processus de décodage peut se terminer correctement.



WIreshark affiche correctement le trafic Vlan 200 en tant que paquets EIGRP

Utiliser Editcap pour supprimer l'en-tête OTV

Généralement, les installations Wireshark sont fournies avec un outil d'édition de paquets de ligne de commande appelé *Editcap*. Cet outil peut supprimer définitivement la surcharge OTV des paquets capturés. Cela permet d'afficher et d'analyser facilement les paquets capturés dans l'interface utilisateur graphique de Wireshark, sans avoir à ajuster manuellement le comportement d'analyse de Wireshark.

Exécuter Editcap sur la plate-forme Windows

Sur le système d'exploitation Windows, *editcap.exe* est installé par défaut dans le répertoire c:\Program Files\Wireshark>.

Exécutez cet outil avec l'indicateur *-C* pour supprimer la surcharge OTV et enregistrer le résultat dans un fichier *.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>
```

Exécuter Editcap sur la plate-forme Mac OS

Sur le système d'exploitation Mac OS, editcap est disponible dans le dossier /usr/local/bin.

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

En supprimant l'en-tête OTV des paquets capturés avec*Éditeur*outil, on perd les informations Vlan qui sont codées comme partie de l'en-tête MPLS, qui fait à son tour partie de la shim OTV. N'oubliez pas d'utiliser le filtre de l'interface graphique de Wireshark 'mpls.label == « numéro de VLAN étendu sur OTV> + 32>' avant de supprimer l'en-tête OTV avec l'outil *Editcap*, si l'analyse du trafic d'un VLAN spécifique est requise.

Conclusion

Le dépannage des solutions Cisco OTV nécessite une bonne compréhension de la technologie, du point de vue du fonctionnement du plan de contrôle et de l'encapsulation du plan de données. En appliquant efficacement ces connaissances, les outils d'analyse de paquets gratuits tels que Wireshark peuvent s'avérer très puissants dans l'analyse de paquets OTV. En plus de diverses options d’affichage des paquets, l’installation Wireshark type offre un outil d’édition de paquets qui peut simplifier l’analyse des paquets. Cela permet de concentrer le dépannage sur les parties du contenu du paquet qui sont les plus pertinentes pour une session de dépannage particulière.