Gebruik Wireshark om OTV-oplossingen voor problemen op te lossen

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Beschrijving van probleem](#)
[OTV-pakketindeling](#)
[Topologie](#)
[Packet Capture](#)
[Oplossing](#)
[Decode-pakketten in VLAN 100](#)
[Decode-pakketten in VLAN 200](#)
[Gebruik de optie Bewerken om de OTV-header te verwijderen](#)
[Editcap op Windows platform uitvoeren](#)
[Editcap op Mac OS-platform uitvoeren](#)
[Conclusie](#)

Inleiding

Dit document demonstreert het gebruik van Wireshark, een bekend freeware PacketCapture en Analytics-gereedschap voor het oplossen van Cisco OTV-oplossingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Overlay Transport Virtualization (OTV) op Nexus Series switches
- Basics van Multiprotocol Label Switching (MPLS) Layer 2 Virtual Private Networks (VPN's)
- Wireshark, een gratis en open source pakketanalyzer (https://www.wireshark.org)

Gebruikte componenten

De informatie in dit document is gebaseerd op het Nexus 7000 Series-switchplatform.

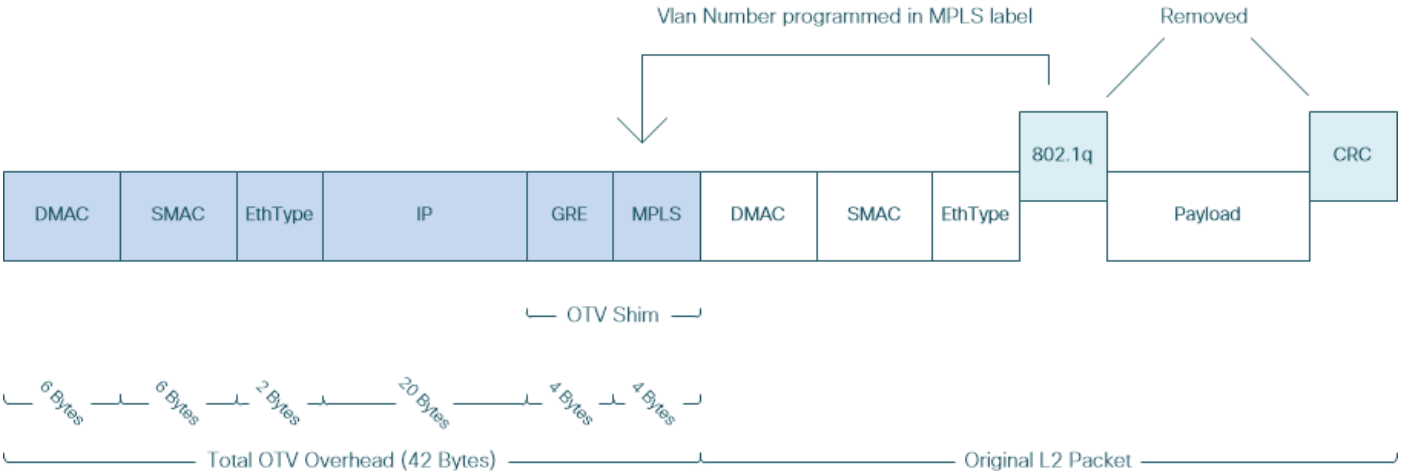
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Beschrijving van probleem

Wanneer u netwerkproblemen in VPN-omgevingen wilt oplossen, omvat een van de technieken de opname en analyse van ingekapselde pakketten. In Cisco OTV-netwerkomgevingen wordt deze benadering echter met een bepaalde uitdaging geconfronteerd. Normaal gebruikte pakketanalysetools, zoals Wireshark, a pakketanalyzer met vrije en open source, kan de inhoud van OTV-ingekapseld verkeer niet op de juiste manier interpreteren. Vandaar dat lastige werkronden, zoals de extractie van ingekapselde gegevens uit een OTV-pakket, gewoonlijk vereist zijn om met succes gegevensanalyse uit te voeren.

OTV-pakketindeling

OTV-insluiting verhoogt de totale MTU-grootte van het pakket met 42 bytes. Dit is het resultaat van de werking van het OTV Edge-apparaat dat CRC en de 802.1Q-velden van het oorspronkelijke Layer 2-frame verwijdert en een OTV-schakelaar (die ook de VLAN- en Overlay-ID-informatie bevat) en een externe IP-kop toevoegt.



In MPLS L2VPN-oplossingen hebben apparaten in het underlay netwerk niet genoeg informatie om de MPLS-pakketlading correct te decoderen. Meestal is dit geen probleem, omdat pakkettransport in een MPLS kernnetwerk uitgevoerd wordt op basis van labels, zodat een diepgaande analyse van de inhoud van MPLS pakketten in het underlay netwerk niet vereist is.

Dit vormt echter een uitdaging als er behoefte is aan gegevensanalyse van OTV-pakketten om de problemen op te lossen en/of te controleren.

Packet Analytics-tools, zoals Wireshark, proberen pakketgegevens te decoderen die de MPLS-header volgen door reguliere MPLS-pakketparseringsregels toe te passen. Aangezien deze echter geen informatie heeft over de resultaten van de onderhandeling van Control Word, die normaal gesproken zou worden uitgevoerd tussen de head-end van MPLS L2VPN en Tail-end routers, vallen de gereedschappen voor pakketanalysen terug op standaard parseringsgedrag en passen deze toe op pakketgegevens die MPLS-header volgen.

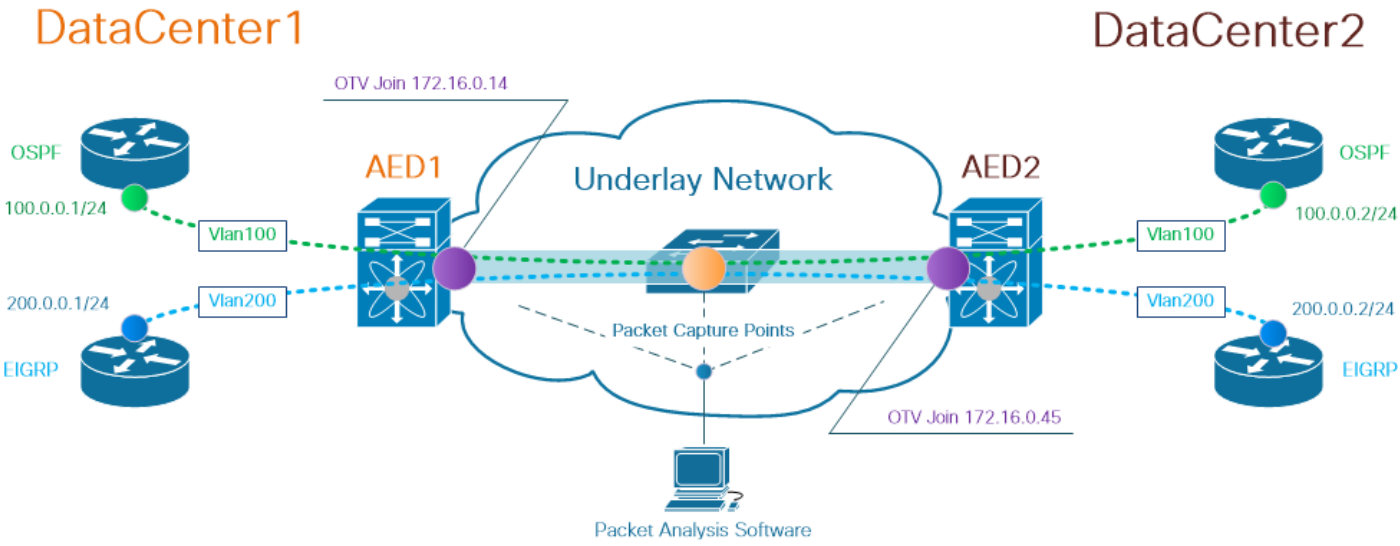
> Opmerking: In MPLS L2VPN-oplossingen, zoals Any Transport Over MPLS (ATOM), onderhandelen pseudo-eindpunten over het gebruik van een Control Word-parameter. Een beheerwoord is een optioneel 4-byte-veld dat zich tussen de MPLS-labelstack en Layer 2-payload in het pseudodraadpakket bevindt. Het controlewoord draagt generieke en Layer 2

payload-specifieke informatie. Als de C-bit op 1 is ingesteld, verwacht de reclameprovider Edge (PE) dat het controlewoord aanwezig is in elk pseudodraadpakket op de aangegeven pseudodraad. Als de C-bit op 0 is ingesteld, wordt er geen control woord verwacht.

Als resultaat hiervan, kan het standaard Woordopsgedrag Wireshark de inhoud van OTV pakketten niet correct interpreteren, waardoor het probleemoplossing proces van OTV netwerk complexer wordt.

Topologie

Het volgende is een netwerkdiagram van een eenvoudig OTV-netwerk. De routers in VLAN 100 en VLAN 200 maken nabijheid OSPF en Ecu tussen twee DataCenters, DataCenter1 en DataCenter2, respectievelijk. DataCenter Interconnect (DCI) wordt geïmplementeerd met OTV-tunnel tussen N7k-switches, zoals weergegeven in het schema als AED1 en AED2.



Opmerking: Cisco OTV-oplossing gebruikt het concept AED-rol (Authoriative Edge Devices), die is toegewezen aan een netwerkapparaat dat OTV-verkeer op een bepaalde website inkapselt en decapsulEERT.

De uitdaging die vaak wordt gezien in tunneling-oplossingen is om te verifiëren of een bepaald type overlay-pakketten (IGP, FHRP, enz.) het aan bepaalde punten in onderlay netwerk maakt. OSPF- en EcoRing-verkeer worden als voorbeeld gebruikt.

Packet Capture

Er zijn meerdere manieren om een pakketvastlegging in het netwerk uit te voeren. Eén optie is om Cisco Switched Port Analyzer (SPAN) te gebruiken, beschikbaar op Cisco Catalyst en Cisco Nexus-switchplatforms.

Als onderdeel van het proces voor het oplossen van problemen moeten pakketvastlegging op meerdere punten mogelijk worden uitgevoerd. OTV kan zich bij interfaces en interfaces in het underlay netwerk worden gebruikt als SPAN-pakketvastlegging.

Oplossing

De standaardiseringsmotor van Wireshark kan eerste paar bytes van een door OTV ingekapselde overlay-pakketten met de verkeerde interpretatie interpreteren alsof ze deel uitmaken van Pseudo-Emulation Edge-to-Edge (PWE3) Control Word, die doorgaans in MPLS L2VPN's wordt gebruikt via een MPLS pakketgeschakeld netwerk.

> Opmerking: MPLS Pseudo-Emulation Edge-to-Edge (PWE3) Control Word wordt in de rest van dit document *Control Word* genoemd.

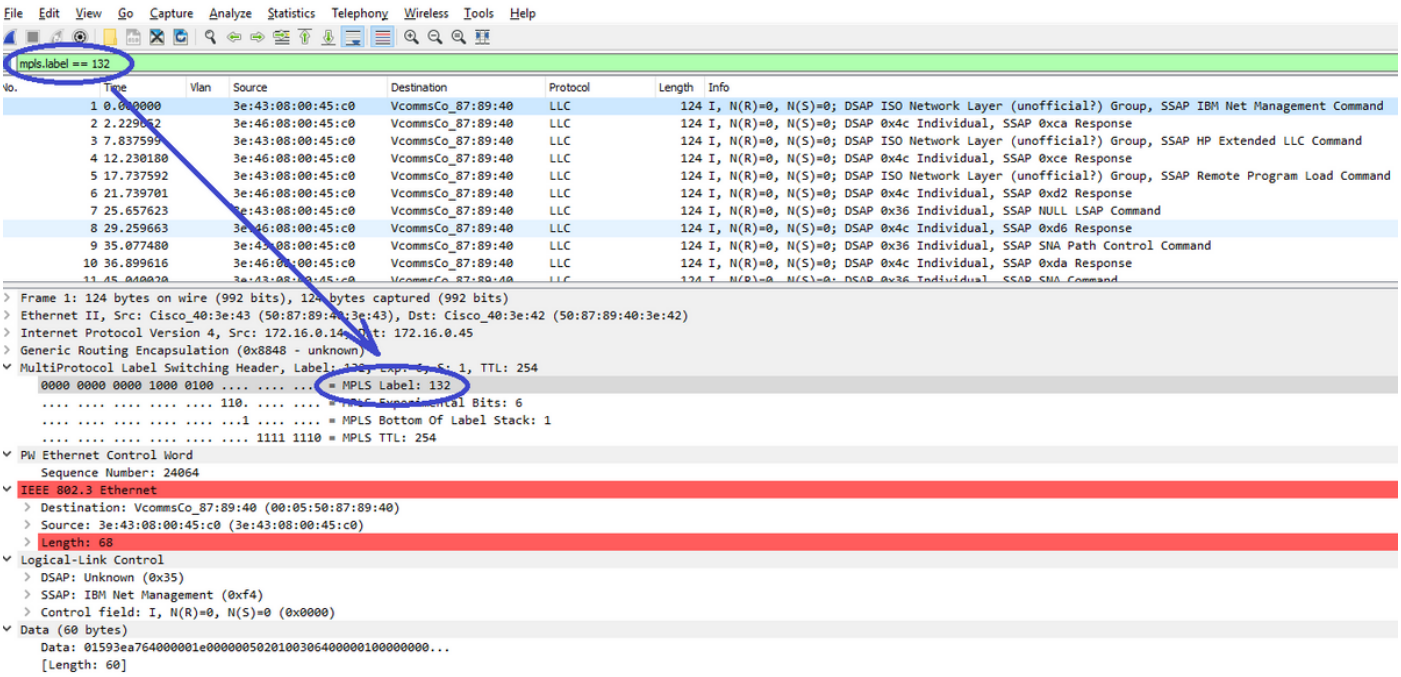
Om er zeker van te zijn dat het gereedschap voor de pakketanalyse Wireshark de inhoud van door OTV ingekapselde pakketten correct interpreteert, is het handmatig aanpassen van het pakketdecodeproces nodig.

> Opmerking: MPLS-label dat in OTV-header wordt gebruikt, is gelijk aan boven VLAN-nummer + 32.

Decode-pakketten in VLAN 100

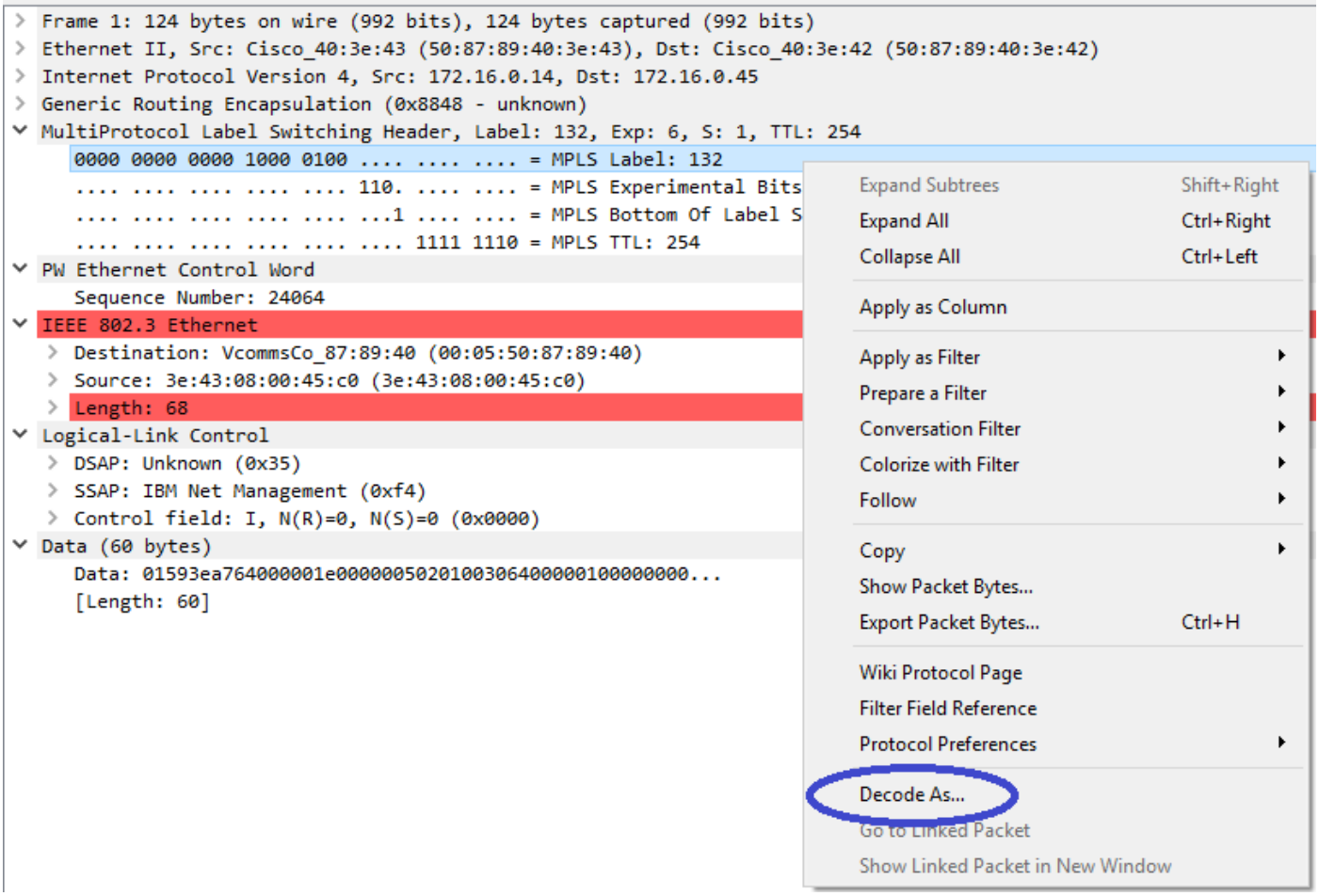
Als eerste stap bij het decodeproces worden alleen in OTV ingekapselde pakketten weergegeven die inhoud van OTV-uitgebreid VLAN 100 bevatten. Er wordt gebruikgemaakt van een filter is mpls.label = 132, dat VLAN 100 vertegenwoordigt.

> Opmerking: Als u OTV-ingekapselde pakketten voor een bepaald VLAN wilt weergeven dat via OTV is uitgebreid, gebruikt u de volgende Wireshark display filter: mpls.label = <<VLAN-nummer uitgebreid via OTV> + 32>



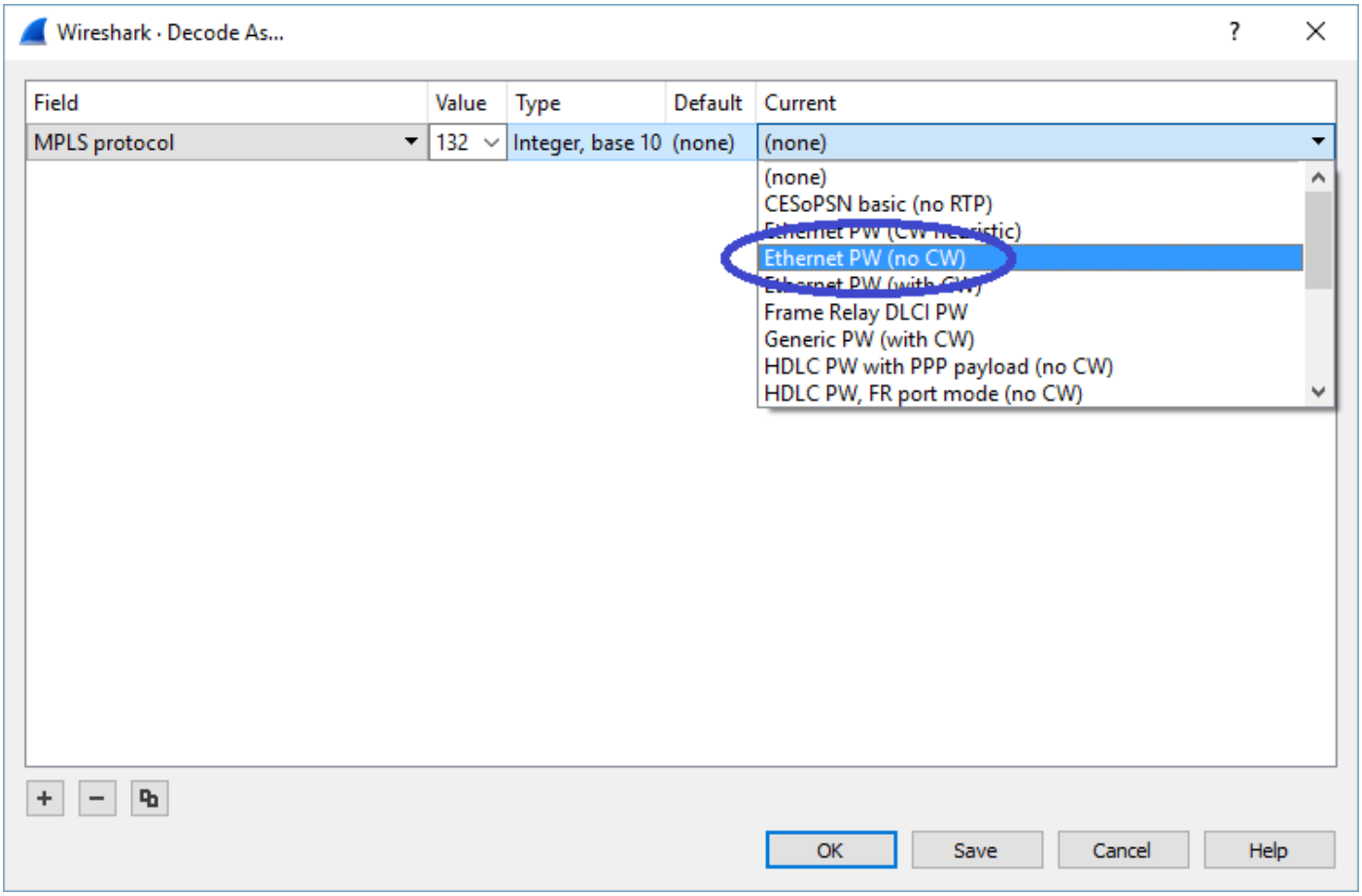
Geef OTV-ingekapselde pakketten op voor VLAN 100, uitgebreid via OTV

Standaard zal Wireshark de eerste vier bytes van de inhoud van MPLS L2VPN-pakketten als Control Word interpreteren. Dit moet worden gecorrigeerd voor OTV-ingekapselde pakketten. Om dit te doen, klik met de rechtermuisknop op het MPLS-labelveld van een van de pakketten en kies *Decode As...* optie.



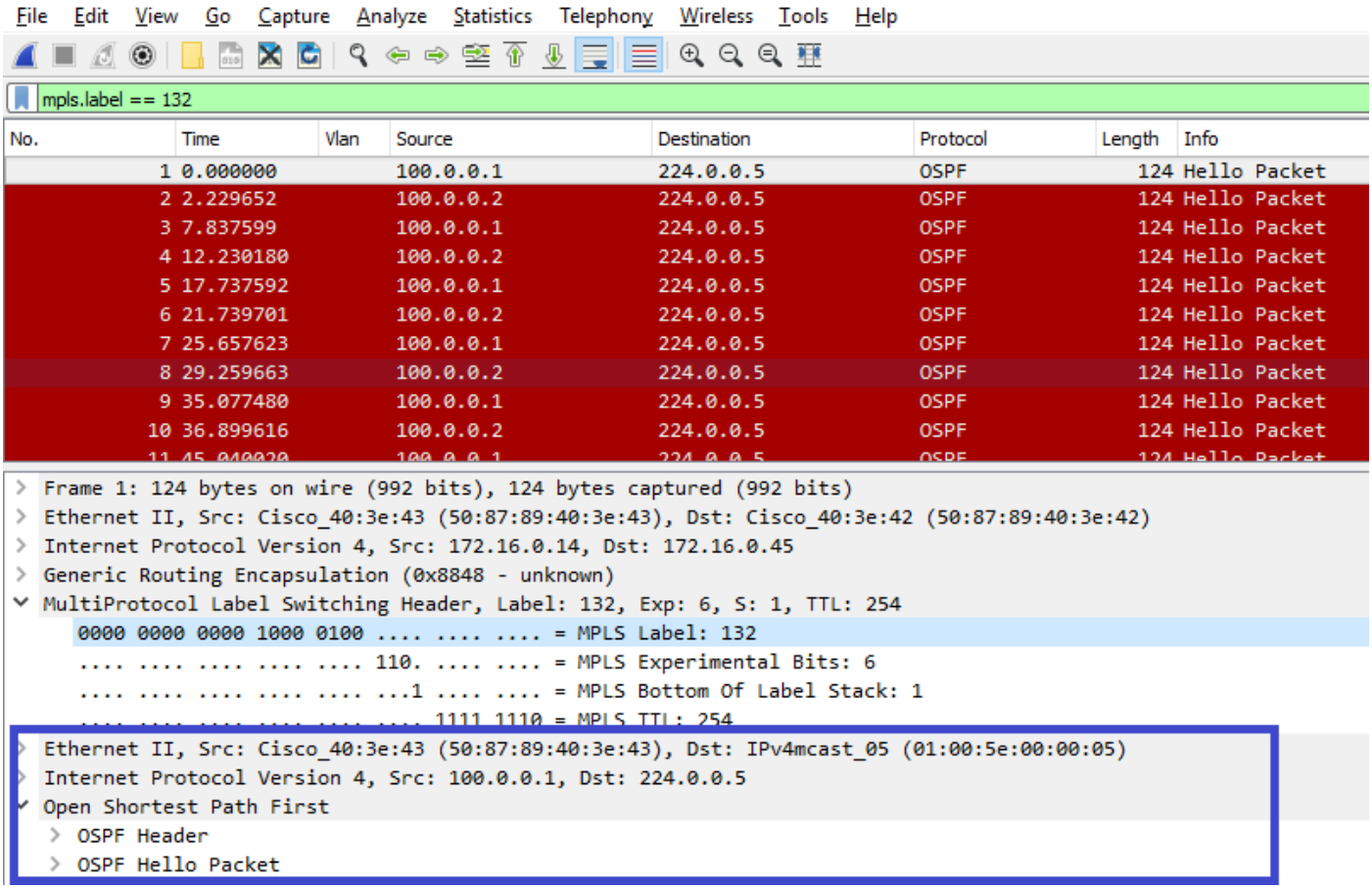
Klik met de rechtermuisknop op het veld MPLS-label en kies optie Decode als...

De volgende stap is om Wireshark te vertellen dat de ingekapselde inhoud geen Controle Word heeft.



Kies "geen CW" optie

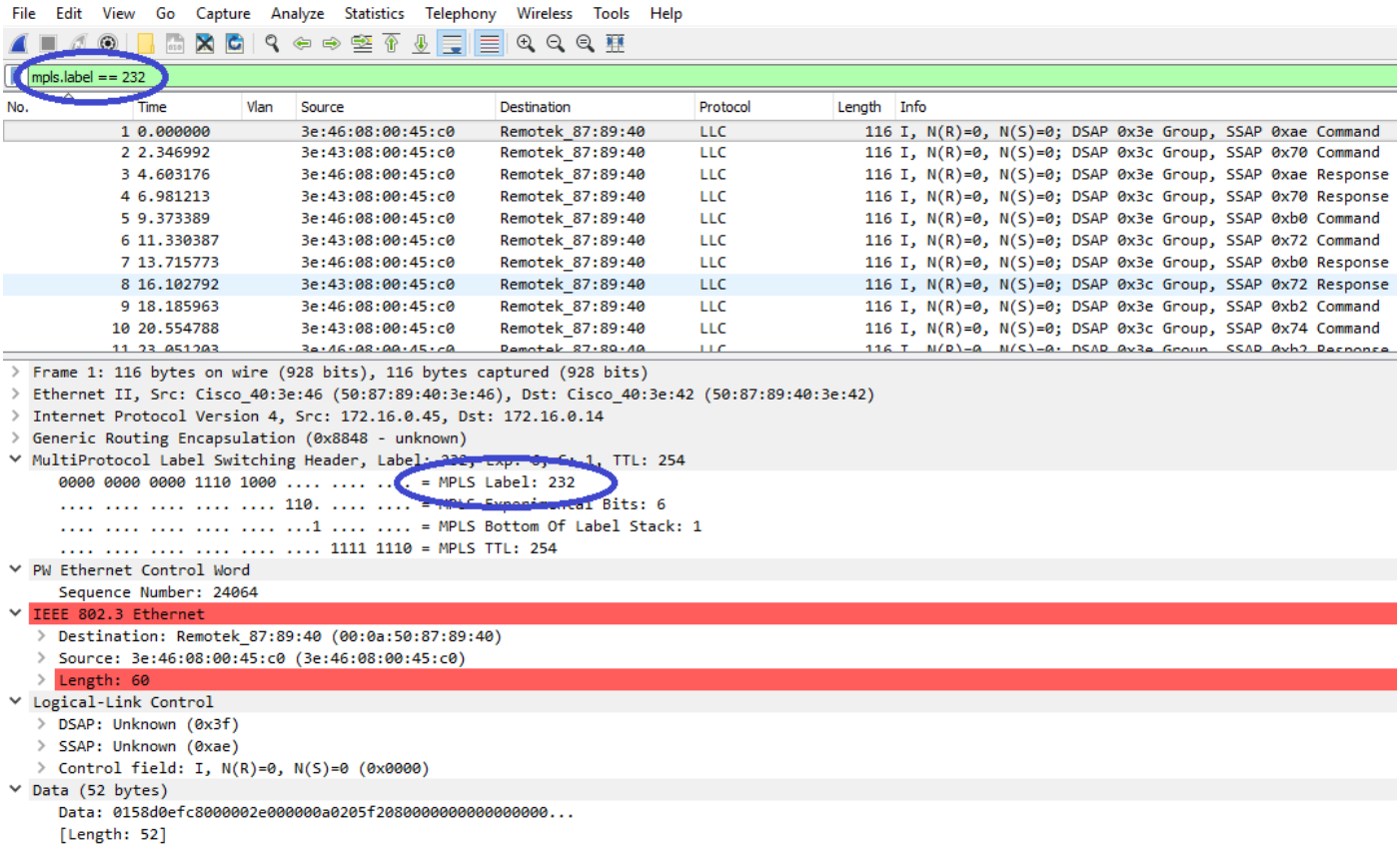
Nadat deze verandering door op OK te klikken is aangebracht, zal het gereedschap Wireshark analyse inhoud van de met OTV ingekapselde pakketten correct weergeven.



Wireshark toont correct inhoud van OTV ingekapselde pakketten

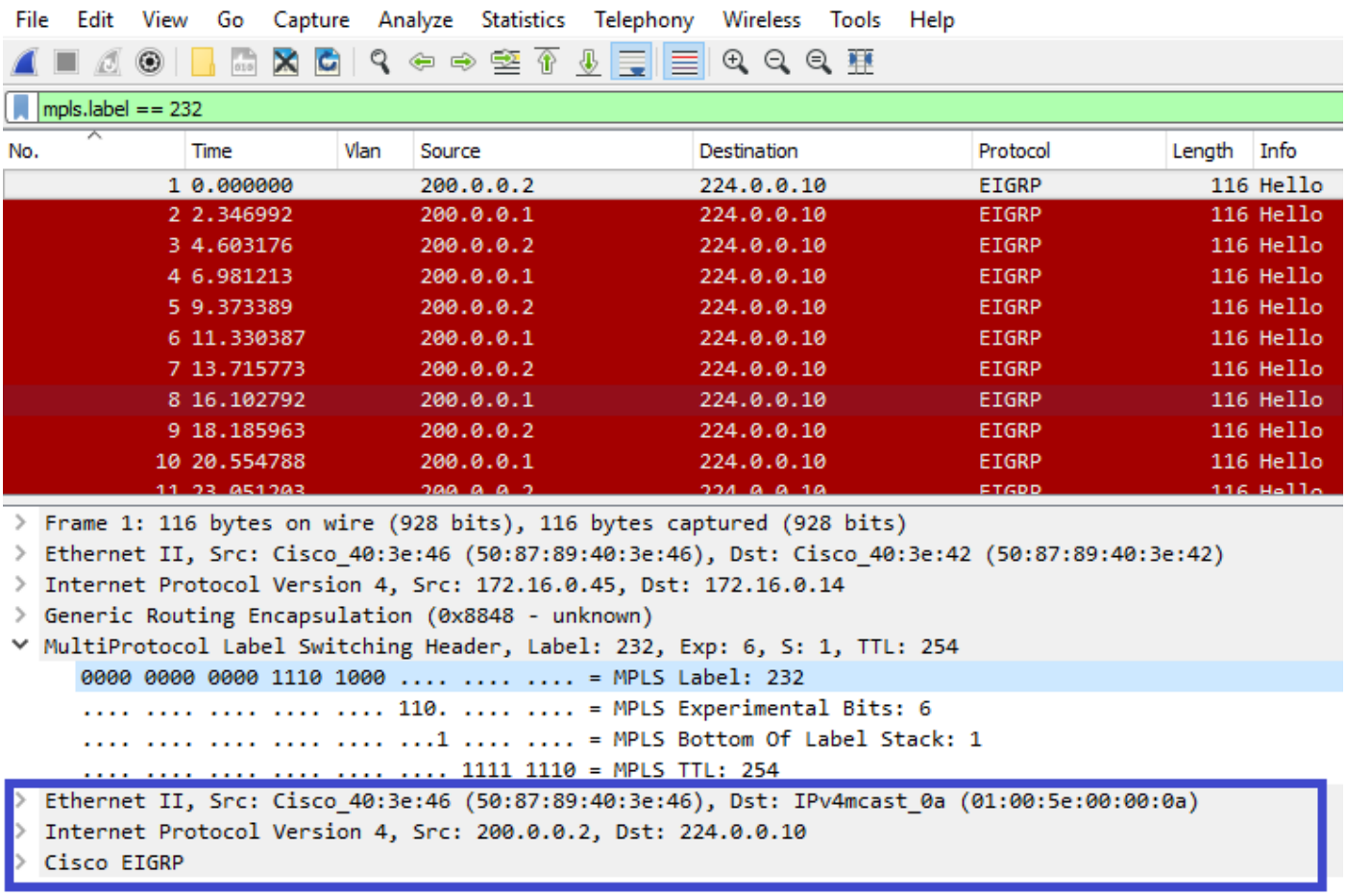
Decode-pakketten in VLAN 200

Bovenstaande stappen zijn van toepassing op alle VLAN's die via OTV zijn uitgebreid. Met een Wireshark filter bijvoorbeeld om alleen pakketten van VLAN 200 weer te geven, krijgen we de volgende output in een analyse tool.



Weergave-pakketten voor VLAN 200, uitgebreid via OTV

Zodra Wireless-shark is geïnstrueerd om de eerste paar bytes van MPLS-pakket niet te interpreteren als PW Control Word, kan het decodeproces worden voltooid.



WIreshark toont correct Vlan 200 verkeer als pakketten EHW

Gebruik de optie Bewerken om de OTV-header te verwijderen

Meestal worden draadloze installaties geleverd met een *bewerkingsgereedschap* voor de opdrachtregel, genaamd *Editcap*. Met dit gereedschap kan OTV-overhead van de opgenomen pakketten permanent worden verwijderd. Hiermee kan de opgenomen pakketten eenvoudig worden weergegeven en geanalyseerd in de WinShark Graphical User Interface (GUI), zonder dat u het ontkenningsgedrag van Wireshark handmatig hoeft aan te passen.

Editcap op Windows platform uitvoeren

Op het besturingssysteem van Windows wordt *Editcap.exe* standaard geïnstalleerd in een directory c:\Program Files\Wireshark.

Start dit gereedschap met *-C* vlag om OTV-overhead te verwijderen en bewaar het resultaat in een *.pcap-* bestand.

```
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>
```

Editcap op Mac OS-platform uitvoeren

Op het Mac OS-besturingssysteem is de bewerkingsdop beschikbaar in de map /usr/local/bin.

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

Door de OTV-header van opgenomen pakketten te verwijderen met*Editcap*werktuigBovendien verliest men VLAN-informatie die is gecodeerd als onderdeel van de MPLS-header, die op zijn beurt een onderdeel is van het OTV-scherm. Vergeet niet om 'mpls.label == <<lan nummer verlengd via OTV> + 32>' Wireshark GUI filter te gebruiken voordat de OTV-header wordt verwijderd met *Editcap* tool als alleen een VLAN-unit moet worden geanalyseerd.

Conclusie

Problemen oplossen en Cisco OTV oplossingen vereisen een goed begrip van de technologie, zowel vanuit het perspectief van de bediening van het besturingsplane als van de insluiting van het gegevensvliegtuig. Effectief het toepassen van de kennis, kunnen de middelen van de vrije pakketanalyse zoals Wireshark zeer krachtig in OTV pakketanalyse blijken. Naast de verschillende opties voor pakketweergave biedt de standaardinstallatie voor Windows op een pakketbewerkingsgereedschap dat de pakketanalyse kan vereenvoudigen. Hierdoor kan de probleemoplossing worden toegespitst op de onderdelen van de pakketinhoud die het meest relevant zijn voor een bepaalde sessie voor probleemoplossing.