Wireshark zur Fehlerbehebung bei OTV-Lösungen verwenden

Inhalt

Einführung

In diesem Dokument wird die Verwendung von Wireshark, einem bekannten Tool für die Paketerfassung und -analyse mit Freeware, bei der Fehlerbehebung für die Cisco OTV-Lösung veranschaulicht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Overlay Transport Virtualization (OTV) auf Switches der Nexus-Serie
- Grundlagen von Multiprotocol Label Switching (MPLS) Layer-2 Virtual Private Networks (VPNs)
- Wireshark, ein kostenloser und Open-Source-Paketanalysator (https://www.wireshark.org)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Nexus Switch-Plattform der Serie 7000.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

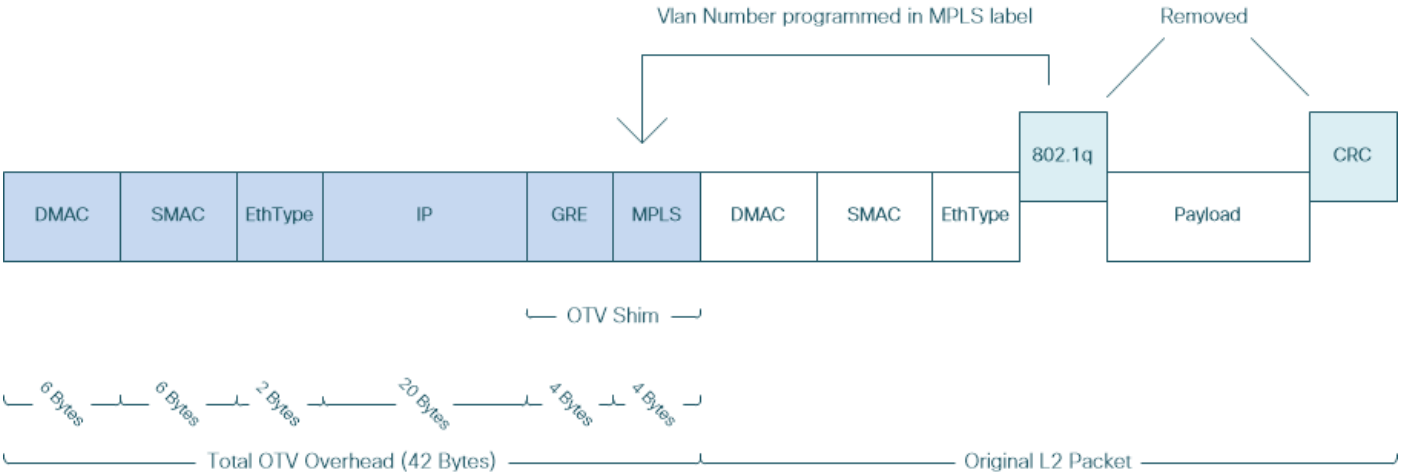
(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Beschreibung des Problems

Bei der Behebung von Netzwerkproblemen in VPN-Umgebungen umfasst eine der Techniken die Erfassung und Analyse gekapselter Pakete. In Cisco OTV-Netzwerkumgebungen ist dieser Ansatz jedoch mit einer gewissen Herausforderung verbunden. Häufig verwendete Paketanalysetools wie Wireshark, eine kostenloser und Open Source Packet Analyzer, kann den Inhalt des OTV-gekapselten Datenverkehrs möglicherweise nicht korrekt interpretieren. Daher sind aufwändige Workarounds wie die Extraktion gekapselter Daten aus einem OTV-Paket normalerweise erforderlich, um eine Datenanalyse erfolgreich durchführen zu können.

OTV-Paketformat

Die OTV-Kapselung erhöht die MTU-Gesamtgröße des Pakets um 42 Byte. Dies ist das Ergebnis des Betriebs des OTV-Edge-Geräts, das das CRC-Feld und die 802.1Q-Felder aus dem ursprünglichen Layer-2-Frame entfernt und einen OTV-Shim (der auch die VLAN- und Overlay-ID-Informationen enthält) sowie einen externen IP-Header hinzufügt.



Bei MPLS-L2VPN-Lösungen verfügen die Geräte im Underlay-Netzwerk nicht über genügend Informationen, um die Payload des MPLS-Pakets korrekt zu decodieren. In der Regel ist dies kein Problem, da die Paketweiterleitung in einem MPLS-Core-Netzwerk auf Labels basiert. Daher ist keine detaillierte Analyse des Inhalts von MPLS-Paketen im zugrunde liegenden Netzwerk erforderlich.

Dies stellt jedoch eine Herausforderung dar, wenn eine Datenanalyse von OTV-Paketen für Fehlerbehebungs- und/oder Überwachungszwecke erforderlich ist.

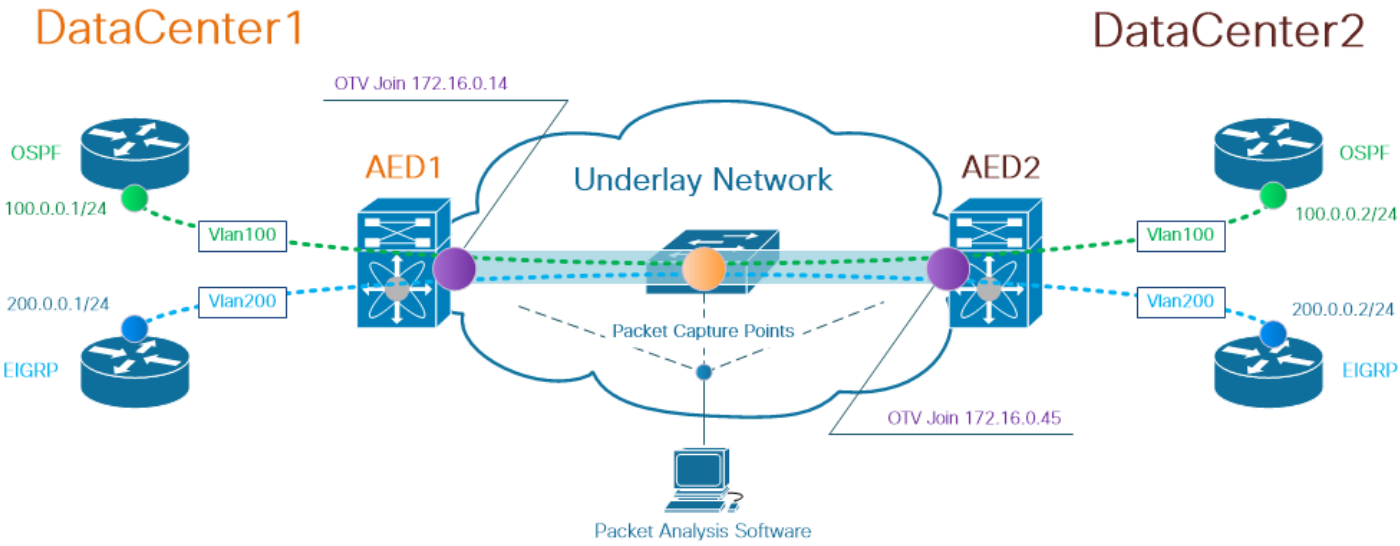
Paketanalysetools wie Wireshark versuchen, Paketdaten, die dem MPLS-Header folgen, zu dekodieren, indem sie die üblichen Regeln für die MPLS-Paketanalyse anwenden. Da jedoch möglicherweise keine Informationen über die Ergebnisse der Control Word-Aushandlung vorliegen, die normalerweise zwischen MPLS-L2VPN-Head-End- und Tail-End-Routern durchgeführt wird, setzen die Paketanalyse-Tools auf das Standardparsing-Verhalten zurück und wenden es auf Paketdaten an, die dem MPLS-Header folgen.

Hinweis: In MPLS-L2VPN-Lösungen, wie z. B. Any Transport Over MPLS (ATOM), handeln Pseudowire-Endpunkte die Verwendung von Control Word-Parametern aus. Ein Kontrollwort ist ein optionales 4-Byte-Feld zwischen dem MPLS-Label-Stack und der Layer-2-Nutzlast im Pseudowire-Paket. Das Kontrollwort enthält generische und Layer-2-Payload-spezifische Informationen. Wenn das C-Bit auf 1 festgelegt ist, erwartet der Werbe-Provider-Edge (PE), dass das Kontrollwort in jedem Pseudowire-Paket auf dem Pseudowire vorhanden ist, das signalisiert wird. Wenn das C-Bit auf 0 gesetzt ist, wird kein Kontrollwort erwartet.

Daher interpretiert das standardmäßige Wireshark-Analyseverhalten OTV-Pakete möglicherweise nicht korrekt, wodurch die Fehlerbehebung im OTV-Netzwerk komplexer wird.

Topologie

Im Folgenden sehen Sie ein Netzwerkdiagramm eines einfachen OTV-Netzwerks. Router in VLAN 100 und VLAN 200 stellen OSPF- und EIGRP-Adjacencies zwischen zwei DataCenter, DataCenter1 und DataCenter2 her. Die Data Center Interconnect (DCI) wird mit dem OTV-Tunnel zwischen N7k-Switches implementiert, der im Diagramm als AED1 und AED2 angezeigt wird.



Hinweis: Die OTV-Lösung von Cisco verwendet das Konzept der AED-Rolle (Authoritative Edge Device), das Netzwerkgeräten zugewiesen wird, die den OTV-Datenverkehr an einem bestimmten Standort kapselt und entkapselt.

Die Herausforderung, die bei Tunneling-Lösungen häufig auftritt, besteht darin, zu überprüfen, ob ein bestimmter Typ von Overlay-Paketen (IGP, FHRP usw.) ihn zu bestimmten Punkten im Underlay-Netzwerk bringt. Als Beispiel wird OSPF- und EIGRP-Overlay-Datenverkehr verwendet.

Paketerfassung

Es gibt mehrere Möglichkeiten, eine Paketerfassung im Netzwerk durchzuführen. Eine Option ist die Verwendung der Cisco Switched Port Analyzer (SPAN)-Funktion, die auf Cisco Catalyst- und Cisco Nexus Switching-Plattformen verfügbar ist.

Im Rahmen der Fehlerbehebung müssen möglicherweise an mehreren Stellen Paketerfassungen durchgeführt werden. OTV Join-Schnittstellen und -Schnittstellen im Underlay-Netzwerk können

als SPAN-Paketerfassungspunkt verwendet werden.

Lösung

Die Wireshark-Standardanalyseengine kann die ersten paar Bytes eines OTV-gekapselten Overlay-Pakets falsch interpretieren, als ob sie Teil von Pseudowire Emulation Edge-to-Edge (PWE3) Control Word sind, das in der Regel in MPLS-L2VPNs über ein MPLS-Paketvermittlungsnetzwerk verwendet wird.

> **Hinweis**: MPLS Pseudowire Emulation Edge-to-Edge (PWE3) Control Word wird im übrigen Dokument als *Kontrollwort* bezeichnet.

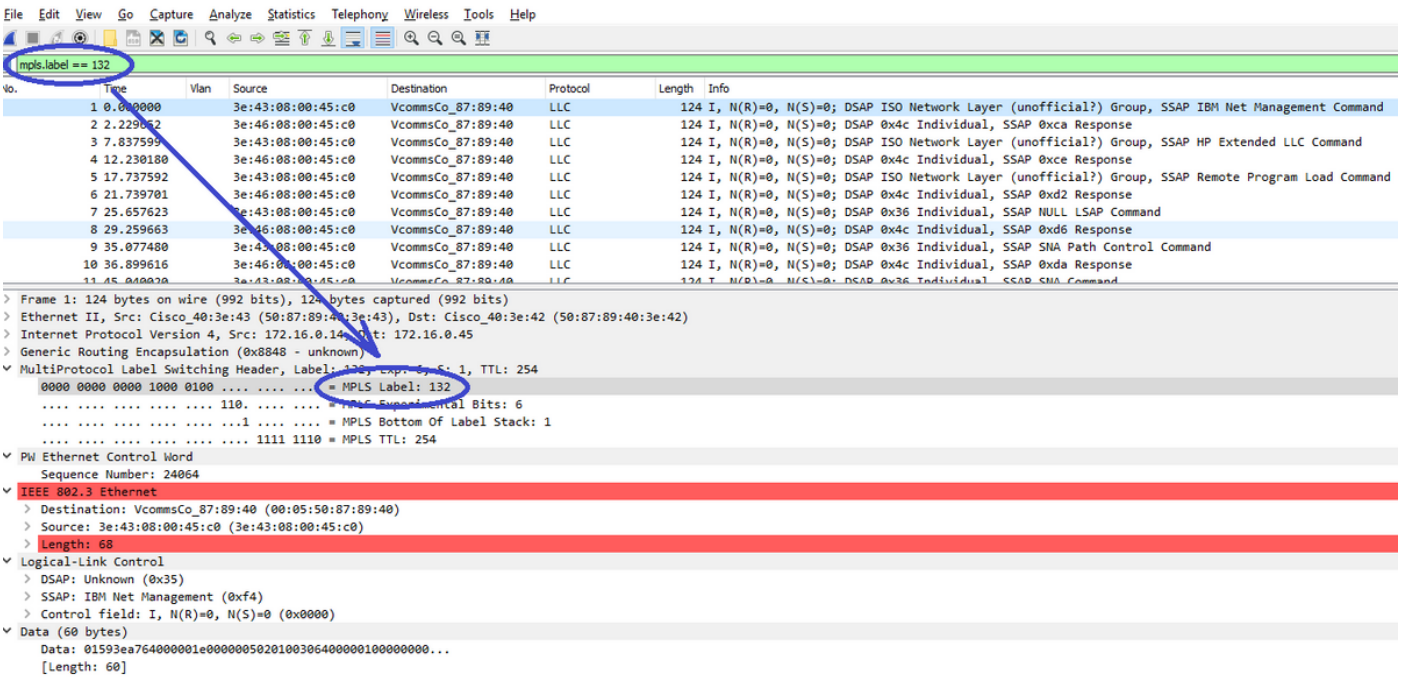
Um sicherzustellen, dass das Wireshark-Paketanalysetool den Inhalt von OTV-gekapselten Paketen korrekt interpretiert, ist eine manuelle Anpassung an den Paketdecodierungsprozess erforderlich.

> **Hinweis**: Das im OTV-Header verwendete MPLS-Label entspricht der Overlay-VLAN-Nummer + 32.

Decodieren von Paketen in VLAN 100

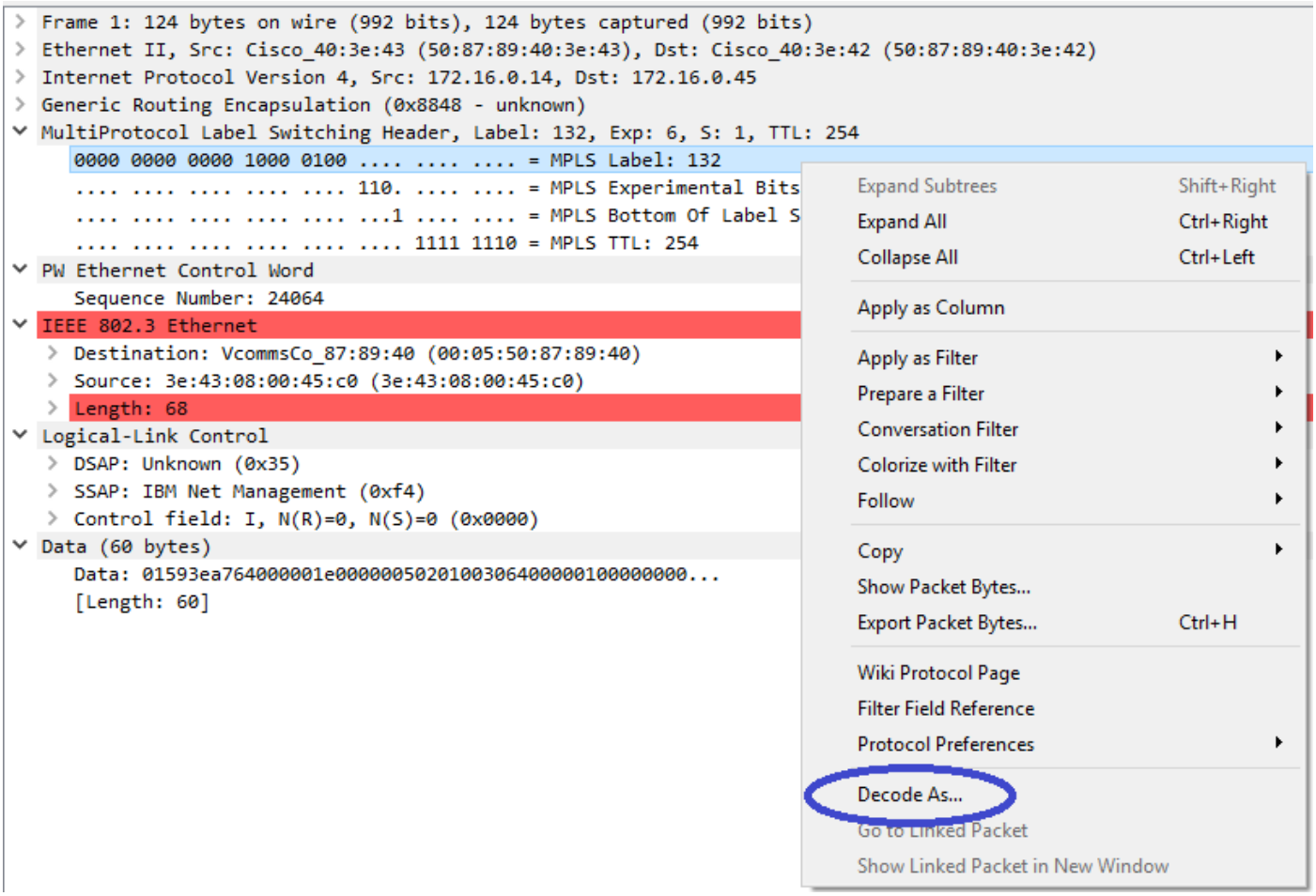
In einem ersten Schritt des Decodierungsprozesses werden nur OTV-gekapselte Pakete angezeigt, die den Inhalt des OTV-erweiterten VLAN 100 enthalten. Verwendeter Filter ist mpls.label == 132, der VLAN 100 darstellt.

> **Hinweis**: Um OTV-gekapselte Pakete für ein bestimmtes VLAN anzuzeigen, das über OTV erweitert wurde, verwenden Sie den folgenden Wireshark-Anzeigefilter: mpls.label == <<VLAN-Nummer, die über OTV> + 32> erweitert wurde.



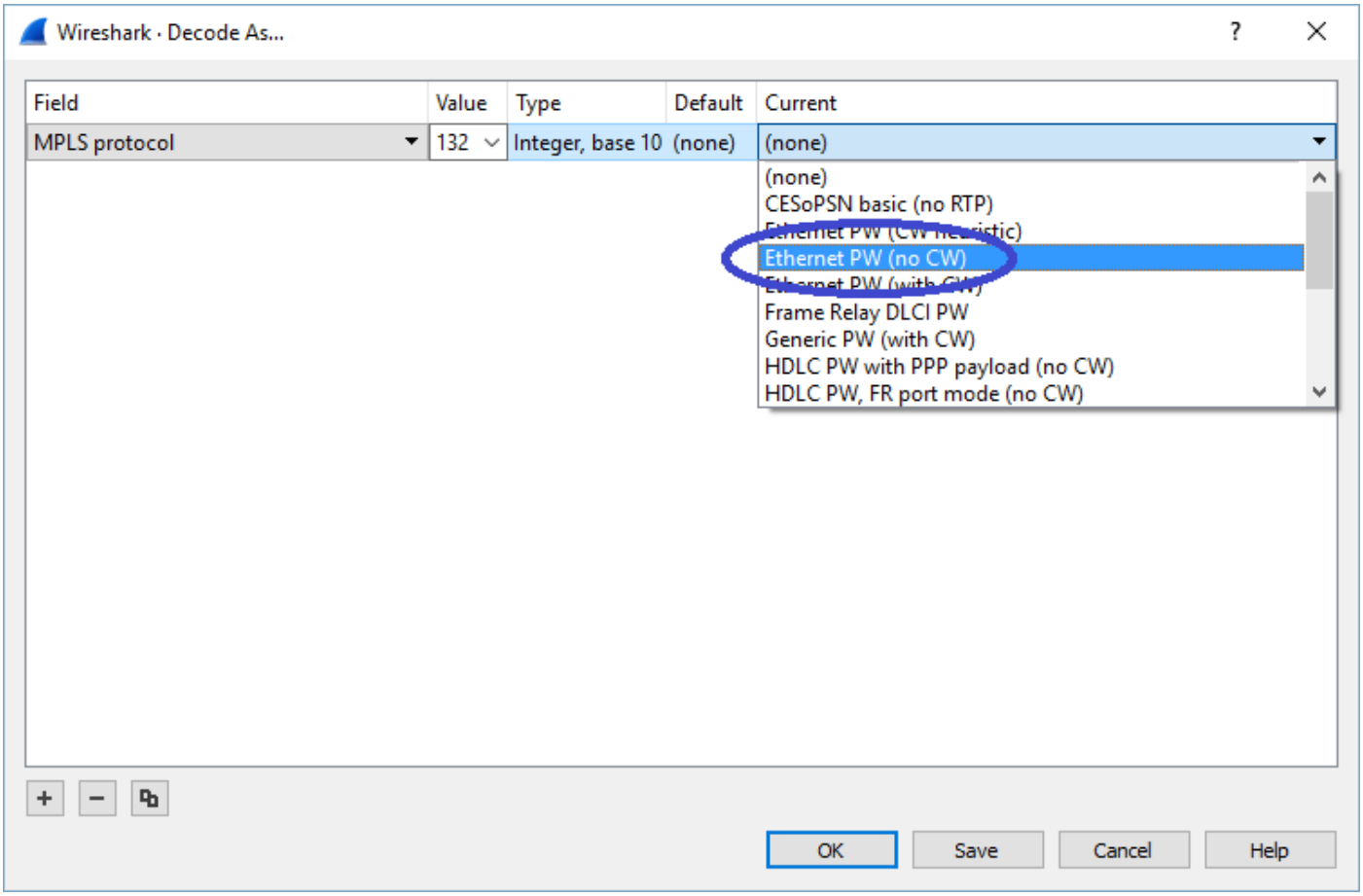
Anzeigen von OTV-gekapselten Paketen für VLAN 100, erweitert auf OTV

Standardmäßig interpretiert Wireshark die ersten vier Byte des Inhalts von MPLS-L2VPN-Paketen als Control Word. Dies muss für OTV-gekapselte Pakete korrigiert werden. Klicken Sie dazu mit der rechten Maustaste auf das Feld für das MPLS-Label der Pakete und wählen Sie *Decode As.. (Als..).* Option.



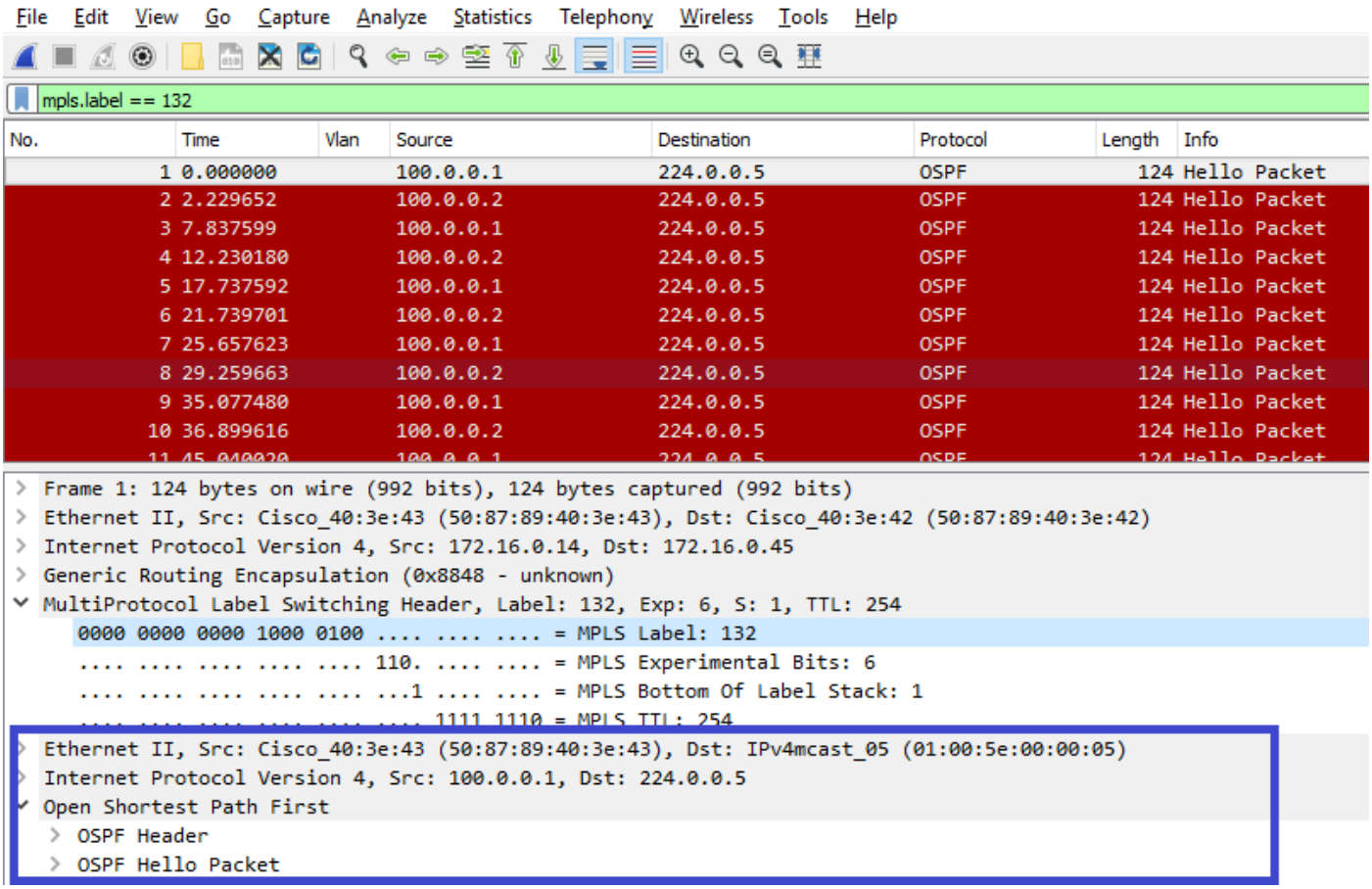
Klicken Sie mit der rechten Maustaste auf das Feld für das MPLS-Label, und wählen Sie Decode As.. Option

Der nächste Schritt besteht darin, Wireshark mitzuteilen, dass gekapselte Inhalte kein Control Word haben.



Option "Kein CW" auswählen

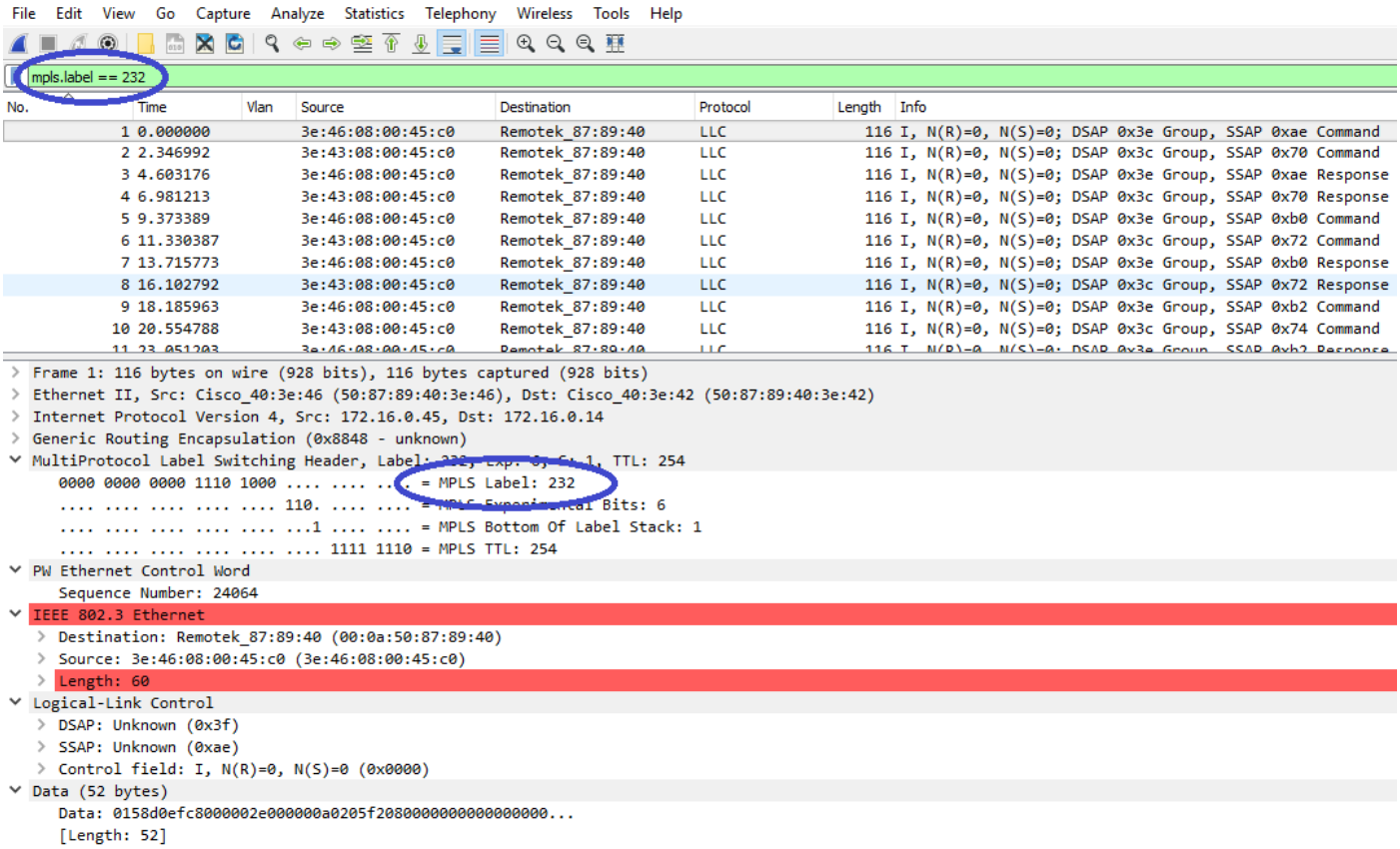
Nachdem diese Änderung über die Schaltfläche OK gesendet wurde, zeigt das Wireshark-Analyse-Tool den Inhalt der OTV-gekapselten Pakete korrekt an.



Wireshark zeigt den Inhalt von OTV-gekapselten Paketen korrekt an

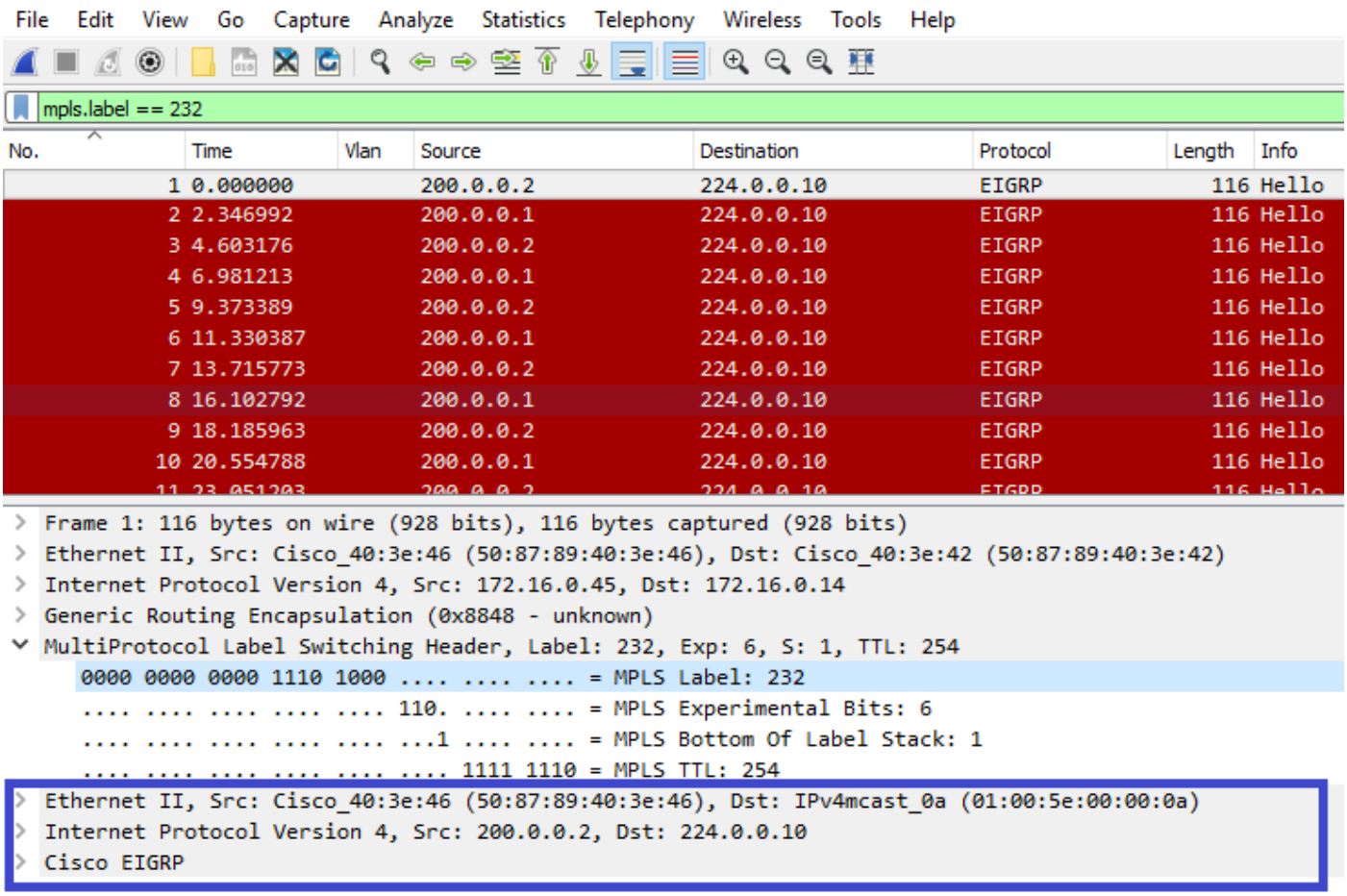
Decodieren von Paketen in VLAN 200

Die oben beschriebenen Schritte gelten für alle VLANs, die über OTV erweitert werden. Wenn Sie beispielsweise den Wireshark-Filter verwenden, um nur Pakete von VLAN 200 anzuzeigen, erhalten Sie die folgende Ausgabe im Analyse-Tool.



Anzeigepakete für VLAN 200, erweitert über OTV

Sobald Wireshark angewiesen ist, die ersten paar Byte des MPLS-Pakets nicht als PW Control Word zu interpretieren, kann der Dekodierungsprozess erfolgreich abgeschlossen werden.



WIreshark zeigt VLAN 200-Datenverkehr korrekt als EIGRP-Pakete an

Entfernen des OTV-Headers mithilfe von Editcap

In der Regel enthalten Wireshark-Installationen ein Paket-Bearbeitungstool für die Befehlszeile, das *Editcap* heißt. Dieses Tool kann den OTV-Overhead dauerhaft aus erfassten Paketen entfernen. Dies ermöglicht die einfache Anzeige und Analyse von erfassten Paketen in der grafischen Benutzeroberfläche von Wireshark, ohne dass das Parsing-Verhalten von Wireshark manuell angepasst werden muss.

Ausführen von Editcap auf Windows-Plattform

Unter Windows wird *editcap.exe* standardmäßig im Verzeichnis c:\Program Files\Wireshark> installiert.

Führen Sie dieses Programm mit *-C*-Flag aus, um OTV-Overhead zu entfernen und das Ergebnis in einer *.pcap*-Datei zu speichern.

```
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>
```

Ausführen von Editcap auf Mac OS-Plattform

Unter Mac OS ist editcap im Ordner /usr/local/bin verfügbar.

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

Durch Entfernen des OTV-Headers aus erfassten Paketen mit*Editcap*Werkzeugverliert man VLAN-Informationen, die als Teil des MPLS-Headers kodiert sind, der wiederum Teil des OTV-Shims ist. Denken Sie daran, den Wireshark-GUI-Filter "mpls.label == <<VLAN-Nummer, die über OTV> + 32> erweitert wurde, zu verwenden, bevor Sie den OTV-Header mit dem *Editcap*-Tool entfernen, wenn nur eine Analyse des Datenverkehrs eines bestimmten VLAN erforderlich ist.

Schlussfolgerung

Die Fehlerbehebung bei Cisco OTV-Lösungen erfordert ein gutes Verständnis der Technologie, sowohl hinsichtlich des Betriebs auf der Kontrollebene als auch hinsichtlich der Kapselung auf der Datenebene. Durch die effektive Anwendung des Wissens können sich Tools zur Analyse von Freeware-Paketen wie Wireshark bei der OTV-Paketanalyse als sehr leistungsstark erweisen. Zusätzlich zu den verschiedenen Paketanzeigeoptionen bietet die typische Wireshark-Installation ein Paketbearbeitungstool, das die Paketanalyse vereinfachen kann. Dadurch kann die Fehlerbehebung auf die Teile des Paketinhalts konzentriert werden, die für eine bestimmte Sitzung zur Fehlerbehebung am relevantesten sind.