Utilizzare Wireshark per risolvere i problemi relativi alle soluzioni OTV

Sommario

Introduzione

Questo documento dimostra l'uso di Wireshark, un noto strumento di analisi e acquisizione di pacchetti freeware, per la risoluzione dei problemi delle soluzioni Cisco OTV.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Overlay Transport Virtualization (OTV) su switch serie Nexus
- Nozioni fondamentali sulle reti VPN (Virtual Private Network) di layer 2 Multiprotocol Label Switching (MPLS)
- Wireshark, un analizzatore di pacchetti open source e gratuito (https://www.wireshark.org)

Componenti usati

Per la stesura del documento, è stata usata la piattaforma dello switch Nexus serie 7000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

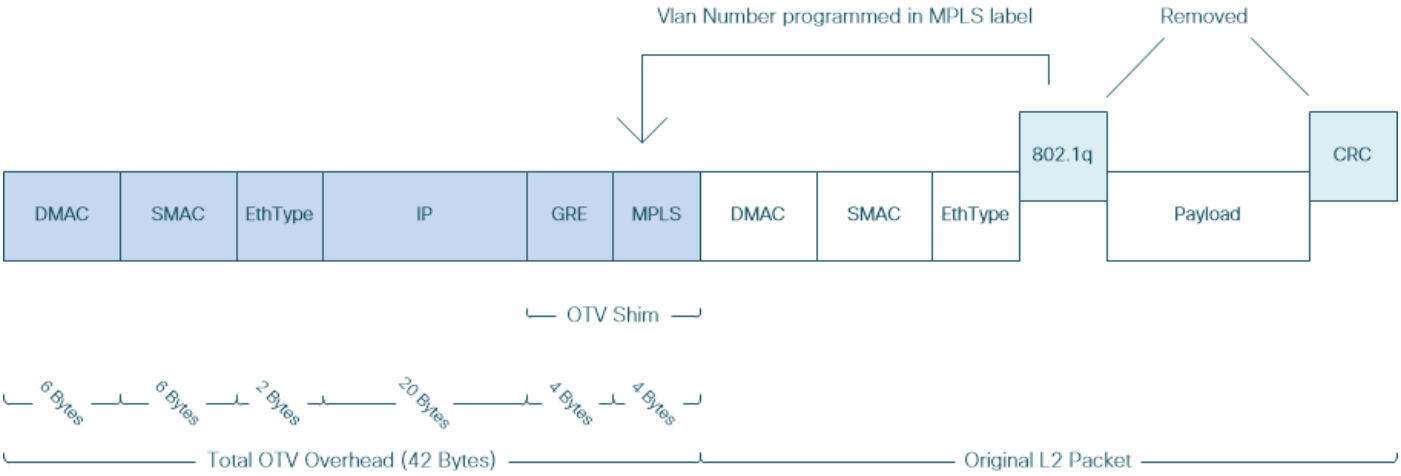
conseguenze derivanti dall'uso dei comandi.

Descrizione del problema

Quando si risolvono i problemi di rete in ambienti VPN, una delle tecniche prevede l'acquisizione e l'analisi dei pacchetti incapsulati. Tuttavia, negli ambienti di rete Cisco OTV, questo approccio viene incontro a una certa sfida. Strumenti di analisi dei pacchetti comunemente utilizzati, come Wireshark, a analizzatore di pacchetti open source e gratuito, potrebbe non interpretare correttamente il contenuto del traffico incapsulato OTV. Pertanto, per eseguire correttamente l'analisi dei dati, sono in genere necessarie soluzioni laboriose, come l'estrazione di dati incapsulati da un pacchetto OTV.

Formato pacchetto OTV

L'incapsulamento OTV aumenta le dimensioni MTU complessive del pacchetto di 42 byte. Questo è il risultato del funzionamento del dispositivo OTV Edge che rimuove il CRC e i campi 802.1Q dal frame di layer 2 originale e aggiunge uno slot OTV (contenente anche le informazioni sull'ID della VLAN e della sovrapposizione) e un'intestazione IP esterna.



Nelle soluzioni MPLS L2VPN, i dispositivi nella rete sottostante non dispongono di informazioni sufficienti per decodificare correttamente il payload del pacchetto MPLS. In genere, questo non è un problema, poiché l'inoltro dei pacchetti in una rete principale MPLS viene eseguito in base alle etichette, non è necessaria un'analisi approfondita del contenuto dei pacchetti MPLS nella rete sottostante.

Tuttavia, questa operazione può essere problematica se l'analisi dei dati dei pacchetti OTV è richiesta a scopo di risoluzione dei problemi e/o monitoraggio.

Gli strumenti di analisi dei pacchetti, ad esempio Wireshark, tentano di decodificare i dati del pacchetto che seguono l'intestazione MPLS applicando le normali regole di analisi dei pacchetti MPLS. Tuttavia, poiché potrebbe non contenere informazioni sui risultati della negoziazione Control Word, che verrebbe normalmente eseguita tra router headend L2VPN e router finali MPLS, gli strumenti di analisi dei pacchetti tornano al comportamento di analisi predefinito e li applicano ai dati dei pacchetti che seguono l'intestazione MPLS.

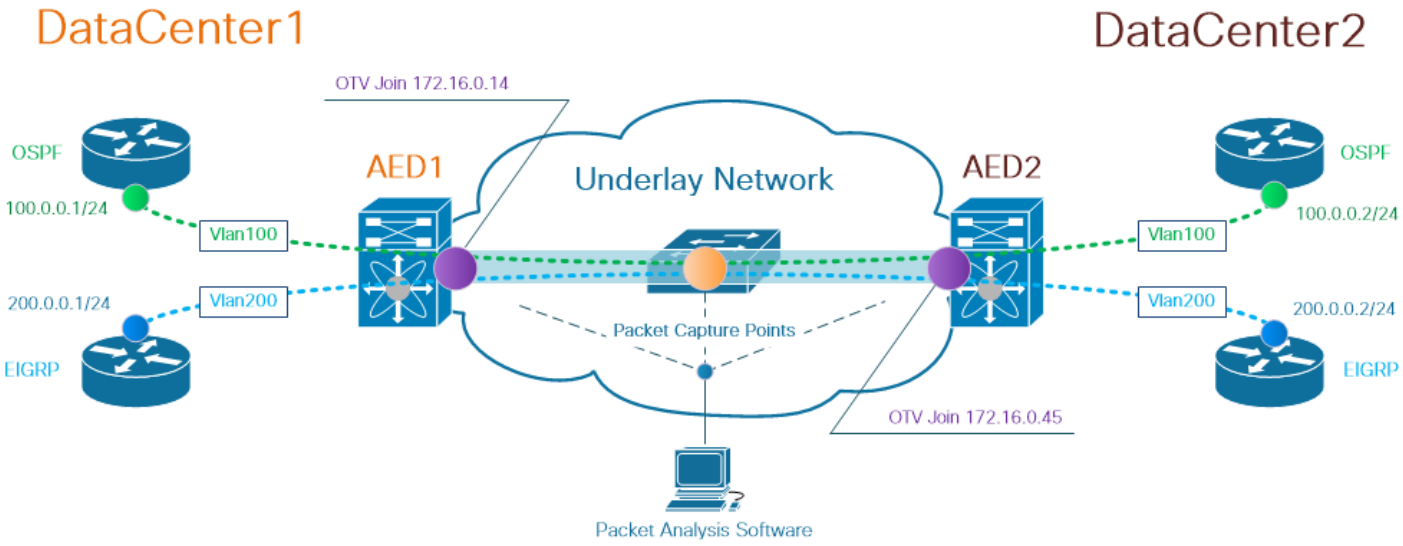
Nota: Nelle soluzioni MPLS L2VPN, ad esempio Any Transport Over MPLS (ATOM), gli

endpoint di tipo pseudowire negoziano l'utilizzo del parametro Control Word. Una parola di controllo è un campo opzionale di 4 byte situato tra lo stack di etichette MPLS e il payload di layer 2 nel pacchetto pseudowire. La parola di controllo contiene informazioni generiche e specifiche del payload di layer 2. Se il bit C è impostato su 1, il provider di pubblicità Edge (PE) si aspetta che la parola di controllo sia presente in ogni pacchetto di pseudofili sullo pseudofilo segnalato. Se il bit C è impostato su 0, non è prevista alcuna parola di controllo.

Di conseguenza, il comportamento di analisi predefinito di Wireshark potrebbe non interpretare correttamente il contenuto dei pacchetti OTV, rendendo più complessa la risoluzione dei problemi della rete OTV.

Topologia

Di seguito è riportato un diagramma di rete di una semplice rete OTV. I router della Vlan 100 e della Vlan 200 stabiliscono adiacenze OSPF ed EIGRP tra due data center, rispettivamente DataCenter1 e DataCenter2. Il protocollo DCI (Data Center Interconnect) viene implementato con il tunnel OTV tra gli switch N7k, che nel diagramma sono rappresentati come AED1 e AED2.



Nota: la soluzione Cisco OTV utilizza il concetto di ruolo Authoritative Edge Device (AED), assegnato al dispositivo di rete che incapsula e decapsula il traffico OTV in un particolare sito.

La sfida che si vede spesso nelle soluzioni di tunneling è verificare se un particolare tipo di pacchetto di sovrapposizione (IGP, FHRP, ecc.) lo porta a determinati punti della rete sottostante. Ad esempio, viene utilizzato il traffico di overlay OSPF ed EIGRP.

Acquisizione pacchetti

Esistono diversi modi per acquisire un pacchetto nella rete. Un'opzione consiste nell'utilizzare la funzionalità Cisco Switched Port Analyzer (SPAN), disponibile sulle piattaforme di switching Cisco Catalyst e Cisco Nexus.

Durante il processo di risoluzione dei problemi, potrebbe essere necessario acquisire i pacchetti in più punti. Le interfacce di join OTV e le interfacce nella rete sottostante possono essere usate come punto di acquisizione del pacchetto SPAN.

Soluzione

Il motore di analisi predefinito Wireshark può interpretare in modo errato i primi byte di un pacchetto di overlay incapsulato OTV come se facessero parte di Pseudowire Emulation Edge-to-Edge (PWE3) Control Word, che viene in genere utilizzato nelle VPN MPLS L2P su una rete a commutazione di pacchetto MPLS.

> **Nota:** PWE3 (MPLS Pseudowire Emulation Edge-to-Edge). Nel resto del documento, la parola di controllo viene indicata come *parola di controllo*.

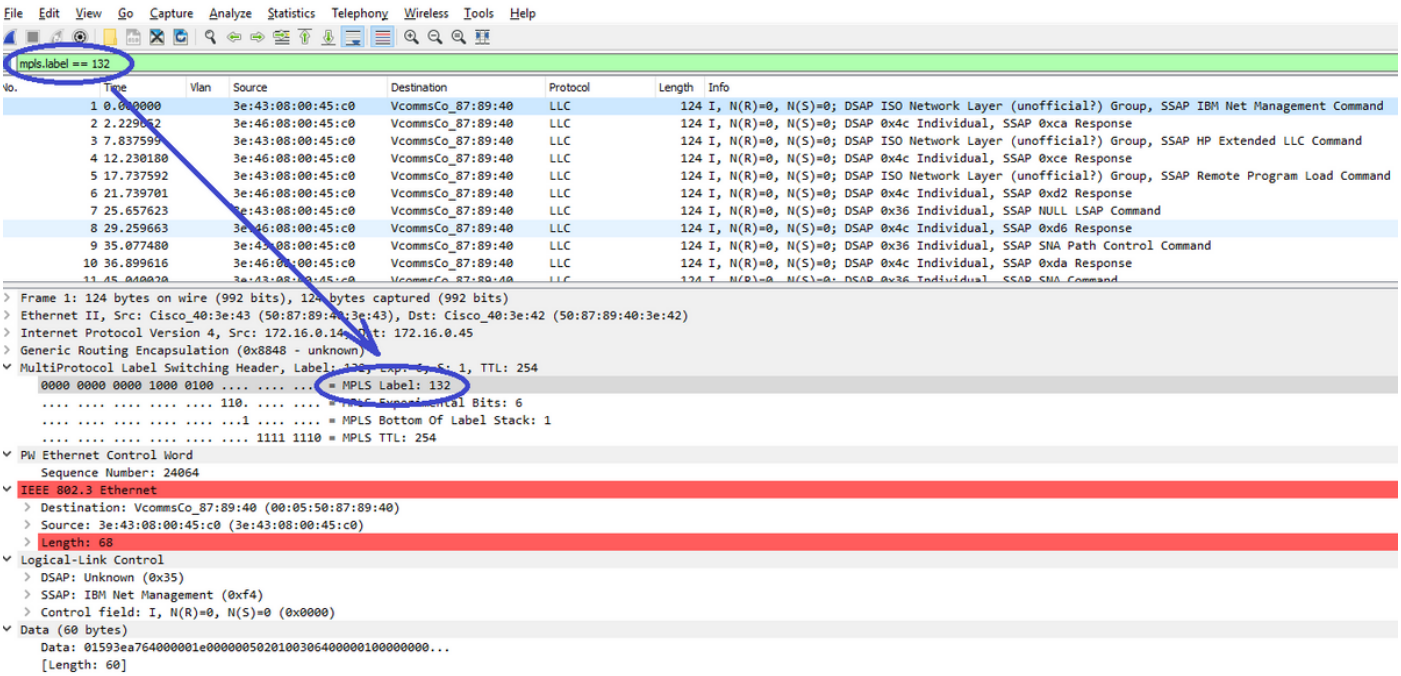
Per garantire che lo strumento di analisi dei pacchetti Wireshark interpreti correttamente il contenuto dei pacchetti incapsulati OTV, è necessario regolare manualmente il processo di decodifica dei pacchetti.

> **Nota:** L'etichetta MPLS utilizzata nell'intestazione OTV è uguale al numero di vlan sovrapposto + 32.

Decodifica dei pacchetti nella VLAN 100

Come primo passo del processo di decodifica, visualizzare solo i pacchetti incapsulati OTV che trasportano il contenuto della vlan estesa OTV 100. Il filtro usato è mpls.label == 132, che rappresenta la vlan 100.

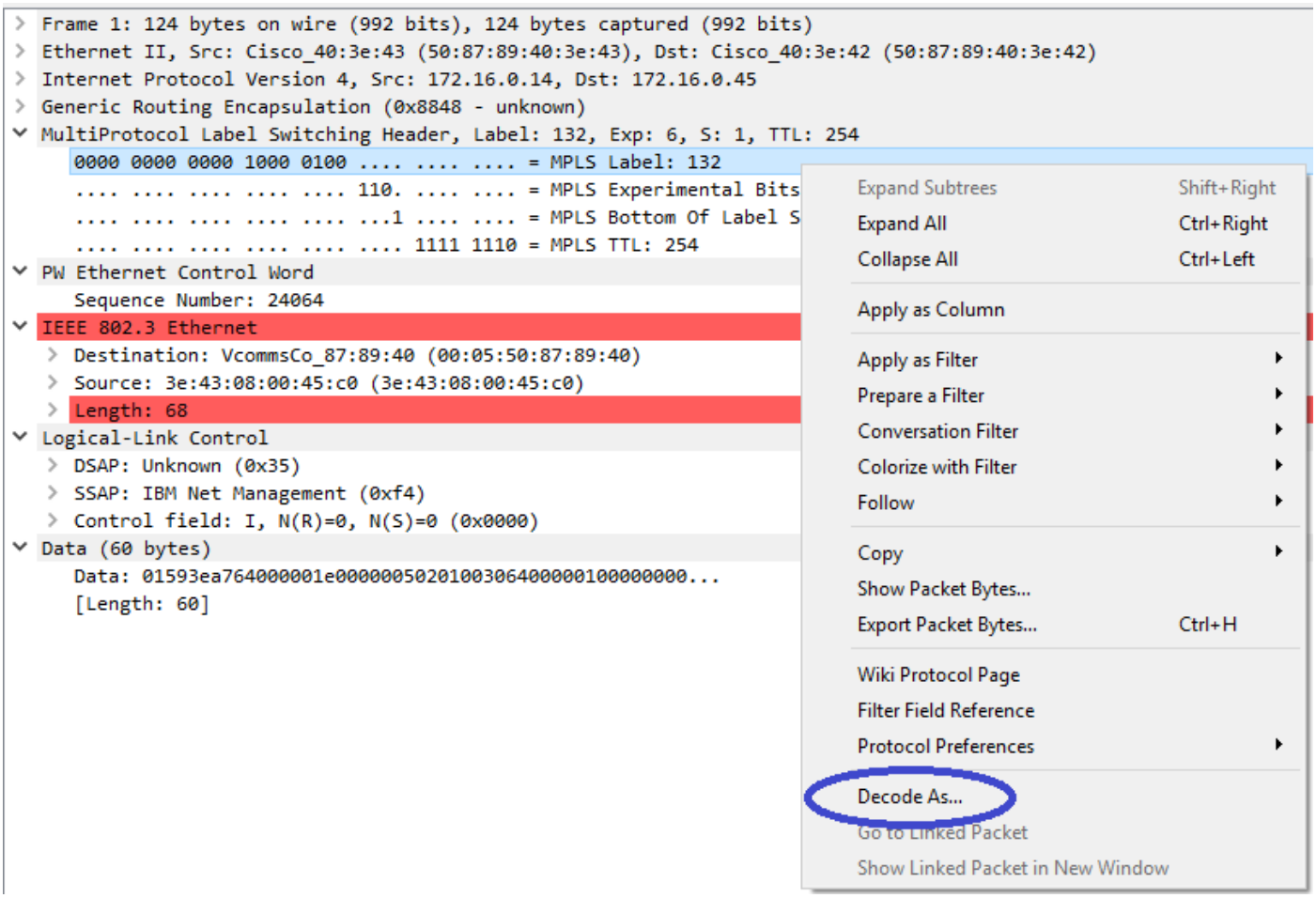
> **Nota:** Per visualizzare i pacchetti incapsulati da OTV per una particolare vlan estesa su OTV, usare il seguente filtro di visualizzazione Wireshark: mpls.label == <<numero vlan esteso su OTV> + 32>



Visualizza pacchetti incapsulati OTV per Vlan 100, estesi su OTV

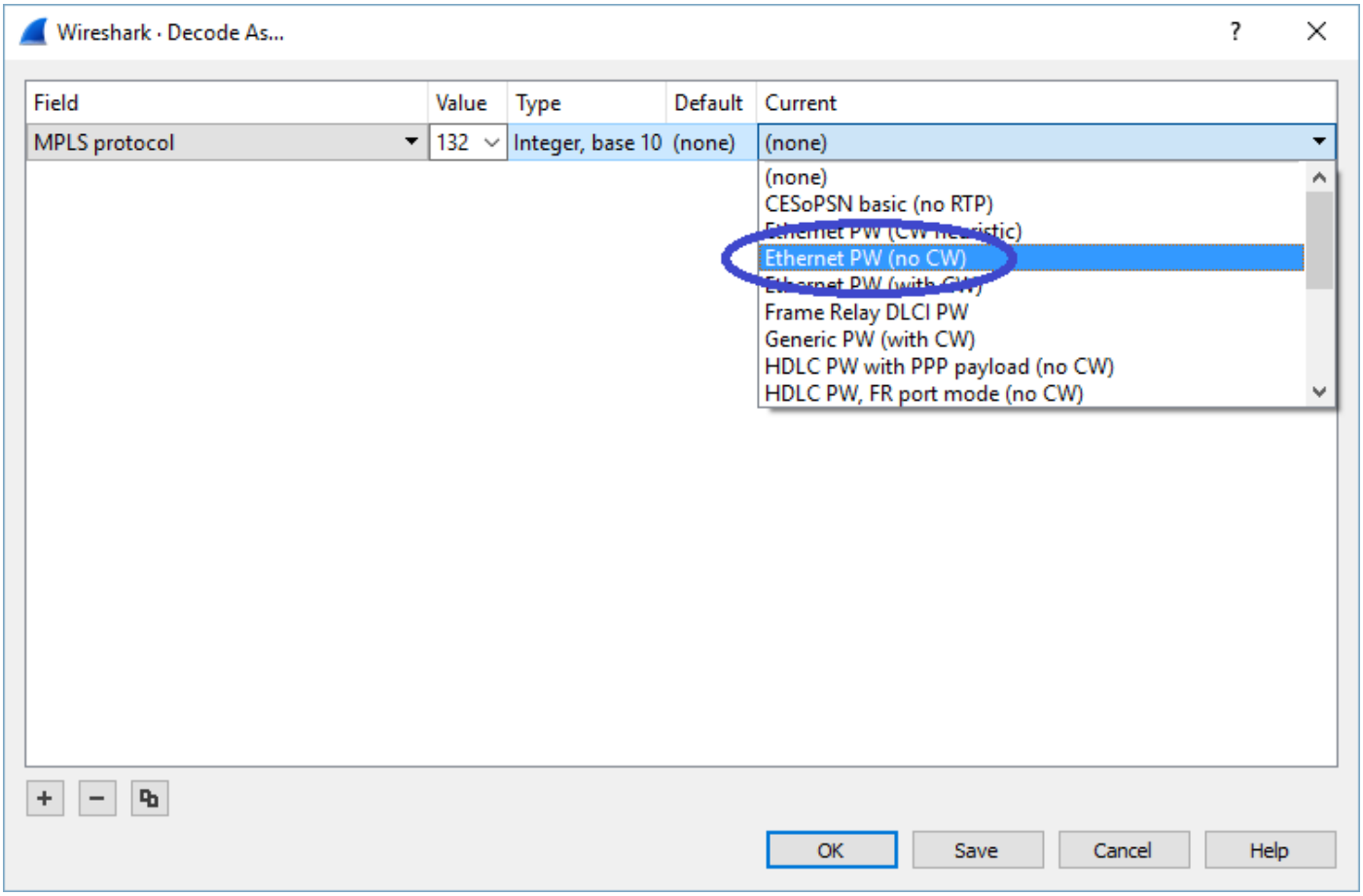
Per impostazione predefinita, Wireshark interpreta i primi quattro byte del contenuto dei pacchetti MPLS L2VPN come Control Word. Questo problema deve essere risolto con i pacchetti

incapsulati OTV. A tale scopo, fare clic con il pulsante destro del mouse sul campo etichetta MPLS di uno dei pacchetti e scegliere *Decodifica come...* opzionale.



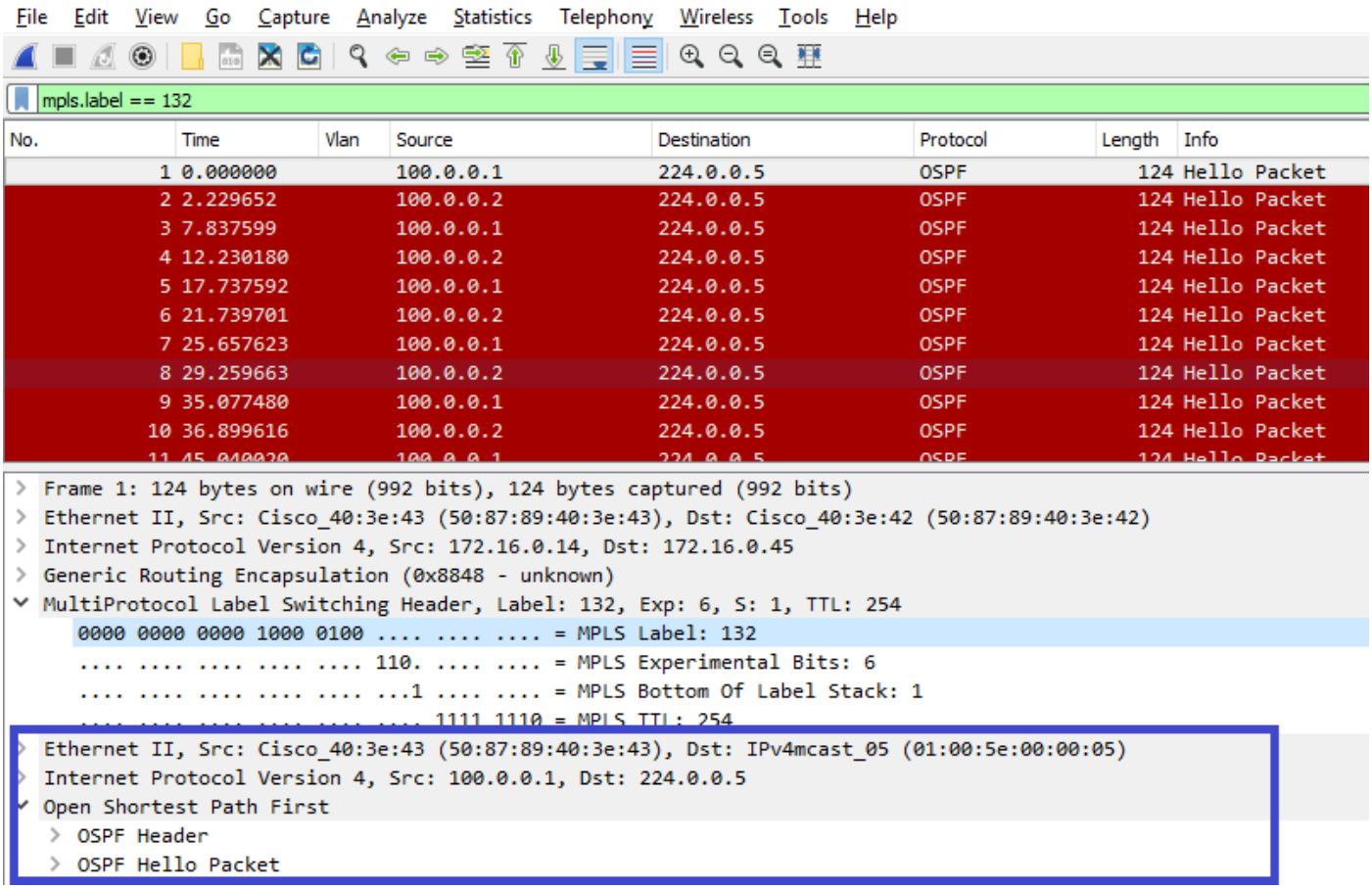
Fare clic con il pulsante destro del mouse sul campo etichetta MPLS e scegliere Decodifica come... opzione

Il passo successivo è quello di dire a Wireshark che il contenuto incapsulato non ha parole di controllo.



Selezionare l'opzione "Nessun peso variabile"

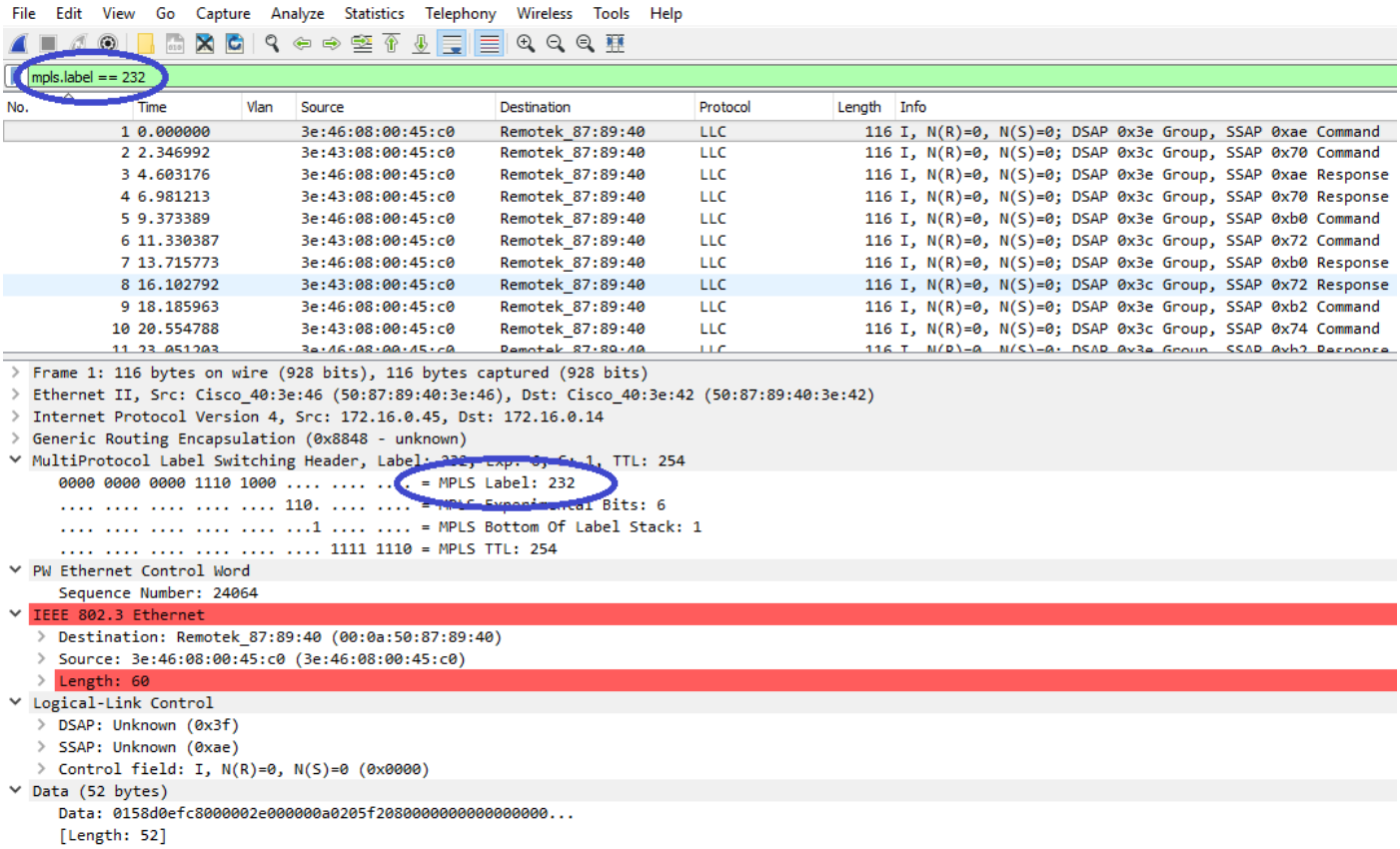
Dopo aver inviato la modifica facendo clic sul pulsante OK, lo strumento di analisi Wireshark visualizzerà correttamente il contenuto dei pacchetti incapsulati OTV.



Wireshark visualizza correttamente il contenuto dei pacchetti incapsulati OTV

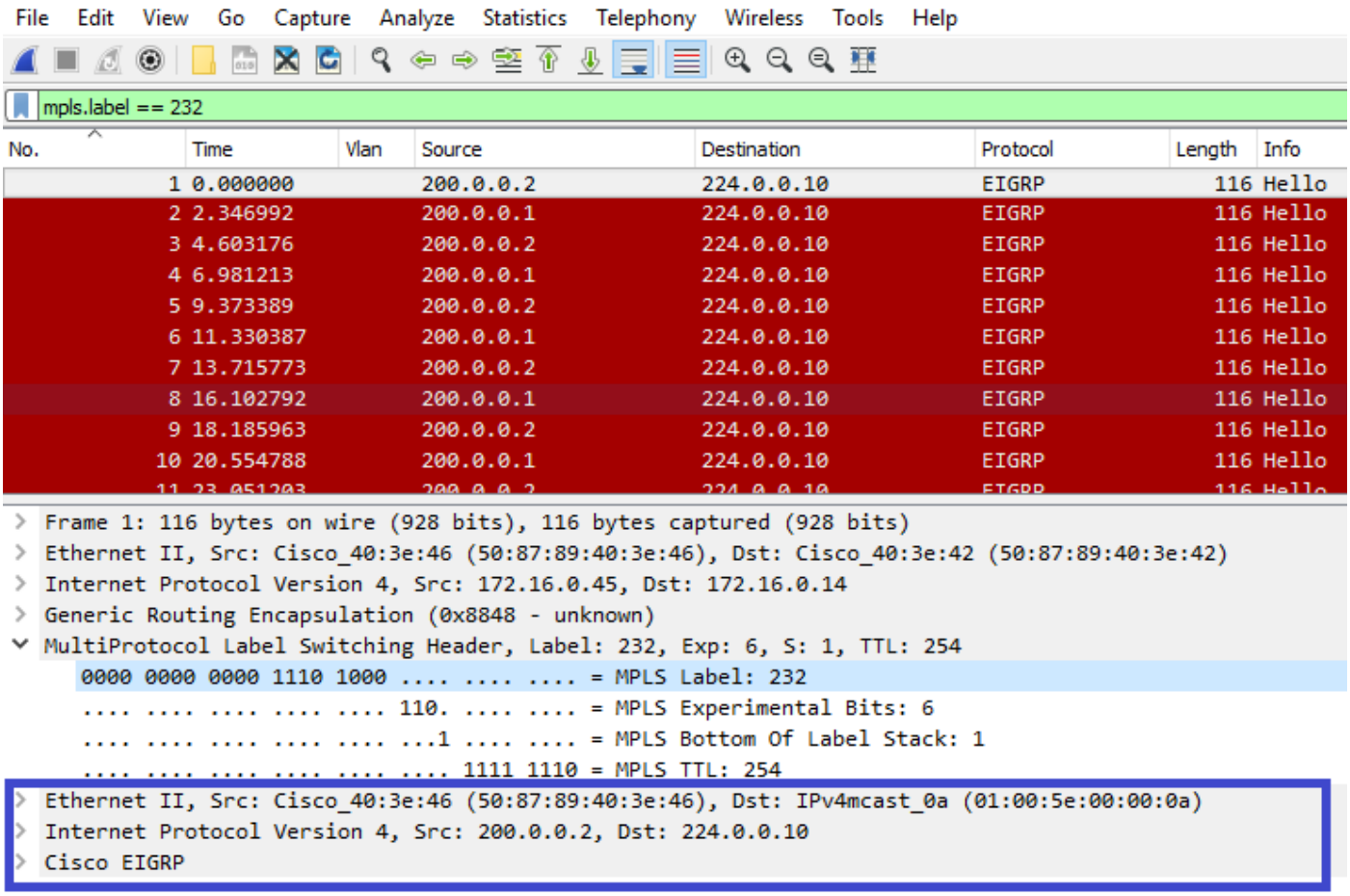
Decodifica dei pacchetti nella VLAN 200

Le fasi precedenti sono applicabili a tutte le vlan estese su OTV. Ad esempio, se si usa il filtro Wireshark per visualizzare solo i pacchetti della vlan 200, nello strumento di analisi viene restituito il seguente output.



Visualizza pacchetti per vlan 200, estesi su OTV

Quando a Wireshark viene chiesto di non interpretare i primi byte del pacchetto MPLS come PW Control Word, il processo di decodifica può essere completato correttamente.



WIreshark visualizza correttamente il traffico VLAN 200 come pacchetti EIGRP

Usa ModificaTap per rimuovere l'intestazione OTV

In genere, le installazioni di Wireshark vengono fornite con uno strumento di modifica dei pacchetti della riga di comando denominato *Editcap*. Questo strumento può rimuovere in modo permanente il sovraccarico OTV dai pacchetti acquisiti. Ciò consente una facile visualizzazione e analisi dei pacchetti catturati nell'interfaccia grafica di Wireshark (GUI), senza la necessità di regolare manualmente il comportamento di analisi di Wireshark.

Esegui Editcap su piattaforma Windows

Nel sistema operativo Windows, *editcap.exe* viene installato per impostazione predefinita nella directory c:\Programmi\Wireshark>.

Eseguire questo strumento con il flag *-C* per rimuovere il sovraccarico OTV e salvare il risultato in un file *.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>
```

Esegui Editcap sulla piattaforma Mac OS

Sul sistema operativo Mac OS, editcap è disponibile nella cartella /usr/local/bin.

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

Rimuovendo l'intestazione OTV dai pacchetti acquisiti con*Editcap*strumento, si perdono le informazioni sulla VLAN codificate come parte dell'intestazione MPLS, che a sua volta è parte della correzione rapida per la compatibilità OTV. Ricordare di usare il filtro GUI 'mpls.label == <<vlan number extended over OTV> + 32>' Wireshark prima di rimuovere l'intestazione OTV con lo strumento *Editcap*, se è richiesta l'analisi del traffico solo di una VLAN specifica.

Conclusioni

La risoluzione dei problemi delle soluzioni Cisco OTV richiede una buona comprensione della tecnologia, sia dal punto di vista del funzionamento del control plane sia da quello dell'incapsulamento del data plane. Applicando efficacemente la conoscenza, gli strumenti freeware packet analysis come Wireshark possono rivelarsi molto potenti nell'analisi dei pacchetti OTV. Oltre alle varie opzioni di visualizzazione dei pacchetti, la tipica installazione di Wireshark offre uno strumento di modifica dei pacchetti in grado di semplificare l'analisi dei pacchetti. In questo modo, la risoluzione dei problemi può essere focalizzata sulle parti del contenuto del pacchetto che sono più rilevanti per una particolare sessione di risoluzione dei problemi.