# Utilizzare Wireshark per risolvere i problemi relativi alle soluzioni OTV

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Descrizione del problema Formato pacchetto OTV Topologia Acquisizione pacchetti Soluzione Decodifica dei pacchetti nella VLAN 100 Decodifica dei pacchetti nella VLAN 200 Usa ModificaTap per rimuovere l'intestazione OTV Esegui Editcap su piattaforma Windows Esegui Editcap sulla piattaforma Mac OS Conclusioni

## 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.

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>

<u>F</u> ile <u>E</u> di	it <u>V</u> iew <u>G</u> o <u>C</u> aptur	e <u>A</u> nalyze <u>S</u> tatistics Tel	ephon <u>y W</u> ireless <u>T</u> ools <u>H</u> e	elp								
	🚺 🛒 🙆 📙 🛅 🗙 🖾 🔍 🗢 👄 🧟 🖉 💆 🚍 📃 Q, Q, Q, 표											
mpis.la	mpis.label == 132											
NO.	Time	Vlan Source	Destination	Protocol	Lenath Info							
	1 0.0.0000	3e:43:08:00:45:0	0 VcommsCo 87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP ISO Network Laver (unofficial?) Group, SSAP IBM Net Management Command							
	2 2.229052	3e:46:08:00:45:0	0 VcommsCo 87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xca Response							
	3 7.837599	3e:43:08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP HP Extended LLC Command							
	4 12.230180	3e:46:08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xce Response							
	5 17.737592	3e:43:08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP Remote Program Load Command							
	6 21.739701	3e:46:08:00:45:0	Ø VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xd2 Response							
	7 25.657623	Se:43:08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x36 Individual, SSAP NULL LSAP Command							
	8 29.259663	3e.46:08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xd6 Response							
	9 35.077480	3e:43 08:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x36 Individual, SSAP SNA Path Control Command							
	10 36.899616	3e:46:00:00:45:0	0 VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xda Response							
	11 15 010020	30.13.08.09.15.2	A VcommeCo 87+89+40		12A T N/DI-Q N/SI-Q+ DSAD Qx26 Todividual SSAD AMA Command							
> Ether > Inter > Gener > Multi 00   > PW Et Se > IEEE	<pre>&gt; Prame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) &gt; Ethernet II, Src: (5:co_40:3e:42) (50:87:84):4(3:e):4(3), Dist: (5:co_40:3e:42) (50:87:89:40:3e:42) &gt; Internet Protocol Version 4, Src: 172.16.0.14, Dit: 172.16.0.45 &gt; Generic Routing Encapsulation (0x8848 - unknown) &gt; WhilipProtocol Label Switching Header, Label: 152 or (5: 1, TTL: 254 0000 0000 0000 1000 0100</pre>											
> De	stination: VcommsC	o_87:89:40 (00:05:50:8)	7:89:40)									
> So	urce: 3e:43:08:00:	45:c0 (3e:43:08:00:45:0	:0)									
> Le	ngth: 68											
✓ Logic	al-Link Control											
> DS	AP: Unknown (0x35)											
> SS	AP: IBM Net Manage	ment (0xf4)										
> Co	ntrol field: I, N(	R)=0, N(S)=0 (0x0000)										
✓ Data	(60 bytes)											
Da	ta: 01593ea7640000	01e00000050201003064000	000100000000									
ſL	ength: 601											

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.

> Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)	its)									
Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42)										
Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45										
Generic Routing Encapsulation (0x8848 - unknown)										
✓ MultiProtocol Label Switching Header, Label: 132, Exp: 6, S: 1, 1	TTL: 254									
0000 0000 1000 0100 = MPLS Label: 132										
= MPLS Experimental Bi	its Expand Subtrees Shift+Right									
= MPLS Bottom Of Labe	L S Expand All Ctrl+Right									
1111 1110 = MPLS TTL: 254	Collance All Ctrlu Left									
✓ PW Ethernet Control Word	Conapse An Cur+Leit									
Sequence Number: 24064	Apply as Column									
IEEE 802.3 Ethernet										
> Destination: VcommsCo_87:89:40 (00:05:50:87:89:40)	Apply as Filter									
<pre>Source: 3e:43:08:00:45:c0 (3e:43:08:00:45:c0)</pre>	Prepare a Filter									
> Length: 68	Commention Filter									
Logical-Link Control	Conversation Filter									
> DSAP: Unknown (0x35)	Colorize with Filter									
> SSAP: IBM Net Management (0xf4)	Follow									
> Control field: I, N(R)=0, N(S)=0 (0x0000)										
✓ Data (60 bytes)	Сору									
Data: 01593ea764000001e0000005020100306400000100000000	Show Packet Bytes									
[Length: 60]	Evport Packet Bytes Ctrl+H									
	Wiki Protocol Page									
	Filter Field Reference									
	Protocol Preferences									
	Decode As									
	Decode Pain									
	Go to Linked Packet									
	Show Linked Packet in New Window									
1										

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.

🧲 Wireshark · Decode As					?	×
Field	Value	Туре	Default	Current		
MPLS protocol 🔹	132 ~	Integer, base 10	(none)	(none)		•
			C	(none) CESoPSN basic (no RTP) Ethernet PW (Cwrnet Pistic) Ethernet PW (with CW) Frame Relay DLCI PW Generic PW (with CW) HDLC PW with PPP payload (no CW) HDLC PW, FR port mode (no CW)		~
+ – Pa				OK Save Cancel	Help	

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.

<u>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</u>

🦲 🔳 🙍 💿	📙 🛅 🔀 ট	९ 🗢 🔿 🗟 🖗 👲	📃 📃 २, २, १								
mpls.label == 132											
No.	Time	Vlan Source	Destination	Protocol	Length Info						
1	0.000000	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet						
2	2.229652	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet						
3	7.837599	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet						
4	12.230180	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet						
5	17.737592	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet						
6	21.739701	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet						
7	25.657623	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet						
8	29.259663	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet						
9	35.077480	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet						
10	36.899616	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet						
11	15 010000	100 0 0 1	22/ 0 0 5	OSDE	124 Hello Dacket						
> Frame 1: 12	4 bytes on w	ire (992 bits), 124 by	tes captured (992 bits	)							
> Ethernet II	, Src: Cisco	_40:3e:43 (50:87:89:40	:3e:43), Dst: Cisco_40	:3e:42 (50:87:89:	40:3e:42)						
> Internet Pr	otocol Versi	on 4, Src: 172.16.0.14	, Dst: 172.16.0.45								
> Generic Rou	ting Encapsu	lation (0x8848 - unkno	wn)								
<ul> <li>MultiProtoc</li> </ul>	ol Label Swi	tching Header, Label:	132, Exp: 6, S: 1, TTL	: 254							
0000 000	0 0000 1000 (	0100 =	MPLS Label: 132								
		110 =	MPLS Experimental Bits	: 6							
		=	MPLS Bottom Of Label St	tack: 1							
		1111 1110 =	MPLS TTL: 254								
Ethernet II	, Src: Cisco	_40:3e:43 (50:87:89:40	:3e:43), Dst: IPv4mcas	t_05 (01:00:5e:00	:00:05)						
Internet Pr	otocol Versi	on 4, Src: 100.0.0.1,	Dst: 224.0.0.5								
<ul> <li>Open Shorte</li> </ul>	st Path Firs	t									
> OSPF Hea	der										
> OSPF Hel	lo Packet										

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.

File	Edit View Go Capture	Analyze Statistics Telepho	ony Wireless Tools He	lp						
	🔳 🖉 💽 📙 🗟 🗙 🖸 🗌	९ 🗢 🗢 🕾 🕢 📃	📃 Ə. Ə. Ə. 🎹							
	npls.label == 232									
No.	Time Vla	an Source	Destination	Protocol	Length Info					
	1 0.000000	3e:46:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xae Command					
	2 2.346992	3e:43:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x70 Command					
	3 4.603176	3e:46:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xae Response					
	4 6.981213	3e:43:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x70 Response					
	5 9.373389	3e:46:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb0 Command					
	6 11.330387	3e:43:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x72 Command					
	7 13.715773	3e:46:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb0 Response					
	8 16.102792	3e:43:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x72 Response					
	9 18.185963	3e:46:08:00:45:c0	Remotek_87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3e Group, SSAP 0xb2 Command					
	10 20.554788	3e:43:08:00:45:c0	Remotek 87:89:40	LLC	116 I, N(R)=0, N(S)=0; DSAP 0x3c Group, SSAP 0x74 Command					
	11 23 051203	30.16.08.00.15.00	Demotek 27.20.10		116 T M/D)-A M/S)-A. DSAD Av3e Group SSAD Avb2 Personne					
~ ~ ~ ~	Frame 1: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) Ethernet II, Src: Cisco_40:3e:46 (50:87:89:40:3e:46), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42) Internet Protocol Version 4, Src: 172.16.0.45, Dst: 172.16.0.14 Generic Routing Encapsulation (0x8848 - unknown) (MultiProtocol Leal Switching Header Label: 202 - unit Contact 1, TTL: 254									
	0000 0000 1110 1000									
			Bottom Of Label Stac	k: 1						
		1111 1110 = MPLS	TTI : 254	-						
$\sim$	PW Ethernet Control Word									
	Sequence Number: 24064									
$\sim$	IFFE 802.3 Ethernet									
	> Destination: Remotek 87	7:89:40 (00:0a:50:87:89:	40)							
	> Source: 3e:46:08:00:45:	:c0 (3e:46:08:00:45:c0)	/							
	> Length: 60	(								
$\sim$	Logical-Link Control									
	> DSAP: Unknown (0x3f)									
	> SSAP: Unknown (Øxae)									
	> Control field: I. N(R)=	=0. N(S)=0 (0x0000)								
$\sim$	Data (52 bytes)	-, -, - , - , - , - , - , - , - , - , -								
	Data: 0158d0efc8000002e	000000a0205f2080000000	00000000							
	[Length: 52]									

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.

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help				
		0	010	🗙 🖻	۹ 🗢 🖻	2 👔	& ☴   ☴	⊕, ⊖, €	Q. 🎹					
mpls.label == 232														
No.	~	т	ïme	Vl	an Source	2	D	estination			Protocol		Length	Info
		10	.0000	900	200.	0.0.2	2	24.0.0.1	0		EIGRP		116	Hello
		22	.3469	92	200.	0.0.1	2	24.0.0.1	0		EIGRP		116	Hello
		34	.6031	176	200.	0.0.2	2	24.0.0.1	0		EIGRP		116	Hello
		46	.9812	213	200.	0.0.1	2	24.0.0.1	0		EIGRP		116	Hello
		59	.3733	389	200.	0.0.2	2	24.0.0.1	0		EIGRP		116	Hello
		61	1,330	9387	200.	0.0.1	2	24.0.0.1	0		EIGRP		116	Hello
		71	3.715	5773	200.	0.0.2	2	24.0.0.1	0		EIGRP		116	Hello
		81	6.102	2792	200.	0.0.1	2	24.0.0.1	0		EIGRP		116	Hello
		91	8.185	5963	200.	0.0.2	2	24.0.0.1	0		EIGRP		116	Hello
		10 2	0.554	1788	200.	0.0.1	2	24.0.0.1	0		EIGRP		116	Hello
		11.2	3 051	203	200	202	2	<u>04 0 0 1</u> 0	a		FTGDD		116	Hello
>	Frame 1	: 116	byte	s on wir	e (928 bi	ts), 110	5 bytes capt	ured (92	28 bits)	)				
>	Etherne	t II,	Snc:	Cisco_4	0:3e:46 (	50:87:89	9:40:3e:46),	Dst: Ci	lsco_40:	:3e:42	(50:87	:89:40:3e	e:42)	
>	Interne	t Prot	tocol	Version	4, Src:	172.16.0	0.45, Dst: 1	72.16.0.	14					
>	Generic	Routi	ing E	ncapsula	tion (0x8	848 - ur	1known)							
~	MultiPr	otocol	l Lab	el Switc	hing Head	er, Labe	el: 232, Exp	: 6, S:	1, TTL:	: 254				
	0000	0000	0000	1110 10	00		= MPLS Lab	el: 232						
			• • • •		110		= MPLS Exp	erimenta	l Bits:	: 6				
			• • • •		1 .		= MPLS Bot	tom Of L	abel St	tack: 1	L			
					1	111 1110	) = MPLS TTL	: 254						
>	Etherne	t II,	Src:	Cisco_4	0:3e:46 (	50:87:89	9:40:3e:46),	Dst: IP	v4mcast	t_0a (0	01:00:50	e:00:00:0	)a)	
>	Interne	t Prot	tocol	Version	4, Src:	200.0.0.	.2, Dst: 224	.0.0.10						
>	Cisco E	IGRP												

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-noheader.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.