# Wiresharkを使用したOTVソリューションのトラ ブルシューティング

# 内容

概要
前提条件
要件
使用するコンポーネント
問題の説明
OTVパケット形式
トポロジ
パケット キャプチャ
解決方法
Vlan 100のパケットのデコード
Vlan 200のパケットのデコード
Editcapを使用したOTVヘッダーの削除
WindowsプラットフォームでEditcapを実行
Mac OSプラットフォームでのEditcapの実行
結論

# 概要

このドキュメントでは、Cisco OTVソリューションのトラブルシューティングにおける、既知の フリーウェアパケットキャプチャおよび分析ツールであるWiresharkの使用について説明します。

# 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- NexusシリーズスイッチのOverlay Transport Virtualization(OTV)
- マルチプロトコルラベルスイッチング(MPLS)レイヤ2仮想プライベートネットワーク(VPN)の 基礎
- Wiresharkは、無料でオープンソースのパケットアナライザ(<u>https://www.wireshark.org</u>)

## 使用するコンポーネント

このドキュメントの情報は、Nexus 7000 シリーズ スイッチ プラットフォームに基づいています 。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

# 問題の説明

VPN環境でネットワークの問題をトラブルシューティングする際には、カプセル化されたパケットのキャプチャと分析を行う技術の1つが必要です。ただし、Cisco OTVネットワーク環境では、 このアプローチには特定の課題があります。Wiresharkなどの一般的に使用されるパケット分析ツ ール、a無料およびオープンソースパケットアナライザ OTVカプセル化トラフィックの内容が正 しく解釈されない可能性があります。したがって、通常、データ分析を正常に実行するには、カ プセル化されたデータをOTVパケットから抽出するなどの手間のかかる回避策が必要です。

### OTVパケット形式

OTVカプセル化は、パケットの全体的なMTUサイズを42バイト増やします。これは、元のレイヤ 2フレームからCRCフィールドと802.1Qフィールドを削除し、OTV Shim(VLANおよびオーバー レイID情報も含む)と外部IPヘッダーを追加するOTVエッジデバイスの動作の結果です。



MPLS L2VPNソリューションでは、アンダーレイネットワーク内のデバイスに、MPLSパケット ペイロードを正しくデコードするための十分な情報がありません。MPLSコアネットワークでの パケット転送はラベルに基づいて行われるため、アンダーレイネットワークでのMPLSパケット の内容を詳細に分析する必要はありません。

ただし、OTVパケットのデータ分析がトラブルシューティングやモニタリングの目的で必要な場合は、これは課題となります。

Wiresharkなどのパケット分析ツールは、通常のMPLSパケット解析ルールを適用して、MPLSへ ッダーに続くパケットデータのデコードを試みます。ただし、通常はMPLS L2VPNヘッドエンド ルータとテールエンドルータの間で実行されるコントロールワードネゴシエーションの結果に関 する情報がない場合があるため、パケット分析ツールはデフォルトの解析動作に戻り、MPLSへ ッダーに続くパケットデータに適用されます。

注: Any Transport Over MPLS(ATOM)などのMPLS L2VPNソリューションでは、疑似配線 エンドポイントが制御語パラメータの使用をネゴシエートします。制御語は、MPLSラベル スタックと疑似配線パケットのレイヤ2ペイロードの間にあるオプションの4バイトフィー ルドです。コントロールワードは、汎用およびレイヤ2ペイロード固有の情報を伝送します 。Cビットが1に設定されている場合、アドバタイジングプロバイダーエッジ(PE)は、シグ ナリングされる疑似回線のすべての疑似回線パケットにコントロールワードが存在すること を想定します。Cビットが0に設定されている場合、コントロールワードは存在しません。

その結果、デフォルトのWireshark解析動作ではOTVパケットの内容が正しく解釈されない可能性 があるため、OTVネットワークのトラブルシューティングプロセスがより複雑になります。

### トポロジ

次に、単純なOTVネットワークのネットワークダイアグラムを示します。Vlan 100とVlan 200の ルータは、2つのデータセンター(DataCenter1とDataCenter2)間にそれぞれOSPFとEIGRPの 隣接関係を確立します。DataCenter Interconnect(DCI)は、N7kスイッチ間にOTVトンネルを使用 して実装されます。図では、AED1とAED2として示されています。



注:Cisco OTVソリューションでは、Authoritative Edge Device(AED)の役割の概念を使用し ます。この役割は、特定のサイトでOTVトラフィックをカプセル化およびカプセル化解除す るネットワークデバイスに割り当てられます。

トンネリングソリューションでよく見られる課題は、特定の種類のオーバーレイパケット (IGP、FHRPなど)がアンダーレイネットワークの特定のポイントに到達するかどうかを確認す ることです。例として、OSPFとEIGRPのオーバーレイトラフィックを使用します。

#### パケット キャプチャ

ネットワークでパケットキャプチャを実行するには、複数の方法があります。1つのオプションは、Cisco CatalystおよびCisco Nexusスイッチングプラットフォームで使用可能なCisco Switched Port Analyzer(SPAN)機能を使用することです。

トラブルシューティングプロセスの一部として、複数のポイントでパケットキャプチャを実行す る必要がある場合があります。アンダーレイネットワークのOTV Joinインターフェイスおよびイ ンターフェイスは、SPANパケットキャプチャポイントとして使用できます。

# 解決方法

Wiresharkのデフォルト解析エンジンは、OTVカプセル化オーバーレイパケットの最初の数バイト を、Pseudowire Emulation Edge-to-Edge(PWE3)コントロールワードの一部として誤って解釈す る可能性があります。

**注**:MPLS擬似回線エミュレーションエッジツーエッジ(PWE3)コントロールワードは、このドキュメントの残りの部分で*はコントロールワード*と呼ばれています。

Wiresharkパケット分析ツールがOTVカプセル化パケットの内容を正しく解釈するには、パケット デコードプロセスを手動で調整する必要があります。

注:OTVヘッダーで使用されるMPLSラベルは、オーバーレイVLAN番号+32と同じです。

#### Vlan 100のパケットのデコード

デコードプロセスの最初のステップとして、OTV拡張VLAN 100の内容を伝送するOTVカプセル 化パケットのみを表示します。使用されるフィルタは、VLAN 100を表すmpls.label == 132です。

**注**:OTV経由で拡張された特定のVLANのOTVカプセル化パケットを表示するには、 Wiresharkの表示フィルタmpls.label == <<vlan number extended over OTV> + 32>を使用し ます

<u>F</u> ile <u>E</u> dit	: <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	nalyze <u>S</u> tatistics Telephon	<u>wireless</u> <u>T</u> ools <u>H</u> elp						
	( 🔲 🖉 💿 📙 🛅 🗙 🖾 🔍 👄 🗠 🔄 📜 🔍 Q. Q. A. A.								
mpls.label == 132									
vo.	Time Vlan	Source	Destination	Protocol	Length Info				
	1 0.00000	3e:43:08:00:45:c0	VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP ISO Network Layer (unofficial?) Group, SSAP IBM Net Management Command				
	2 2.229052	3e:46:08:00:45:c0	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:c0	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:c0	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:c0	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:c0	VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xd2 Response				
	7 25.657623	3e:43:08:00:45:c0	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:c0	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:c0	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:c0	VcommsCo_87:89:40	LLC	124 I, N(R)=0, N(S)=0; DSAP 0x4c Individual, SSAP 0xda Response				
	11 15 010000	30-13-02-02-15-00	VcommeCo 87.89.40	110	124 T N/D)-Q N/S)-Q+ DSAD Qx36 Todividual SSAD SNA Command				
> Frame	1: 124 bytes on wire (	(992 bits), 124 bytes c	aptured (992 bits)						
> Ether	net II, Src: Cisco_40:3	3e:43 (50:87:89:40:3e:4	3), Dst: Cisco_40:3e:4	2 (50:87:89:4	40:3e:42)				
> Inter	net Protocol Version 4,	Src: 172.16.0.14, 0 t	: 172.16.0.45						
> Gener	ic Routing Encapsulatio	on (0x8848 - unknown)							
✓ Multi	Protocol Label Switchir	ng Header, Label: 132,	LAP. 0, 5: 1, TTL: 254	•					
000	0000 0000 1000 1000 MPLS Label: 132								
	110								
		1 = MPLS	Bottom Of Label Stack:	1					
		1111 1110 = MPLS	TTL: 254						
· PW Et	nernet Control Word								
Sec.	quence Number: 24064								
* 1000 G	obz.5 ctnernet	80.40 (00.05.50.87.80.	40)						
> De:	scindcion: vcommsco_o/:	(20.42.02.00.45.00)	40)						
> 10	arte: 52145100100145100	(32:43:08:00:43:00)							
Y Logic	al-Link Control								
	AP: Unknown (0x35)								
> 55	AP: TRM Net Management	(9xf4)							
> Cor	ntrol field: I, N(R)=0.	N(S)=0 (0x0000)							

/ Data (60 bytes)
Data: 01593ea764000001e0000005020100306400000100000000...
[Length: 60]

OTV経由で拡張されたVlan 100のOTVカプセル化パケットを表示する

デフォルトでは、WiresharkはMPLS L2VPNパケットのコンテンツの最初の4バイトをコントロー ルワードとして解釈します。これは、OTVカプセル化パケットに対して修正する必要があります 。これを行うには、任意のパケットのMPLSラベルフィールドを右クリックし、[*Decode As...]を 選択します。*オプション.

> Frame 1: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)									
<pre>&gt; Ethernet II, Src: Cisco_40:3e:43 (50:87:89:40:3e:43), Dst: Cisco_40:3e:42 (50:87:89:40:3e:42) &gt; Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45</pre>									
<pre>&gt; Internet Protocol Version 4, Src: 172.16.0.14, Dst: 172.16.0.45 &gt; Generic Routing Encapsulation (0x8848 - unknown)</pre>									
> Generic Routing Encapsulation (0x8848 - unknown)									
MultiProtocol Label Switching Header, Label: 132, Exp: 6, S: 1, TTL:	254								
0000 0000 0000 1000 0100 = MPLS Label: 132									
110 = MPLS Experimental Bits	Expand Subtrees	Shift+Right							
= MPLS Bottom Of Label S	Expand All	Ctrl+Right							
1111 1110 = MPLS TTL: 254	Collance All	Ctrivia							
✓ PW Ethernet Control Word	Collapse All	Cui+Leit							
Sequence Number: 24064	Apply as Column								
✓ IEEE 802.3 Ethernet									
<pre>&gt; Destination: VcommsCo_87:89:40 (00:05:50:87:89:40)</pre>	Apply as Filter	+							
> Source: 3e:43:08:00:45:c0 (3e:43:08:00:45:c0)	Prepare a Filter	•							
> Length: 68									
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]	Evenent Dacket Puter	Chello LL							
	Export Packet Bytes	Cui+n							
	Wiki Protocol Page								
	Filter Field Peterence								
	Protocol Preferences	•							
	Decode As								
	Decode As								
	Go to Linked Packet								
	Show Linked Packet in New Win	ndow							

[MPLS label]フィールドを右クリックし、[Decode As...]オプションを選択します

次のステップは、カプセル化されたコンテンツにコントロールワードがないことをWiresharkに 通知することです。

Wireshark · Decode As						?	×
Field		Value	Туре	Default	Current		
MPLS protocol	•	132 ~	Integer, base 10	(none)	(none)		•
				<	(none) CESOPSN basic (no RTP) Ethernet PW (cw new istic) 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)		
+ - Pb					OK Save Cancel	He	elp

#### [no CW]オプションを選択します

[OK]ボタンをクリックしてこの変更を送信すると、Wireshark分析ツールはOTVカプセル化パケットの内容を正しく表示します。

<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> na	alyze <u>S</u> tatistics	Telephony <u>W</u> ireless <u>T</u> ools <u>H</u>	<u>H</u> elp					
	a 🔳 🖉 🐵 📙 🛅 🗙 🖆 I 🍳 🗢 🗢 🗟 🗿 🕹 🧮 🗮 🔍 Q. Q. X. X									
m	mpls.label == 132									
No.	Time	Vlan	Source	Destination	Protocol	Length Info				
	1 0.00000	90	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet				
	2 2.22965	52	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet				
	3 7.83759	99	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet				
	4 12.2301	180	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet				
	5 17.7375	592	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet				
	6 21.7397	701	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet				
	7 25.6576	523	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet				
	8 29.2596	563	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet				
	9 35.0774	180	100.0.0.1	224.0.0.5	OSPF	124 Hello Packet				
	10 36.8996	516	100.0.0.2	224.0.0.5	OSPF	124 Hello Packet				
	11 15 0100	120	100 0 0 1	224 0 0 5	OSDE	124 Hallo Dacket				
> Fi	rame 1: 124 bytes	on wire (9	92 bits), 124	bytes captured (992 bits)						
> E1	thernet II, Src: (	Cisco_40:3e	:43 (50:87:89	:40:3e:43), Dst: Cisco_40:3	e:42 (50:87:89:	40:3e:42)				
> II	nternet Protocol	Version 4,	Src: 172.16.0	.14, Dst: 172.16.0.45						
> Ge	eneric Routing En	capsulation	(0x8848 - un	known)						
~ <u>M</u> i	ultiProtocol Labe	l Switching	; Header, Labe	1: 132, Exp: 6, S: 1, TTL:	254					
	0000 0000 1000 1000 = MPLS Label: 132									
	110 = MPLS Experimental Bits: 6									
	•••••		1	= MPLS Bottom Of Label Sta	ck: 1					
	1111 1110 = MPIS TTI: 254									
P Et	thernet II, Src: (	Cisco_40:3e	:43 (50:87:89	:40:3e:43), Dst: IPv4mcast_	05 (01:00:5e:00	:00:05)				
≥ Ir	nternet Protocol	Version 4,	Src: 100.0.0.	1, Dst: 224.0.0.5						
Y OF	en Shortest Path	First								
>	OSPF Header									
>	OSPF Hello Packe	et								

Wiresharkは、OTVカプセル化パケットの内容を正しく表示します

# Vlan 200のパケットのデコード

上記の手順は、OTVを介して拡張されたVLANに適用できます。たとえば、Wiresharkフィルタを 使用してVLAN 200のパケットのみを表示すると、分析ツールに次の出力が表示されます。

File	Edit View Go Capture An	alyze Statistics Telepho	ny Wireless Tools Help	þ					
	🕻 💻 🖉 📵 📙 🛅 🗙 🖻 🔍 👄 🕸 🗑 👲 🚍 🔳 🍳 Q. Q. 🎚								
	mpls.label == 232								
No.	Time Vlan	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 87.89.10		116 T N/D)-Q N/S)-Q. DSAD Quize Group SSAD Qub? Desponse				
<pre>&gt; Enternet 11, Stct Cisto_40:3e:40 (S0:07:05:40:3e:40), Ustc Cisto_40:3e:42 (S0:07:09:40:3e:42) &gt; Internet Protocol Version 4, Src: 172.16.0.45, Dst: 172.16.0.14 &gt; Generic Routing Encapsulation (0x8848 - unknown) &gt; MultiProtocol Label Switching Header, Label: 210, Exp. 0, C+1, TTL: 254</pre>									
	<pre>&gt; Destination: Remotek_87:89:40 (00:0a:50:87:89:40) &gt; Source: 3e:46:08:00:45:c0 (3e:46:08:00:45:c0) &gt; Length: 60</pre>								
¥ I	Ogical-Link Control								
	> Down: Unknown (0xae) > Control field: J, N(R)=0, N(S)=0 (0x0000)								
× [	Data (52 bytes)								
	Data: 0158d0efc8000002e000000a0205f208000000000000000 [Length: 52]								

### OTVで拡張されたVLAN 200のパケットを表示する

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

WiresharkがMPLSパケットの最初の数バイトをPW Control Wordとして解釈しないように指示されると、デコードプロセスは正常に完了します。

🛋 🔳 🖉 🐵 📙 🔚 🕱 🖆 🔍 🗢 🗢 ≊ 🗿 🦺 📃 📃 🍳 Q, Q, II										
mpis.label == 232										
No.	Time	Vlan Source	Destination	Protocol	Length	Info				
	1 0.000000	200.0.0.2	224.0.0.10	EIGRP	116	Hello				
	2 2.346992	200.0.0.1	224.0.0.10	EIGRP	116	Hello				
	3 4.603176	200.0.0.2	224.0.0.10	EIGRP	116	Hello				
	4 6.981213	200.0.0.1	224.0.0.10	EIGRP	116	Hello				
	5 9.373389	200.0.0.2	224.0.0.10	EIGRP	116	Hello				
	6 11.330387	200.0.0.1	224.0.0.10	EIGRP	116	Hello				
	7 13.715773	200.0.0.2	224.0.0.10	EIGRP	116	Hello				
	8 16.102792	200.0.0.1	224.0.0.10	EIGRP	116	Hello				
	9 18.185963	200.0.0.2	224.0.0.10	EIGRP	116	Hello				
	10 20.554788	200.0.0.1	224.0.0.10	EIGRP	116	Hello				
	11 23 051203	<u> 200 0 0 2</u>	224 0 0 10	FTGDD	116	Hello				
> Fra	me 1: 116 bytes on w	/ire (928 bits), 116	bytes captured (928 bits	;)						
> Eth	ernet II, Src: Cisco	_40:3e:46 (50:87:89	:40:3e:46), Dst: Cisco_40	:3e:42 (50:87:89:4	40:3e:42)					
> Int	ernet Protocol Versi	on 4, Src: 172.16.0	.45, Dst: 172.16.0.14							
> Gen	eric Routing Encapsu	lation (0x8848 - un	known)							
Y Mul	tiProtocol Label Swi	tching Header, Labe	1: 232, Exp: 6, S: 1, TTL	: 254						
	0000 0000 0000 1110 1000 = MPLS Label: 232									
	110 = MPLS Experimental Bits: 6									
		1111 1110	= MPLS TTL: 254							
> Eth	ernet II, Src: Cisco	40:3e:46 (50:87:89	:40:3e:46), Dst: IPv4mcas	t 0a (01:00:5e:00	:00:0a)					
> Int	ernet Protocol Versi	on 4, Src: 200.0.0.	2, Dst: 224.0.0.10		,					
> Cis	co EIGRP									

Wiresharkは、Vian 200トラフィックをEIGRPパケットとして正しく表示します

### Editcapを使用したOTVヘッダーの削除

通常、Wiresharkのインストールには、Editcapというコマンドラインパケット編集ツールが付属 します。このツールは、キャプチャされたパケットからOTVオーバーヘッドを永久に削除できま す。これにより、Wiresharkの解析動作を手動で調整しなくても、Wiresharkグラフィカルユーザ インターフェイス(GUI)でキャプチャされたパケットを簡単に表示および分析できます。

#### WindowsプラットフォームでEditcapを実行

Windowsオペレーティングシステムでは、*editcap.exe*はデフォルトでc:\Program Files\Wireshark>ディレクトリにインストールされます。

このツールを – Cフラグを*付けて実行*し、OTVオーバーヘッドを削除し、結果を.pcapファイルに *保存*します。

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>

c:\Users\cisco\Desktop>

#### Mac OSプラットフォームでのEditcapの実行

Mac OSオペレーティングシステムでは、 editcapは/usr/local/binフォルダにあります。

CISCO:cisco\$ /usr/local/bin/editcap -C 42 otv-underlay-capture.pcap otv-underlay-capture-noheader.pcap

CISCO:cisco\$

キャプチャされたパケットからOTVヘッダーを削除し、EditcapツールMPLSヘッダーの一部とし てエンコードされたVlan情報が失われ、OTV shimの一部になります。特定のVLANのトラフィッ クのみを分析する必要がある場合、Editcapツールを使用してOTVヘッダーを削除する前に、「 mpls.label == <<vlan number extended over OTV> + 32>' Wireshark GUIフィルタを使用してくだ さい。

# 結論

Cisco OTVソリューションのトラブルシューティングには、コントロールプレーンの動作とデー タプレーンのカプセル化の両方の観点から、テクノロジーを十分に理解する必要があります。知 識を効果的に活用することで、Wiresharkなどのフリーウェアパケット分析ツールは、OTVパケッ ト分析において非常に強力であることを証明できます。さまざまなパケット表示オプションに加 えて、一般的なWiresharkのインストールでは、パケット分析を簡素化できるパケット編集ツール が提供されます。これにより、特定のトラブルシューティングセッションに最も関連するパケッ トコンテンツの部分にトラブルシューティングを集中させることができます。