# WildPackets OmniPeek および EtherPeek 3.0 ソ フトウェアでの LWAPP デコードの有効化

### 内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>表記法</u> <u>LWAPP デコード ファイルの変更</u> <u>TCP\_UDP\_Ports.dcd の変更</u> <u>Pspecs.xml ファイルの変更</u> <u>OmniPeek 5.0 の LWAPP のデコード</u> <u>確認</u> 関連情報

### 概要

WildPackets OmniPeek(および EtherPeek)では、Lightweight Access Point Protocol(LWAPP)デコードを利用できますが、接続されていません。このドキュメントでは、 LWAPP デコードをイネーブルにし、ソフトウェアを使用して LWAPP を調べる方法を説明しま す。このドキュメントでは、EtherPeek 3.0 および OmniPeek 5.0 の手順を使用します。

- 注: OmniPeek 3.0の手順は、EtherPeek 3.0の手順と同じです。
- 注:OmniPeekソフトウェアとEtherPeekソフトウェアの唯一の違いは、ファイルの場所です。
  - OmniPeekのパスはC:/Program Files/WildPackets/OmniPeekです。
  - EtherPeekのパスは、C:/Program Files/WildPackets/EtherPeekです。

# <u>前提条件</u>

### <u>要件</u>

シスコでは、EtherPeek ソフトウェアおよび OmniPeek 3.0 と 5.0 の各ソフトウェアの知識があ ることを推奨します。EtherPeekの詳細は、『EtherPeek FAQ』を参<u>照してください</u>。 OmniPeekの詳細については、『Omniについて』を参<u>照してください</u>。

### <u>使用するコンポーネント</u>

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

#### <u>表記法</u>

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# <u>LWAPP デコード ファイルの変更</u>

LWAPPデコードファイルを変更するには、LWAPP機能に「ETHR 0 0 90 c2 AP Identity:;」を追 加します。これは、LWAPP-light\_weight\_の「LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:」行のすぐ下にあります。protocol.dcdファイル(C:\Program Files\WildPackets\EtherPeek\Decodes)。

# <u>TCP\_UDP\_Ports.dcd の変更</u>

ファイル TCP\_UDP\_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes)で、次の 2 行を追加します。

0x2fbe | LWAPP;

0x2fbf | LWAPP;

**注:このプ**ロセスの結果、ホストコンピュータ上でポートが開かれることはありません。したがって、この手順はホスト コンピュータをセキュリティ リスクさらしません。

この方法で、12222 および 12223 の 2 のポート を追加します。

# Pspecs.xml ファイルの変更

次のステップを実行します。

1. ファイル pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033)の User Datagram Protocol (UDP、ユーザ データグラム プロトコル)のセクションで、次の行を追加します。注:最初に元のファイルをバックアップしてください。

```
<PSpec Name="LWAPP">

<PSpecID>6677</PSpecID>

<LName>LWAPP</LName>

<SName>LWAPP</SName>

<Desc>LWAPP</Desc>

<Color>color_1</Color>

<CondSwitch>12222</CondSwitch>

<CondSwitch>12223</CondSwitch>

<PSpec Name="LWAPP Data">

<PSpecID>6688</PSpecID>

<LName>LWAPP Data</LName>

<SName>LWAPP-D</SName>

<DescID>6677</DescID>

<CondExp><![CDATA[(SrcPort == 12222) || (DestPort == 12222)]]></CondExp>

</PSpec>
```

```
<PSpecID>6699</PSpecID>
<LName>LWAPP Control</LName>
<SName>LWAPP-C</SName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
</PSpec>
</PSpec>
```

2. 変更を有効にするために OmniPeek や EtherPeek を再起動します。

# <u>OmniPeek 5.0 の LWAPP のデコード</u>

OmniPeekバージョン5.0は、OmniPeekバージョン3.0の次世代キャプチャツールです。5.0バージョンでは、LWAPPデコードはデフォルトで組み込まれています。したがって、ファイルの変更の 必要はありません。ただし、IP アドレスとポート番号を使用して 5.0 バージョンでプロトコル フィルタを定義する方法を示す例を次に示します。

- 1. OmniPeek 5.0 アプリケーションを開きます。
- 2. [New Packet Capture] ウィンドウを開くために、[Start] ページで、[File] > [New] の順にクリ ックします。[Capture Options] という名前の小さいウィンドウが表示されます。このウィン ドウには、パケット キャプチャのオプションのリストが含まれています。
- [Adapter] オプションから、そのアダプタを使用してパケットをキャプチャするアダプタを 選択します。アダプタに関する説明は、アダプタを強調表示するとその下に表示されます。 ローカルのイーサネット アダプタを使用してパケットをキャプチャするには、[Local Area Connection] を選択します。
- 4. [OK] をクリックします。[New Capture] ウィンドウが表示されます。
- 5. [Start Capture] **ボタンをクリックします。**ツールはソフトウェアで定義されたプロトコルの パケットのキャプチャを開始します。キャプチャしたパケットを表示するには、左側の [Capture] **メニューで [Packets] オプションをクリックします。**
- 6. 新しいプロトコルを定義するには、キャプチャしたパケットを右クリックし [Make Filter] を クリックします。[Insert Filter] ウィンドウが表示されます。
- [Filter] ボックス内に名前を入力して、プロトコルを識別します。[Address] フィルタを有効 にします。特定の IP アドレスから送受信されるパケットをキャプチャする [IP] のタイプを 選択します。[Address1] に送信元の IP アドレスを入力します。宛先がスタティック IP の場 合は [Address 2] に IP アドレスを入力します。宛先が DHCP 経由で IP アドレスを受け取る 場合、[Any Address] のオプションを選択します。パケット フローの方向を指定するには、 [Both directions] ボタンをクリックし次に 3 種類のオプションのいずれかをクリックします 。ボタンの矢印は選択された方向を表します。[Port] フィルタを有効にします。プロトコル (たとえば TCP)によって使用されるポートのタイプを選択します。[Port 1] に送信元で使 用するポートを入力します。宛先が標準の適切に定義されたポートを使用する場合、[Port 2] にポート番号を入力します。それ以外の場合で、宛先が任意にポートを使用する場合、[Any port] オプションを選択します。要件に基づいて方向を [Both Directions] ボタンから選択しま す。
- 8. 新しいカスタム プロトコルを定義するには、この手順を繰り返してください。

### 確認

OmniPeek 5.0 では、LWAPP のイベントがトリガーされるとデフォルトでツールでキャプチャされる LWAPP プロトコルをが [Capture] 画面から確認できます。図1は、ディスカバリ要求が

LAP のよって作成される間にキャプチャされた LWAPP プロトコルを示します。

File Edit View	Capture Send Monitor Tool	s Window Help		1		1.	1		
A		9 Y 9 3 11 10 1	10	0 0	3 Day New				
Packets received	707 Buffer um 707 Filter st	aget 19% Accept al packets			and the second second		n ar an an an an the shirt of the shirt	- 54	Caphara
¥-								C. C	
Capture	de mit 100 52 62 153		(a) (d)	100					1.1
Deshboard					and the second		and a second		
Packets	Source	Destnation	Flags	524	Relative Tane	Protocol	Summary		
Log	3 10.77.244.209	IP Buoadcast		96	0:01:10.277675	DW3	C OVERY NAME-CISC	O-LWAPP-	CONTROL
Filters	#900:1A:A1:54:30:AB	BROAFT 802.14 BE	•	64	0:01:11.067006	002.1			
Expert	2 10.77.244.209	👷 IP Broadcast		168	0:01:11.276397	syslog	SEC-60909,D#t= 5	14 ,1-	122
Herarchy	10.77.244.209	IP Broadcast		141	0:01:11.276981	sAsjod	Szc=60909,Dst= 5	14,1-	95
Flat	3 10.77.244.209	🔮 IP Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t= 5	14 , Le -	91
Application	00:1A:A1:54:30:AB	. BBRcast 802.1d Br	•	64	0:01:13.072054	002.1			
Web	10.77.244.209	IF Excadeast		96	0:01:13.277035	083	C QUERT NAME+CISC	0-14827-	CONTROL
Servers	#900:1A:A1:54:30:AB	BCast 802.14 BE	•	64	0:01:15.077120	602.1			
Clerks.	3 10.77.244.209	🔮 IF Stoadcast		96	0:01:16.275883	08/5	C QUERT NAME-CISC	0-14427-	-CONTROL
Pages	#900:1A:A1:54:30:AB	MyRcast 002.14 St		64	0:01:17.081615	002.1			
Requests	B00:1A:A1:54:30:AB	Mass 002.1d Sr		64	0:01:19.088698	802.1			
Voice & Video	B00:18:D4:E3:A6:18	BEthemet Scondcast		64	0:01:19.275905	ARP Request	10.77.244.204 + 7		
Calls	2900:1A:A1:54:30:AB	200:1A:AI:54:30:AB		64	0:01:20.042094	Loopback			
Media	10.77.244.209	IP Broadcast		151	0:01:20.274075	syslog	SEC+60909,Det+ 5	14 .14	105
Visuals	10.77.244.209	IP Broadcast		156	0:01:20.275459	syslog	Scc+60909,Det+ 5	14 .14	110
Apdex	10.77.244.209	🚽 IF Szosdcast		1.46	0:01:20.276394	14472	Scc-14977,Dat+123	23.,14	100
Peer Map	200:1A:A1:54:30:AB	BCASE 002.10 St		64	0:01:21.090924	802.1			
Graphs	#00:1A:A1:54:30:AB	Boast 602.1d Bg		64	0:01:23.095938	002.1			
Statistics	200:1A:A1:54:30:AB	01:00:0C:CC:CC:CC		64	0:01:23.481099	00-00-00-20-04			
Nodes	#900:1A:A1:54:30:AB	B01:00:0C:00:00:00		-94	0:01:23.481160	00-00-00-00-03			
Protocols	#900:1A:A1:54:30:A5	BROAST 002.14 BE		64	0:01:25.102850	602.1			
Summery	#900:1A:A1:54:30:AB	BRCAST 802.1d BE		64	0:01:27.107696	802.1			
	#900:1A:A1:54:30:A8	BReast 802.1d Sc		64	0:01:29.112083	802.1			
	200:1A:A1:54:30:AB	#900:1A:A1:54:30:A8		64	0:01:30.051235	Loopback			
	#900:18:D4:E3:A8:18	Ethernet Broadcast		64	0:01:30.292150	APP Request	10.77.244.203 - 7		
	#900:1A:A1:54:30:AB	BRCAST. 002.1d BE		64	0:01:31.116975	802.1			
	8900:18:D4:E3:A8:18	BEthemet Broadcast		64	0:01:31.291080	ARP Request	10.77.244.203 - 7		
	200:1A:A1:54:30:A8	BReast 802.14 St		64	0:01:33,122176	602.1			
	10.77.244.209	IF Broadcast		132	0:01:34.336071	syslog	frc-60909.Det= 5	14 .1-	64
	10.77.244.209	TP Broadcast		132	0:01:34,336407	syslog	Szc+60909_Dyt= 5	14 .1-	64
	8900:1A:A1:54:30:A8	BO Mcast 002.14 Br		64	0:01:35.126796	802.1			
	10.77.244.209	IP Spoadcast		132	0:01:35.348150	syslog	Src-60909,Dat- 5	14 .1-	66
	#9-00:1A:A1:54:30:A5	BEAST 002.1d Br		64	0:01:37.135293	802.1			
	BRAN, 13.33.48.00.00.00	BRAT				And an a second second			

パケットに関する詳細情報を表示するにはパケットをダブルクリックします。

# <u>関連情報</u>

- ・<u>EtherPeek に関する FAQ</u>
- <u>Omni について</u>
- <u>OmniPeek 5.0 のダウンロード</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>