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

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。

前提条件

要件

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』を参照してください 。OmniPeekの詳細については、『Omniについて』を参照してください 。

使用するコンポーネント

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

表記法

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。

LWAPP デコード ファイルの変更

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)。

TCP_UDP_Ports.dcd の変更

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>

     <PSpec Name="LWAPP Control">
```

```
 <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。

OmniPeek 5.0 の LWAPP のデコード

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。

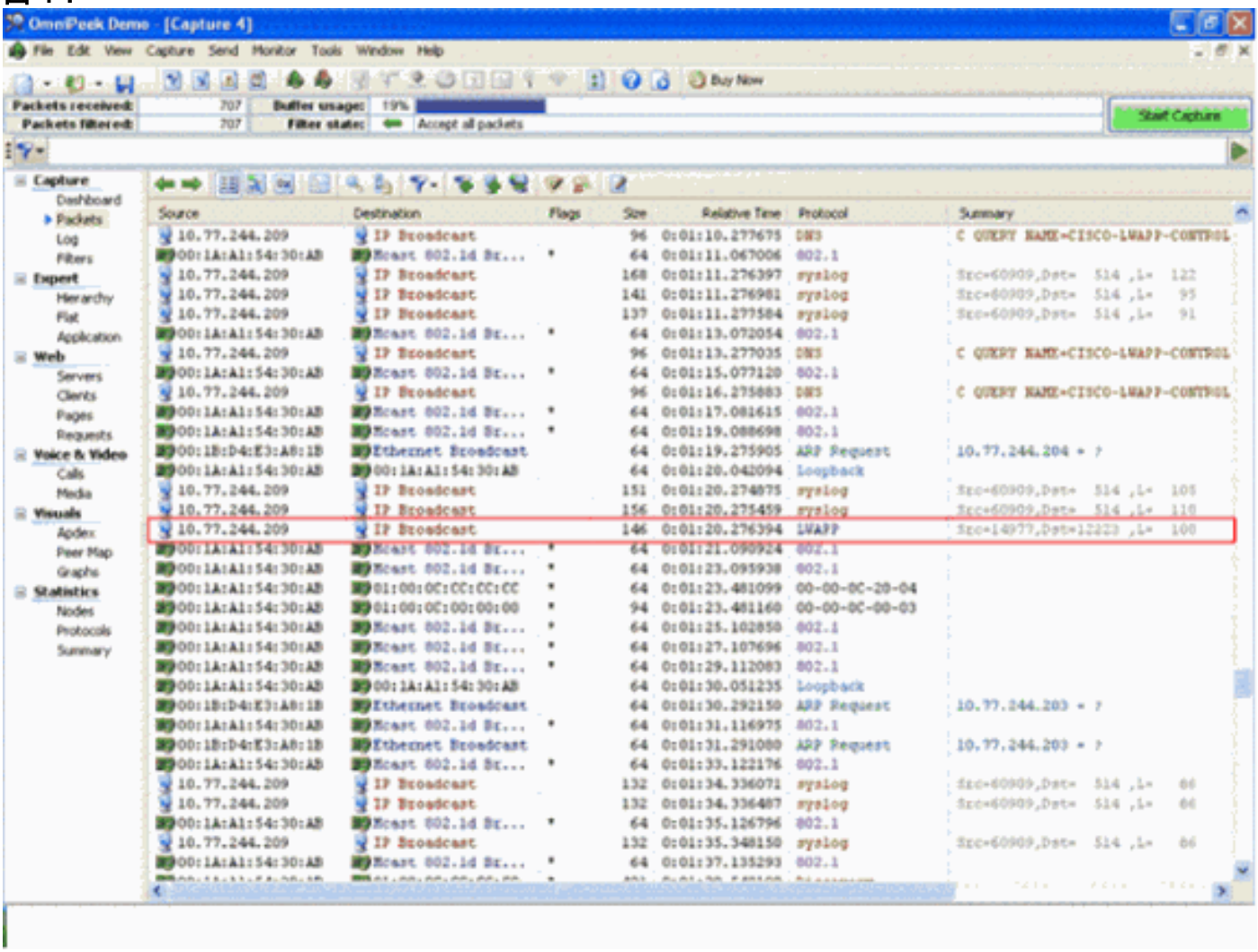
1. OmniPeek 5.0 アプリケーションを開きます。
2. [New Packet Capture] ウィンドウを開くために、[Start] ページで、[File] > [New] の順にクリックします。[Capture Options] という名前の小さいウィンドウが表示されます。このウィンドウには、パケット キャプチャのオプションのリストが含まれています。
3. [Adapter] **オプションから、そのアダプタを使用してパケットをキャプチャするアダプタを選択します。**アダプタに関する説明は、アダプタを強調表示するとその下に表示されます。ローカルのイーサネット アダプタを使用し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。
7. [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。

図 1：



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。

関連情報

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