# LWAPP dekodiert Enablement für WildPackets OmniPeek- und EtherPeek 3.0-Software

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Ändern Sie die LWAPP-Decode-Datei. Ändern Sie TCP\_UDP\_Ports.dcd Ändern Sie die Datei PSPT.XML LWAPP-Decode in OmniPeek 5.0 Überprüfen Zugehörige Informationen

#### **Einführung**

WildPackets OmniPeek (und EtherPeek) verfügen über LWAPP-Decodes (Lightweight Access Point Protocol), sind jedoch nicht angeschlossen. In diesem Dokument wird erläutert, wie Sie die LWAPP-Decodierung aktivieren und die Software zum Anzeigen von LWAPP verwenden. In diesem Dokument wird das Verfahren für EtherPeek 3.0 und OmniPeek 5.0 verwendet.

Hinweis: Das Verfahren für OmniPeek 3.0 ist mit dem von EtherPeek 3.0 identisch.

**Hinweis:** Der einzige Unterschied zwischen OmniPeek und EtherPeek ist der Speicherort der Dateien.

- Der Pfad für OmniPeek ist C:/Programme/WildPackets/OmniPeek.
- Der Pfad für EtherPeek ist C:/Programme/WildPackets/EtherPeek.

## Voraussetzungen

#### <u>Anforderungen</u>

Cisco empfiehlt, über Kenntnisse der Softwareprogramme EtherPeek und OmniPeek 3.0 und 5.0 zu verfügen. Weitere Informationen zu EtherPeek finden Sie in den <u>EtherPeek-FAQ</u>. Informationen zu OmniPeek finden Sie in <u>Einführung von Omni</u>.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- OmniPeek 3.0
- EtherPeek 3.0
- OmniPeek 5.0

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

# Ändern Sie die LWAPP-Decode-Datei.

Um die LWAPP-Dekodierungsdatei zu ändern, fügen Sie der LWAPP-Funktion "ETHR 0 90 c2 AP Identity:;" hinzu. Diese befindet sich direkt unter der Leitung "LABL 0 0 0 b1 Light Weight Access Point Protocol\LWAPP:;" in der Zeile LWAPP-light\_weight\_..protocol.dcd-Datei (C:\Program Files\WildPackets\EtherPeek\Decodes).

# Ändern Sie TCP\_UDP\_Ports.dcd

In der Datei TCP\_UDP\_Ports.dcd (C:\Program Files\WildPackets\EtherPeek\Decodes) müssen die folgenden beiden Zeilen enthalten sein:

0x2fbe | LWAPP; 0x2fbf | LWAPP;

**Hinweis:** Durch diesen Prozess werden keine Ports auf dem Host-Computer geöffnet. Aus diesem Grund sind bei diesem Schritt keine Sicherheitsrisiken für den Host-Computer vorhanden.

Auf diese Weise sind die beiden Ports 1222 und 12223 enthalten.

# Ändern Sie die Datei PSPT.XML

Gehen Sie wie folgt vor:

 Fügen Sie im Abschnitt User Datagram Protocol (UDP) der Datei pspecs.xml (C:\Program Files\WildPackets\EtherPeek\1033) die folgenden Zeilen hinzu:Hinweis: Sichern Sie zuerst die Originaldatei.

```
<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 Control</LName>
<DescID>6677</DescID>
<CondExp><![CDATA[(SrcPort == 12223) || (DestPort == 12223)]]></CondExp>
</PSpec>
</PSpec>
```

2. Starten Sie OmniPeek oder EtherPeek neu, damit Ihre Änderungen wirksam werden.

### LWAPP-Decode in OmniPeek 5.0

OmniPeek Version 5.0 ist das Erfassungstool der nächsten Generation für OmniPeek Version 3.0. In der Version 5.0 sind die LWAPP-Decodes standardmäßig integriert. Daher sind keine weiteren Änderungen in der Datei erforderlich. Im folgenden Beispiel wird jedoch veranschaulicht, wie ein Protokollfilter in der Version 5.0 mithilfe einer IP-Adresse und der Portnummer definiert wird:

- 1. Öffnen Sie die Anwendung OmniPeek 5.0.
- Klicken Sie auf der Startseite auf Datei > Neu, um ein Fenster zur Erfassung neuer Pakete zu öffnen. Ein kleines Fenster mit dem Namen Capture Options (Erfassungsoptionen) wird angezeigt. Sie enthält eine Liste von Optionen für die Paketerfassung.
- 3. Wählen Sie aus der Adapter-Option einen Adapter aus, um Pakete mit diesem Adapter zu erfassen. Die Beschreibung des Adapters wird unten angezeigt, während Sie den Adapter markieren. Wählen Sie Local Area Connection aus, um Pakete mit dem lokalen Ethernet-Adapter zu erfassen.
- 4. Klicken Sie auf OK.Das Fenster Neue Erfassung wird angezeigt.
- 5. Klicken Sie auf die Schaltfläche **Erfassung starten**.Das Tool erfasst Pakete für die in der Software definierten Protokolle. Um die erfassten Pakete anzuzeigen, klicken Sie auf die Option **Pakete** unter dem Menü **Erfassung** links.
- Klicken Sie mit der rechten Maustaste auf eines der erfassten Pakete, und klicken Sie auf Filter erstellen, um ein neues Protokoll zu definieren. Das Fenster Filter einfügen wird angezeigt.
- 7. Geben Sie im Feld Filter einen Namen ein, um das Protokoll zu identifizieren. Aktivieren Sie den Adressfilter. Wählen Sie den Typ als IP aus, um Pakete zu und von bestimmten IP-Adressen zu erfassen. Geben Sie für die Adresse1 die Quell-IP-Adresse ein. Geben Sie für die Adresse 2 eine IP-Adresse ein, wenn das Ziel über eine statische IP-Adresse verfügt. Wählen Sie Option als Any Address (Beliebige Adresse) aus, wenn das Ziel über DHCP eine IP-Adresse erhält. Um die Richtung des Paketflusses anzugeben, klicken Sie auf die Schaltfläche Both (Beide Richtungen), und wählen Sie eine der drei Optionen aus. Das Pfeilsymbol auf der Schaltfläche gibt die gewählte Richtung an. Aktivieren Sie den Port-Filter. Wählen Sie den Typ für den vom Protokoll verwendeten Port aus, z. B. TCP. Geben Sie für Port 1 einen Port ein, der in der Quelle verwendet wird. Geben Sie für Port 2 eine Portnummer ein, wenn für das Ziel ein gut definierter Standardport verwendet wird. Andernfalls wählen Sie die Option Any port (Beliebiger Port), wenn das Ziel einen zufälligen Port verwendet. Wählen Sie eine *Richtung* aus der Schaltfläche Both Directions (Beide Richtungen).

8. Wiederholen Sie diese Schritte, um ein neues benutzerdefiniertes Protokoll zu definieren.

# <u>Überprüfen</u>

Mit OmniPeek 5.0 können Sie im Erfassungsbildschirm überprüfen, ob das Tool standardmäßig das LWAPP-Protokoll erfasst, wenn ein LWAPP-Ereignis ausgelöst wird. <u>Abbildung 1</u> zeigt die LWAPP-Protokollerfassung während der von der LAP durchgeführten Erkennungsanfrage.

ConniPeek Dem	o - [Capture 4]									×
File Edit View	Capiture Send Monitor Tool	s Wedow Help .				and the second second	1			х
(A . 8) - 14		9720001	19113	0	a Day Now					
Packets received: Packets filtered:	707         Buffer usaget         19%           707         Filter statet         4m           Accept all packets						Shet Cephins			
-										•
Capture										
Dashboard Exclusion	Source	Destination	Flags	524	Relative Time	Protocol	Sumary			-
Log	10.77.244.209	IP Broadcast		96	0:01:10.277675	DW3	C OVERY NAME-CISC	CO-LWAPP-	-CONTROL	
Fitters	#00:1A:A1:54:30:AB	BROAST 802.14 BE		64	0:01:11.067006	402.1				
Expert	10.77.244.209	IP Broadcast		168	0:01:11.276397	syslog	SEC-60909,D#t= 3	514 .1+	122	
Herarchy	9 10.77.244.209	IP Broadcast		141	0:01:11.276981	syslog	Szc=60909,D#t= 3	514 ,1+	95	
Flat	2 10.77.244.209	IF Broadcast		137	0:01:11.277584	syslog	SEC-60909,D9t- 3	514 ,1-	91	
Application	#900:1A:A1:54:30:AB	Bass 802.14 BE		64	0:01:13.072054	002.1				
≡ Web	10.77.244.209	🚼 IF EcondCast		96	0:01:13.277035	08/5	C QUERT NAME+CISC	CO-LWAPP-	-CONTROL	
Servers	#900:1A:A1:54:30:A8	BCast 802.14 BE	•	64	0:01:15.077120	802.1				
Clerks	3 10.77.244.209	🔮 IF Buoadcast		96	0:01:16.275883	04/5	C QUERT NAME-CISC	0-14427-	-C0877901	
Pages	#900:1A:A1:54:30:AB	Reast 802.14 Sr		64	0:01:17.081615	002.1				
Requests	B900:1A:A1:54:30:AB	Micast 802.1d Sr	•	64	0:01:19.088698	802.1				
🗟 Yoice & Video	B900:18:D4:E3:A8:18	Ethernet Scoadcast		64	0:01:19.275905	ARP Request	10.77.244.204 + 1	P		
Calls	2900:1A:A1:54:30:AB	B) 0011A1A11541301A8		64	0:01:20.042094	Loopback				
Media	10.77.244.209	IP Buosdcast		151	0:01:20.274975	syslog	SEC-60909,D95+ 1	514 JLA	105	
R Visuals	10.77.244.209	IP Broadcast		156	0:01:20.275459	syslog	SEC+60909,Date	514 .14	110	i.
Apdex	3 10.77.244.209	IF Brosdcast		146	0:01:20.276394	14472	SEC+14977,Dat+121	- «باير 201	100	J.
Peer Map	#900:1A1A1:54:30:A8	BCASE 802.14 St		64	0:01:21.090924	002.1				λ.
Graphs	#P00:1A:A1:54:30:AB	My Scart 602.1d Br	•	64	0:01:23.095938	002.1				
Statistics	BP00:1A:A1:54:30:AB	B0110010C1CC1CC1CC	•	64	0:01:23,481099	00-00-00-20-04				
Nodes	2900:1A:A1:54:30:AB	B9 0110010C100100100		94	0:01:23.481160	00-00-00-00-03				
Protocols	#900:1A:A1:54:30:AB	MONST 002.14 DE	. *	64	0101125.102850	002-1				
Summary	#P00:1A:A1:54:30:AB	BORNE BO2.1d BE	•	64	0101127.107696	802-1				
	#900:1A:A1:54:30:AB	My Mcast 802.1d Br	•	64	0:01:29.112083	802-1				'n
	#900:1A:A1:54:30:AB	19 00: 1A1A1: 54: 30: AB		64	0:01:30.051235	Loopback				
	BP00:18:D4:£3:A8:18	Ethernet Broadcast		64	0:01:30.292150	ARP Request	10.77.244.203 = 1	7		
	#P0011A1A11541301AB	My Nosst, 802.1d Bc	•	64	0:01:31.116975	802.1	Las an ere ere .			
	#900:18:D-4:E3:A8:18	MyEthernet Broadcast		64	0101131.291080	ARP Request	10,77,244,203 = 1	7		
	#900:1A:A1:54:30:AB	BRCast 802.14 St	•	64	0:01:33.122176	002.1	Lass services and the			
	10.77.244.209	IF Broadcast		132	0:01:34.336071	syslog	110-60909,Date 1	114 ,14	01	
	3 10.77.244.209	TF Broadcast		132	0:01:34.336467	mistod	SIC+60909,Date 1	514 ,6*	01	
	##00:1A:A1:54:30:AB	Waters 005.14 BE		64	0:01:35.126796	02.1	Party and a second second			
	10.77.244.209	TF Scoadcast		132	0:01:35.348150	sAsrod	21C+60909,D86+ 1	14,14	06	
	#0011A1A11541301AB	ACASE 002.1d BE		64	0:01:37.135293	002.1				*
	C. Constant Constant of Constant		10000	PARTY AND D	Contract of the second second	Space of the second second second			1.11.1	

Doppelklicken Sie auf das Paket, um die Details zum Paket anzuzeigen.

## Zugehörige Informationen

- <u>EtherPeek-FAQ</u>
- Einführung von Omni
- OmniPeek 5.0 herunterladen
- <u>Technischer Support und Dokumentation Cisco Systems</u>