Verwenden von Wireshark auf einem Cisco Business WAP für die Paketanalyse: Direkter Stream zu Wireshark

Ziel

In diesem Artikel wird erläutert, wie Sie mithilfe eines Cisco Business Wireless Access Point (WAP) eine Paketerfassung des Netzwerkverkehrs durchführen und diesen direkt an Wireshark streamen.

Inhalt

- Einführung und häufig gestellte Fragen
- Was ist eine Paketerfassung?
- Welche Arten von Paketen können erfasst werden?
- Wie kann eine Paketerfassung auf einem WAP durchgeführt werden?
- Wo kann ich das Paket streamen?
- Anwendbare Geräte und Softwareversion
- Wireshark herunterladen
- Melden Sie sich beim WAP an.
- Erläuterung zur Remote-Paketerfassung
- <u>Streamen einer Erfassung direkt an Wireshark</u>

Einführung und häufig gestellte Fragen

Konfigurationsänderungen, Überwachung und Fehlerbehebung sind häufig ein Thema, mit dem sich Netzwerkadministratoren auseinander setzen müssen. Ein einfaches Tool zu verwenden ist unschätzbar! In diesem Artikel sollen die Grundlagen der Paketerfassung und das Streaming der Pakete an Wireshark erläutert werden. Wenn Sie mit diesem Prozess nicht vertraut sind, lassen Sie uns einige Fragen beantworten, die Sie möglicherweise bereits gestellt haben.

Zunächst einmal ist Wireshark ein kostenloser Paket-Analyzer für alle, die eine Fehlerbehebung im Netzwerk durchführen möchten. Wireshark bietet viele Optionen für die Erfassung und Sortierung des Datenverkehrs durch mehrere verschiedene Parameter. Weitere Informationen zu dieser Open-Source-Option finden Sie unter <u>Wireshark</u>.

Was ist eine Paketerfassung?

Eine Paketerfassung, auch als PCAP-Datei bezeichnet, ist ein Tool, das bei der Fehlerbehebung hilfreich sein kann. Sie kann jedes Paket, das zwischen Geräten in Ihrem Netzwerk gesendet wird, in Echtzeit aufzeichnen. Durch das Erfassen von Paketen können Sie die Details des Netzwerkverkehrs eingehend untersuchen. Dies kann alles von der Geräteerkennung, der Protokollierung und der fehlgeschlagenen Authentifizierung umfassen. Sie können den Pfad eines bestimmten Datenverkehrsflusses und jede Interaktion zwischen Geräten in ausgewählten Netzwerken sehen. Diese Pakete können bei Bedarf zur weiteren Analyse gespeichert werden. Es ist wie eine Röntgenaufnahme der internen Abläufe des Netzwerks durch die Übertragung von Paketen.

Welche Arten von Paketen können erfasst werden?

Das WAP-Gerät kann die folgenden Pakettypen erfassen:

·802.11-Pakete, die drahtlos auf den Funkschnittstellen empfangen und übertragen werden. Zu den auf den Funkschnittstellen erfassten Paketen gehört der 802.11-Header.

·802.3-Pakete, die über die Ethernet-Schnittstelle empfangen und übertragen werden.

·802.3-Pakete, die über die internen logischen Schnittstellen empfangen und übertragen werden, z. B. Virtual Access Points (VAPs) und Wireless Distribution System (WDS)-Schnittstellen.

Wie kann eine Paketerfassung auf einem WAP durchgeführt werden?

Es stehen zwei Methoden zur Paketerfassung zur Verfügung:

 Local Capture Method - Erfasste Pakete werden in einer Datei auf dem WAP-Gerät gespeichert. Das WAP-Gerät kann die Datei auf einen TFTP-Server (Trivial File Transfer Protocol) übertragen. Die Datei ist im PCAP-Format formatiert und kann mit Wireshark überprüft werden. Sie können Datei auf diesem Gerät speichern auswählen, um die lokale Erfassungsmethode auszuwählen.

Wenn Sie die lokale Erfassungsmethode mit der neuesten Webbenutzeroberfläche bevorzugen, können Sie mithilfe von Wireshark auf einem WAP für die Paketanalyse auschecken: Datei hochladen.

Wenn Sie einen Artikel anzeigen möchten, der die ältere GUI für die lokale Erfassungsmethode verwendet, sehen Sie sich <u>Configure Packet Capture to Optimize Performance on a Wireless</u> <u>Access Point an</u>.

2. *Remote Capture Method* - Erfasste Pakete werden in Echtzeit an einen externen Computer umgeleitet, auf dem Wireshark ausgeführt wird. Sie können *Stream zu einem Remote-Host* auswählen, um die Remote-Erfassungsmethode auszuwählen. Der Vorteil dieser Methode besteht darin, dass die Menge an Paketen, die erfasst werden können, nicht begrenzt ist.

Der Schwerpunkt dieses Artikels ist Stream zu einem Remote-Host, sodass, wenn dies Ihre Präferenz ist, lesen Sie weiter!

Wo kann ich das Paket streamen?

Die Funktion zur Wireless-Paketerfassung ermöglicht das Erfassen und Speichern der vom WAP-Gerät empfangenen und übertragenen Pakete. Die erfassten Pakete können dann von einem Netzwerkprotokollanalysator zur Fehlerbehebung oder Leistungsoptimierung analysiert werden. Online sind zahlreiche Paketanalyseanwendungen von Drittanbietern verfügbar. In diesem Artikel konzentrieren wir uns auf Wireshark.

Einige Modelle der Cisco Business WAPs können Pakete in Echtzeit an CloudShark, eine webbasierte Website für Paket-Decoder und -Analyse, senden. Sie ähnelt der Wireshark-Benutzeroberfläche für die Paketanalyse, die viele zusätzliche Optionen mit einem Abonnement enthält. Sie können *Stream to CloudShark* auswählen, um die Remote-Erfassungsmethode auszuwählen. Klicken Sie auf die folgenden Links, um weitere Informationen zu erhalten:

- <u>CloudShark</u> (ihre offizielle Website)
- Integration von CloudShark für die Paketanalyse auf einem WAP125 oder WAP581
- <u>CloudShark-Integration mit WAP571 und WAP571E</u>

Weder Wireshark noch CloudShark sind Eigentum von Cisco oder werden von Cisco unterstützt. Sie sind nur zu Demonstrationszwecken enthalten. Wenden Sie sich für Support an <u>Wireshark</u> oder <u>CloudShark</u>.

Anwendbare Geräte und Softwareversion

- WAP125 Version 1.0.2.0
- WAP150 Version 1.1.1.0
- WAP121 Version 1.0.6.8
- WAP361 Version 1.1.1.0
- WAP581 Version 1.0.2.0
- WAP571 Version 1.1.0.4
- WAP571E Version 1.1.0.4

Wireshark herunterladen

Schritt 1

Öffnen Sie die <u>Wireshark</u>-Website. Wählen Sie die entsprechende Version aus. Klicken Sie auf **Download (Herunterladen).** Sie sehen den Fortschritt des Downloads unten links im Bildschirm.

Schritt 2

Gehen Sie zu *Downloads* auf Ihrem Computer, und wählen Sie die Wireshark-Datei aus, um die Anwendung zu installieren.

```
Wireshark-win64-3.0.6.exe 10/30/2019 4:05 PM Application 57,887 KB
```

Melden Sie sich beim WAP an.

Geben Sie in Ihrem Webbrowser die IP-Adresse des WAP ein. Geben Sie Ihre Anmeldeinformationen ein. Wenn Sie zum ersten Mal auf dieses Gerät zugreifen oder das Gerät auf die Werkseinstellungen zurückgesetzt haben, lautet der Standardbenutzername und das Standardkennwort *cisco*. Wenn Sie Anweisungen zur Anmeldung benötigen, können Sie die Schritte im Artikel <u>Access the Web-based Utility (Zugriff auf das webbasierte Dienstprogramm)</u> <u>des Wireless Access Point (WAP)</u> befolgen.

ılıılı cısco

Wireless Access Point



Erläuterung zur Remote-Paketerfassung

Mit der Funktion zur Paketerfassung per Remote-Zugriff können Sie einen Remote-Port als Zielport für die Paketerfassung festlegen. Diese Funktion arbeitet mit dem Wireshark-Netzwerkanalysetool für Windows zusammen. Ein Paketerfassungsserver wird auf dem WAP-Gerät ausgeführt und sendet die erfassten Pakete über eine TCP-Verbindung (Transmission Control Protocol) an das Wireshark-Tool.

Auf einem Microsoft Windows-Computer mit dem Wireshark-Tool können Sie den erfassten Datenverkehr anzeigen, protokollieren und analysieren. Die Remote-Paketerfassung ist eine Standardfunktion des Wireshark-Tools für Windows.

Obwohl die Remote-Paketerfassung von Linux nicht unterstützt wird, funktioniert das Wireshark-Tool unter Linux und bereits erstellte Erfassungsdateien können angezeigt werden.

Wenn der Remote-Erfassungsmodus verwendet wird, speichert das WAP-Gerät keine erfassten Daten lokal in seinem Dateisystem.

Wenn zwischen dem installierten Wireshark-Computer und dem WAP-Gerät eine Firewall installiert ist, muss Wireshark die Firewall-Richtlinie des Computers durchlaufen dürfen. Die Firewall muss auch so konfiguriert werden, dass der Wireshark-Computer eine TCP-Verbindung zum WAP-Gerät initiieren kann.

Streamen einer Erfassung direkt an Wireshark

Um eine Remote-Erfassung auf einem WAP-Gerät mithilfe der Option Stream to a Remote Host (

Stream zu einem Remote-Host) zu initiieren, führen Sie die unten aufgeführten Schritte aus.

Schritt 1

Navigieren Sie auf dem WAP zu Fehlerbehebung > Paketerfassung.

Für die Paketerfassungsmethode:

- 1. Wählen Sie Stream zu einem Remote-Host aus dem Dropdown-Menü aus.
- Verwenden Sie im Feld Remote Capture Port (Remote-Erfassungsport) den Standard-Port von 2002, oder geben Sie, wenn Sie einen anderen als den Standard-Port verwenden, die gewünschte Portnummer ein, die für die Verbindung von Wireshark mit dem WAP-Gerät verwendet wird. Der Port-Bereich liegt zwischen 1025 und 65530.
- 3. Es gibt zwei *Modi* für die Paketerfassung. Wählen Sie aus, was für Ihr Szenario am besten geeignet ist.

·Gesamter Wireless-Datenverkehr - Erfassen Sie alle Wireless-Pakete in der Luft.

·*Datenverkehr zu/von diesem AP* - Erfassen Sie das vom WAP oder vom empfangenen WAP gesendete Paket.

- 4. Aktivieren Sie Filter aktivieren.
- 5. Folgende Optionen stehen zur Auswahl:

·*Ignore Beacons*: Aktivieren oder Deaktivieren der Erfassung von 802.11-Beacons, die vom Funkmodul erkannt oder übertragen werden. Beacon-Frames sind Broadcast-Frames, die Informationen über ein Netzwerk übertragen. Der Zweck eines Beacons besteht darin, ein bestehendes Wireless-Netzwerk anzukündigen.

·Filter on Client: Geben Sie nach der Aktivierung die MAC-Adresse für den WLAN-Client-Filter an. Beachten Sie, dass der Client-Filter nur aktiv ist, wenn eine Erfassung auf einer 802.11-Schnittstelle durchgeführt wird.

·Auf SSID filtern: Diese Option wird für diesen Stream zu einer Remote-Host-Option deaktiviert.

6. Klicken Sie auf Übernehmen, um die Einstellungen zu speichern.

\bigotimes	Getting Started	Cisco WAP150-wap0a4dee cisco ? 🕄	CISCO	• 🛛 🔂
**	Administration			
٠	System Configuration	Packet Capture 3 (Apply Cancel	Packet Capture	Apply Cancel
(î;	Wireless	Beeliet Centure Methods	Desket Centure Methods	
ŝ	Wireless Bridge	Stream to a Remote Host	Packet Capture Method.	
X\$	Fast Roaming	Remote Capture Port: 2002	Remote Capture Port: 💡	
đ.	Single Point Setup	Mode: O All Wireless Traffic O Traffic to/from this AP	Mode:	
T	Access Control	Enable Filters:	Enable Filters:	2
	Cisco Umbrella	Ignore Beacons:	Ignore Beacons:	•
•	Monitor	Filter on Client: ? 00:00:00:00:00:00	Filter on Client: 🧿	
J	Troubleshoot Packet Capture	Filter on SSID:	Filter on SSID:	

Klicken Sie auf das Symbol Erfassung starten.

Packet Capture Status	
Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB
Refresh	

Schritt 3

Ein Popup-Fenster "Bestätigen" wird geöffnet. Klicken Sie auf Ja, um die Erfassung zu starten.



Schritt 4

Klicken Sie auf die Schaltfläche Aktualisieren, um den aktuellen Status zu überprüfen.

Packet Capture Status	
Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB
Refresh	
00 🕹 🔸	

Schritt 5

Sie können jetzt sehen, dass der aktuelle Erfassungsstatus Stream zu einem Remote-Host ist.



Da Wireshark bereits heruntergeladen wurde, können Sie auf das Programm zugreifen, indem Sie **Wireshark** in der Suchleiste von Microsoft Windows eingeben und die Anwendung auswählen, wenn es eine Option ist.

ඛ	Best match
o	Wireshark App Based on past activity
	Apps
	🗐 Word
	📧 WordPad
	Settings
	🕼 Change Wi-Fi settings
	Connect to a wireless display
	$\mathbb{F}_{\mathcal{P}}^{\mathbb{N}}$ Turn wireless devices on or off
	Connect wireless Xbox One controllers
	Search the web
ŝ	✓ wir - See web results
	Documents - This PC (3+)
	Photos (4+) •
	9 wireshark

Schritt 7

Navigieren Sie zu Erfassen > Optionen...



Klicken Sie im neuen Popup-Fenster *Wireshark - Capture Interfaces* (*Wireshark - Erfassungsschnittstellen*) auf **Interfaces verwalten**...

Local Area Connection* 11				2116
Local Area Connection 11		Ethernet	\checkmark	def
Local Area Connection* 10		Ethernet	~	def
> Wi-Fi		Ethernet	\checkmark	def
Local Area Connection* 9		Ethernet	\checkmark	def
> Bluetooth Network Connect	ion	Ethernet	\checkmark	def
> Ethernet	mahul	Ethernet	\checkmark	def
Local Area Connection* 1		Ethernet	\checkmark	def
> Local Area Connection* 2		Ethernet	\checkmark	def
> Ethernet 3		Fthernet	\checkmark	def `
Enable promiscuous mode on all	interfaces		Manage Inter	faces.

Schritt 9

Navigieren Sie im neuen Popup-Fenster *Manage Interfaces (Schnittstellen verwalten*) zu **Remote Interfaces (Remote-Schnittstellen),** und klicken Sie auf das **Plus-Symbol**, um die Schnittstelle hinzuzufügen.

🧲 Manage Interfaces	?	\times
Local Interfaces Pipes Remote Interfaces		
Show Host / Device URL		
2 +- Rer	note Settin	gs
This version of Wireshark does not save remote settings. OK Cancel	Help)

Geben Sie im neuen Popup-Fenster "*Remote Interface*" (*Remote-Schnittstelle*) den *Host ein:* IP-Adressdetails (die IP-Adresse des WAP-Geräts, in der Sie die Remote-Erfassung gestartet haben) und *Port:* Nummer (auf WAP für die Remote-Erfassung konfiguriert). In diesem Fall betrug die IP-Adresse des WAP-Geräts 192.168.1.134. Sie können die Option *Null-Authentifizierung* oder *Passwortauthentifizierung* auf Basis Ihrer Einstellungen auswählen. Wenn Sie diese Option auswählen, geben Sie bitte die entsprechenden *Benutzernamen* und *Passwortdetails* ein. Klicken Sie auf **OK**.

🦲 Rei	mote li	nterface				?	×
Host:	192.1	58.1.134					~
Port:	2002						
				1			
			(2			
Auth	enticati	on					
	Null aut	henticatio	n				
\bigcirc	Passwor	d authen	ticatio	n			
User	name:						
Pass	word:						ノ
		3			OK	Can	cel

Schritt 11

Unter der Registerkarte *Remote-Schnittstellen* können Sie alle Schnittstellen des Remote-WAP-Geräts sehen. Möglicherweise möchten Sie einige dieser Pakete deaktivieren, um das Volumen der erfassten Pakete zu reduzieren. Wenn Beacon-Pakete angezeigt werden sollen, bleiben die ausgewählten Funkschnittstellen erhalten. Klicken Sie auf **OK**.

Manage	Interfaces

?

Show	Host / Device URL
~	192.168.1.134
\checkmark	rpcap://192.168.1.134:2002/sw0
\checkmark	rpcap://192.168.1.134:2002/wlan0
\checkmark	rpcap://192.168.1.134:2002/wlan1
\checkmark	rpcap://192.168.1.134:2002/radio1
\checkmark	rpcap://192.168.1.134:2002/any
\checkmark	rpcap://192.168.1.134:2002/brtrunk
\checkmark	rpcap://192.168.1.134:2002/eth0
\checkmark	rpcap://192.168.1.134:2002/wlan0vap1
\checkmark	rpcap://192.168.1.134:2002/wlan1vap1
\checkmark	rpcap://192.168.1.134:2002/radio2
\checkmark	rpcap://192.168.1.134:2002/lo
	Device Collinso
-	Keniote Settings
version of V	Vireshark does not save remote settings.

Schritt 12

Neu hinzugefügte Schnittstellen spiegeln nun das Fenster *Wireshark - Capture Interfaces* wider. **Wählen Sie** die Schnittstelle aus, die überwacht werden soll, und klicken Sie auf **Start**, um die Pakete anzuzeigen.

	erface	Traffic	Link-layer Header	Promiscuous	Snaplen (Buffer (M	Monito	Capture Filter	1
	Local Area Connection* 9		Ethernet		default	2	_		
>	Bluetooth Network Connection		Ethernet		default	2			
	Ethernet	A	Ethernet		default	2			
×	Local Area Connection* 1		Ethernet		default	2	_		
	Local Area Connection* 2		Ethernet		default	2			
×	Ethernet 3		Ethernet		default	2	_		
	Ethernet 4		Ethernet		default	2	_		
	USBPcap1		USBPcap	_	_		_		
	USBPcap2		USBPcap						
	Cisco remote capture		Remote candent DLT	_					
	Random packet generator		Generatorendent DLT	_					
	SSH remote capture		Remote candent DLT		_	_	_		
	UDP Listener remote capture		Exported PDUs						
-	rpcap://192.168.1.134:2002/sw0		Ethernet	×	default	2	-		
	rpcap://192.168.1.134:2002/wlan0		Ethernet		default	2	_		
	rpcap://192.168.1.134:2002/wlan1		Ethernet		default	2	_		
	rpcap://192.168.1.134:2002/radio1		802.11 plutap header		default	2			
	rpcap://192.168.1.134:2002/any		Linux cooked v1		default	2			
	rpcap://192.168.1.134:2002/brtrunk		Ethernet		default	2			
	rpcap://192.168.1.134:2002/eth0		Ethernet		default	2			
	rpcap://192.168.1.134:2002/wlan0vap1		Ethernet		default	2			
	rpcap://192.168.1.134:2002/wlan1vap1		Ethernet		default	2			
	rpcap://192.168.1.134:2002/radio2		802.11 plutap header		default	2	_		
	rpcap://192.168.1.134:2002/lo (loopback)	Ethernet		default	2	- /		

Wenn beim Versuch, die Pakete anzuzeigen, Probleme auftreten, bedeutet dies, dass der Dienst *Remote Packet Capture Protocol* nicht auf Ihrem System funktioniert. Der Remote Packet Capture Protocol-Dienst muss zuerst auf der Zielplattform ausgeführt werden, bevor Wireshark eine Verbindung zu ihm herstellen kann. Weitere Informationen erhalten Sie, wenn Sie auf den Link <u>Remote Capture Interfaces</u> through Wireshark klicken.

Schritt 13

Klicken Sie auf dem WAP auf das Symbol Stopp Capture (Erfassung beenden), um den

Erfassungsprozess zu stoppen.



Schritt 14

Ein Popup-Fenster *für eine Warnung* wird angezeigt. Klicken Sie auf **OK**, um die Remote-Erfassung zu beenden.



Sie können die Paketerfassung auch unterbrechen, indem Sie in der Anwendung Wireshark auf die **Stopp-**Schaltfläche klicken.

Schritt 15

Jetzt wird der *aktuelle Erfassungsstatus aufgrund von Verwaltungsaktionen* als *Beendet* angezeigt, und die *Paketerfassungszeit* wird angezeigt, um die Gesamtaufzeichnungsdauer anzuzeigen.



Die Dateigröße für die Paketerfassung wird als 0 KB angezeigt. Darüber hinaus funktionieren

Dateidownload-Optionen in diesem Szenario nicht.

Schritt 16

Auf Wireshark können Sie die Paketerfassung anzeigen.

Apply a display filter <				Epression	+ 50
Time	Source	Destination	Protocol	Length Info	
3281 33.150989	9e:93:4e:39:28:b7	Broadcast	882.11	259 Beacon frame, SN+1785, FN+0, Flags=, BI+1_	
3282 33.161422	Cisco_a0:e7:32	Broadcast	882.11	335 Beacon frame, SN+141, FN+0, Flags=, BI+10_	
3283 33.184447	Cisco_44:5a:0b	Broadcast	802.11	362 Beacon frame, SN=1515, FN=0, Flags=, BI=1_	
3284 33.188268	ZyxelCom_e9:05:b5	Broadcast	882.11	303 Beacon frame, SN+3972, FN+0, Flags+, BI+1_	
3285 33.196947	1e:f2:9a:d7:85:18	Broadcast	802.11	246 Beacon frame, SN+3526, FN+0, Flags=, BI=1_	
3286 33.209762	HitronTe_cf:d2:18	Broadcast	882.11	305 Beacon frame, SN=3268, FN=0, Flags=, BI=1_	
3287 33.236448	BelkinIn_d8:57:1e	Broadcast	802.11	254 Beacon frame, SN+1378, FN+0, Flags+, BI+1_	
3288 33.251356	Cisco_c0:74:b8	IPv4mcast_12	802.11	133 Data, SN=0, FN=0, Flags=.pF.	
3289 33.248358	Google_d7:85:18	Broadcast	802.11	272 Beacon frame, SN+1408, FN+0, Flags+, BI+1_	
3290 33.251099	Cisco_c0:74:b8	IPv4mcast_12	802.11	133 Data, SN=0, FN=0, Flags=.pF.	
3291 33.251227	Cisco_c0:74:b8	IPv4mcast_12	802.11	97 Data, SN=0, FN=0, Flags=.pF.	
3292 33.253424	9e:93:4e:39:28:b7	Broadcast	802.11	259 Beacon frame, SN=1786, FN=0, Flags=, BI=1_	
3293 33.263821	Cisco_a0:e7:32	Broadcast	802.11	335 Beacon frame, SN=142, FN=0, Flags=, BI=10	
1204 11 264825	Raspberr_89:85:9c	Broadcast	802.11	123 Data, SN=143, FN=0, Flags=.pmF.	
PEP- 07-204023					
3295 33.266381	Raspberr_89:85:9c	Broadcast	802.11	123 Data, SN=204, FN=0, Flags=.pF.	
3295 33.266381 3296 33.251464 Frame 3358: 303 bj Radiotap Header vi 892.11 radio info	Raspberr_89:85:9c Cisco c0:74:b8 ytes on wire (2424 bit 8, Length 25 mation	Broadcast IPv4mcast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bi	123 Dats, SM-284, FN+0, Flags-pF. 97 Data, SH=0, FN+0, Flags-pF. its) on interface 1	_
3295 33.266381 3296 33.251464 Frame 3358: 303 by Radiotap Header vi 902.11 radio info 1000 1000 1000 1000 1000 1000 1000 100	Raspberr_09:85:9c <u>Cisco c0:74:b8</u> /tes on wire (2424 bit 0, Length 25 mation n frame, Flags: ess LAN	Broadcast IPv4ecast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bi	120 Data, SH-944, New, Flags-gf. 97 Data, SH-RHE, Flags.g., J. its) on interface 1	
2295 33.26581 3296 33.251464 Frame 3358: 303 by Radiotap Header vi 802.11 radio info IEEE 802.11 wirels Malformed Packet	Raspberr_89:85:9c <u>Cisco c0:74:b8</u> /tes on wire (2424 bit 0, Length 25 mation n frame, Flags: rss LAN : IEEE 002.11]	Broadcast IPy4ecast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bi	122 Dets, Skrödek, Friede, Flager-g,F. 25 Dets, Skröde, Friede, Flager-g,F. tsj en interface 1	
3295 33.266381 3295 33.266381 3295 33.251464 irame 3358: 303 bb tadiotap Header vi 802.11 radio info IEEE 802.11 Beaco IEEE 802.11 winel Nalformed Packet	Raspberr_09:85:90 (cisc c0:74:b8 /tes on wire (2424 bit 0, Length 25 mation n frame, Flags: ess LAN : IEEE 002.11]	Broadcast IPv4mcast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bi	12D Deta, SlevBA, File, Flags-pf. 57 Deta, SlevB, File, Flags-pf. Iti) on interface 1	
3295 33.266381 3295 33.266381 3295 33.251464 irame 3358: 303 bb tadiotap Header vi 802.11 radio info IEEE 802.11 Beaco IEEE 802.11 wirel) Nulformed Packet	Raspberr_09:85:90 (cisc c0:74:b8 ytes on wire (2424 bit 0, Length 25 mation n frame, Flags: rss LAN : IEEE 002.11]	Broadcast IPy4ecast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bi	123 Deta, Serba, Frede, Flager, e., F. 25 Deta, Serb, Frede, Flager, e., F. ts) on interface 1	
3295 33.266381 3296 33.251464 frame 3358: 303 by Asdiotap Header vi N02.11 redio info IEEE 002.11 March [Malformed Packet	Raspberr_09:05:96 Cisco c0:74:08 ftes on wire (2424 bit h, Length 25 wation h frame, Flags: ress LAN TETE 002.11]	Broadcast IPy4ecast 12 s), 303 bytes capt 	802.11 802.11 ured (2424 bi	122 Ders, Serbä, Fred, Flager, p., F. 25 Ders, Serb, Fred, Flager, p F. Tsj en interface 1	
3295 33.266381 3296 33.251464 Frame 33553 1083 by Radiotap Header vi NO2.11 radio info IEEE 802.11 March [Nalformed Packet	Raspberr_00:05:90 Cisco c0:74:08 rtes on wire (2424 bit b, Length 25 mation frame, Flags: s LAR : TEEE 002.13]	Broadcast IPv6ncast 12 s), 303 bytes capt 	802.11 802.11 ured (2424 b)	123 Deta, Serba, Frede, Flager, e., F. 29 Deta, Serb, Frede, Flager, e F. ts) on interface 1	
2326 33.266381 3226 33.25164 Frame 3358: 383 header w 902.11 radio info 902.11 radio info 1026 802.11 Beaco IEEE 802.11 Mirel	Raspberr_00:05:06 Cisco.00:24:00 (tes on wire (2424 bit), Length 25 mation s frame, Flags: sss LAN : IEEE 002.11]	Broadcast IPAdecast 12 s), 303 bytes capt 	802.11 802.11 ured (2424 b)	122 Ders, Serbä, Fred, Flager, p., F. 25 Ders, Serb, Fred, Flager, p F. ts) en interface 1	
2205 33.266381 3296 33.251463 3296 33.251464 rame 3358:3483 b tadiotap Header w 002.11 radio infor 1626 802.11 Beacor 1626 802.11 wirel 1/talformed Packet	Raspberr_00:05:9C Cisco c0:74:b0 rtes on wire (2424 bit , Length 25 mation frame, Flags: store LAR : TEEE 002.11]	Broadcest IPvdmczki 12 s), 303 bytes capt	802.11 802.11 ured (2424 b)	12D Ders, SlevBa, Fried, Flager, e., F. 27 Ders, SlevBa, Fried, Flager, e F. ts) on interface 1	
2155 33.266381 1296 33.251464 rame 3358: 383 b kadictap Header W 02.11 radio info CEEE 082.11 Becal in wirele (Malformad Packet	Raspberr_09:05:40 Cisco.02:24:b0 /tes on wire (2424 bit h, Length 22 mation n frame, Flags: rss LAN : IEFE 002.11]	Broadcast IPydencast 12 s), 303 bytes capt	802.11 802.11 ured (2424 bj	122 Ders, Serbä, Fred, Flags-gf. 25 Ders, Serb, Fred, Flags-gf. ts) on interface 1	
00 00 10 00 10 00 01	Raspberr_09:05:40 Cisco.02:74:00 /rts: on wire (2424 bit b, Length 22 mation frame, Flags: rs: LAN : TERE 002.11]	Broadcast DryAdmost 12 s), 303 bytes capt 	802.11 802.11 ured (2424 b)	122 Ders, Serbel, Fried, Flager, d., f. 27 Ders, Serb, Meie, Flager, d., f. ts) on interface 1	
000 00 10 00 10 00 00 10 00 00 00 00 00 29 00 00 00 00 00 00 29 00 00 00	Raspberr_00:05:06 (1soc.07:4:08 /res on wire (2424 bit , length 25 mation frame, Flags: ss LAW 2116 000 00 51 97 08 20 00 53 ss 00 00 00 00	Broadcast IPvekerast 12 s), 303 bytes capt 0 00 00 00 00 0 00 ff ff ff	802.11 802.11 ured (2424 bi	122 Ders, Serbe, Fried, Flager, p., F. 25 Ders, Serb, Fried, Flager, p., F. 1s) on interface 1	
00 00 19 00 17 4 20 00 00 19 00 00 17 4 20 00 00 19 00 19 00 17 00 00 00 19 00 17 00 00 00 19 00 17 00 00 29 09 9 17 17 4 21	Baspber_B0:85:0c Cisco 00:240 bit (rico 00:240 bit (res on wire (2424 bit), Length 32 mation of frame, Flags: res LAN : If the MP2 is a solution : If the MP2 is a solution of the MP2 is a solution is a solution of the MP2 is a solution of the MP2 is a solution of the MP2 is a solution is a soluti	Broadcast IPvekerast 12 s), 303 bytes capt 0 00 00 00 00 0 00 ff ff 0 0 0 ff ff ff	802.11 802.11 ured (2424 b) 	122 Ders, Serbe, Fried, Flager, p., F. 29 Ders, Serb, Fried, Flager, p F. ts) en interface 1	
2255 0.26421 2256 33.254641 2256 33.254643 Frame 3368 383 b Radictap Header V 202.11 radio info TIEE 002.11 select TIEE 002.11	Baspherr, B0:85:6c Cisco d0:240 fres on wire (2424 bit , Length 25 fres on file; Cisco d0:240 fres of file; Cisco d0:240 fres of file; Cisco d0:240 fres of file; Cisco d0:240 file; Cisco d0:240 fil	0 00 00 00 00 00	802.11 802.11 ared (2424 b) 0 0 0 k k k tars(a)	122 Ders, Serbell, Fried, Flager, d., F. 29 Ders, Serbell, Fried, Flager, d., F. ts) en interface 1	
1255 53.265148 1226 53.275148 1226 53.275148 1226 53.275148 1226 53.275148 1226 53.275148 1226 54.27148 1226 54.2714 1226 54.2714 122	Baspherr, BriBick Citos dh740 bit /res on wire (2424 bit y. Length 2 mation ress, Finan, Fings, Fings, we we find on do 51 07 06 2 00 bit as 00 00 00 1 Tite and 100 00 ef 05 56 41 0 at 000 00 46 45 10 2 0 ef 05 56 41 0 at 00 00 00 46 45 10 2 0 ef 05 56 41 0 at 00 00 00 46 45 10 2 0 ef 05 56 40 10 0 ef 05 56 40 10 2 0 ef 05 56 40 00 2 0 ef 05 56 40 10 2 0 ef	Broadcast Drokecast 12 s), 303 bytes capt 0 00 00 00 00 0 00 ff ff 1 50 00 50 00 00 1 500 00 50 00 1 500 00 50 00	0 02.11 802.11 ured (2424 bi k k try(i n4579 den	122 Ders, Serbä, Fried, Flager, e., ., F. 25 Ders, Serb, Fried, Flager, e., ., F. ts) en interface 1	

Fazit

Sie können jetzt ein Paket-Stream direkt zu Wireshark übertragen und es direkt analysieren. Nicht sicher, wohin Sie von hier gehen sollen? Es gibt viele Videos und Artikel online zu erkunden. Was Sie suchen, hängt von den Bedürfnissen Ihrer Situation ab. Du hast das!