

RUCKUS 802.11 PACKET ANALYSIS

Technote

Versie: 1.0
Auteur: Herwin de Rijke
Datum: 29-04-2014

Inhoud

- 1 Inleiding 2
- 2 Configuratie 3
 - 2.1 SSH 3**
 - 2.2 ZD WEBINTERFACE 5**
- 3 Wireshark 6
 - 3.1 WIRESHARK FILTERS..... 8**
- 4 Additionele Informatie11

1 Inleiding

In dit document wordt beschreven hoe u uw Ruckus access points kunt gebruiken voor het analyseren van uw Wi-Fi omgeving op pakket niveau. Door op pakket niveau analyses uit te voeren kunnen problemen makkelijker in kaart gebracht worden en opgelost worden.

De instructies die in dit document gegeven worden gaan uit van een Engelstalige webinterface van de ZoneDirector en eventuele Engelstalige documentatie. Mocht u de webinterface ingesteld hebben op de Nederlandse taal dan zullen de stappen hetzelfde zijn, maar de benaming van de menu's zullen verschillen.

De instructies die in dit document gegeven worden zijn op basis van firmwareversie 9.7.0.0.220. Mocht u een afwijkende firmware versie gebruiken, dan heeft u kans dat sommige functionaliteiten niet aanwezig zijn of anders weergegeven worden.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met de mogelijkheden die het Ruckus systeem biedt voor het troubleshooten van Wi-Fi omgevingen op pakket niveau (middels sniffing).

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel die op pakket niveau troubleshoot werkzaamheden verrichten/willen verrichten binnen Ruckus (managed) WLAN omgevingen.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- OSI Model
- Wireshark
- Ruckus CLI gebruik
- Ruckus GUI gebruik

Om alle stappen goed te kunnen doorlopen heeft u de volgende hardware/software nodig:

- Ruckus ZoneFlex Access Point
- Ruckus ZoneDirector (optioneel)
- Wireshark
- Putty
- Internet Browser

2 Configuratie

In de onderstaande hoofdstukken worden de stappen uitgelegd die doorlopen moeten worden voor het opzetten van een "packet" capture via een Ruckus access point. Het opzetten van een "packet capture" kan op twee manieren. U kunt dit configureren via de webinterface van de ZoneDirector, of u kunt dit configureren via de CLI van het Ruckus access point. Mocht u snel een "packet capture" willen doen, dan raden wij u aan om dit via de ZoneDirector te doen. Wilt graag meer opties configureren dan raden wij u aan om de "packet capture" via de CLI te configureren.

2.1 SSH

Met behulp van een terminal programma zoals Putty kunt u een SSH sessie opzetten met het Ruckus access point. Het is wel belangrijk dat u het juiste IP-adres tot uw beschikking heeft en dat u de correcte inlog gegevens heeft.

Na het inloggen via SSH heeft u twee opties voor het verzamelen van pakketten via het access point. U kunt kiezen voor "**stream mode**" of voor "**save mode**".

Stream mode: via deze optie stuurt het access point de verzamelde pakketten direct naar Wireshark.

Save mode: via deze optie slaat het access point de verzamelde pakketten lokaal op. Daarna kunnen de pakketten via TFTP verstuurd worden.

Voor dat u pakketten kan verzamelen via het access point moet u eerst weten welke interface van het access point u hiervoor kan gebruiken. Sommige access points hebben namelijk meerdere interfaces. Via het onderstaande commando kunt u een overzicht krijgen van de interfaces die aanwezig zijn op het access point:

```
rkscli: get wlanlist
```

De interfaces die geschikt zijn voor het verzamelen van pakketten vallen onder het type "MON". Zoals op de onderstaande screenshot te zien heeft dit access point twee "MON" interfaces. Eén interface voor de 2.4GHz en één interface voor de 5GHz.

```
rkscli: get wlanlist
name      status   type    wlanID  radioID
-----
wlan0     up       AP      wlan0   0
wlan100   down    MON     wlan100 0
wlan32    up       AP      wlan32   1
wlan101   down    MON     wlan101  1
OK
```

Figuur 1: WLAN List

U heeft nu overzicht van de interfaces die u kunt gebruiken voor het verzamelen van pakketten. Nu kunnen we de interface gaan configureren zodat deze in "streaming mode" komt te staan. Om de "packet capture" in "streaming mode" te starten voert u het volgende commando uit:

```
rkscli: set capture <interface> stream
```

```
rkscli: set capture wlan100 stream
Capturing in 20 MHz channel BW
OK
```

Figuur 2: Set Capture

Nu is de interface in streaming mode geconfigureerd. Zoals wij eerder aangaven is het mogelijk om via de CLI extra opties mee te geven. Deze opties kunt u gebruiken om direct bepaalde informatie weg te laten die soms overbodig is in een "packet capture". Via de onderstaande opties kunt u zelf bepalen wat u wel en niet wilt zien:

- -nob : deze optie zorgt ervoor dat u geen beacon informatie terug ziet in uw "packet capture".
- -noc : deze optie zorgt ervoor dat u geen control data terug ziet in uw "packet capture".

De bovenstaande opties kunt u als volgt meegeven tijdens het starten van de "packet capture":

```
rkscli: set capture <interface> stream <optie>
```

Mocht u meerdere opties meegeven dan kunt u dit als volgt doen:

```
rkscli: set capture <interface> stream -nobb
```

Via het bovenstaande commando zullen de beacons en de control data weggelaten worden uit de "packet capture".

Het mee geven van opties is niet verplicht. Verder op in het document wordt uitgelegd hoe u filters kunt maken in Wireshark waarmee u uiteindelijk hetzelfde kunt bereiken.

Als uw access point in standalone modus is geconfigureerd heeft u de mogelijkheid om het access point op een specifiek kanaal te configureren. Het configureren van een kanaal kunt u doen via het volgende commando:

```
rkscli: set channel <interface> <kanaal>
```

Opvragen van het huidige kanaal kunt u doen via het volgende commando:

```
rkscli: get channel <interface>
```

2.2 ZD Webinterface

In dit hoofdstuk wordt uitgelegd hoe een "packet capture" kunt maken via de webinterface van de ZoneDirector. Voor het maken van een "packet capture" navigeert u naar **Administer -> Diagnostics**. Op deze pagina navigeert u naar de categorie **Packet Capture**.

In deze categorie selecteert u op welke frequentie u pakketten wilt verzamelen. U heeft hier een keuze uit de 2.4GHz en de 5GHz. Daarna selecteert u het access point dat u wilt gebruiken voor het verzamelen van de pakketten. Als u het betreffende access point heeft geselecteerd klikt u op **Add to Capture APs**. Nu worden het betreffende access point toegevoegd aan de lijst van access points die pakketten moeten verzamelen.

The screenshot shows the 'Packet Capture' configuration page. At the top, there is a heading 'Packet Capture' and a sub-heading 'Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.' Below this, there are radio buttons for 'Radio' selection: '2.4GHz' (unselected) and '5GHz' (selected). A table titled 'Current Managed APs' has columns for 'MAC Address', 'Device Name', 'Description', and 'Model'. The first row shows a checked checkbox, an empty MAC address field, 'RuckusAP' as the device name, an empty description, and 'zf7363' as the model. Below the table is an 'Add to Capture APs' button and a pagination control '1-1 (1)'. At the bottom, there is a 'Search terms' input field and two radio buttons: 'Include all terms' (selected) and 'Include any of these terms'.

Figuur 3: Packet Capture Configuration

Zodra u het access point heeft toegevoegd kunt u aangegeven in welke modus u pakketten wilt verwerken. U heeft hier de keuze uit **Local Mode** en **Streaming Mode**. In deze technote gebruiken wij de modus **Streaming**.

The screenshot shows the 'Capture APs' configuration page. It features a table with columns 'MAC Address', 'Device Name', 'Description', and 'Model'. The first row has unchecked checkboxes, an empty MAC address field, 'RuckusAP' as the device name, an empty description, and 'zf7363' as the model. Below the table are 'Remove' and 'Remove All' buttons, along with a pagination control '1-1 (1)'. There are two radio buttons for mode selection: 'Local Mode (Capture a limited snapshot on each AP, then Stop and Save to file)' (unselected) and 'Streaming Mode (Use Wireshark's Remote Capture Option to connect to wlan100 or wlan101)' (selected). A 'Filter' input field is present below the 'Local Mode' option, with a note '(Packets to/from one IP or MAC address)'. At the bottom, there is a 'Start' button.

Figuur 4: Local/Streaming Mode

Na het kiezen van de gewenste modus kunt u de "packet capture" starten.

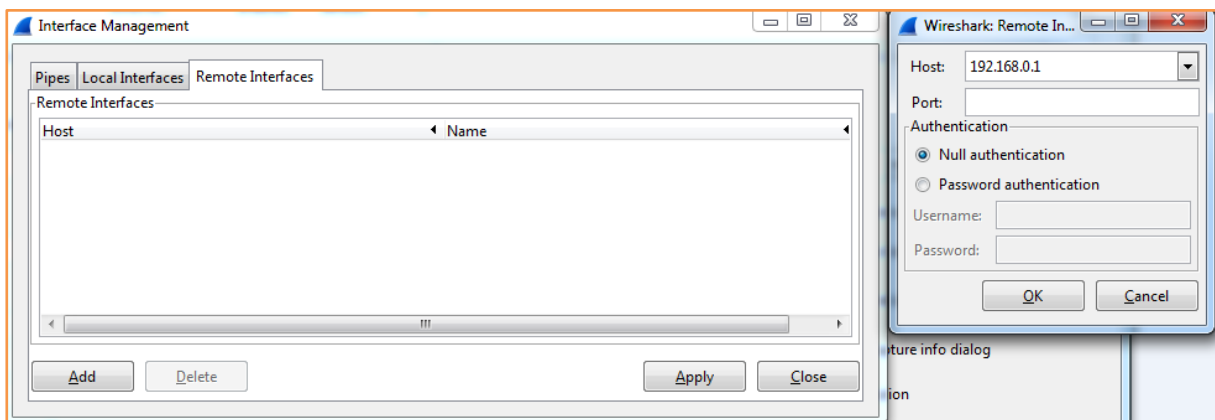
3 Wireshark

Het access points is nu in streaming mode geplaatst en kan uitgelezen worden via Wireshark. Hieronder volgt de configuratie van Wireshark zodat deze de pakketten kan ontvangen van het access point.

Na het opstarten van Wireshark klikt u op "**Capture Options**" of u gebruikt de toetsencombinatie **Ctrl-K** om de "Caputure Options" te openen.

Na het openen van de "Capture Options" klikt u op "**Manage Interfaces**". In dit scherm navigeert u naar "**Remote Interfaces**". Hier voegt u een nieuwe remote interface toe door op "**Add**" te klikken.

In het nieuw geopende scherm geeft u het IP adres op van het access point. De overige instellingen kunt u standaard laten. Na het opgeven van het IP adres van het access point klikt u op "**Ok**".

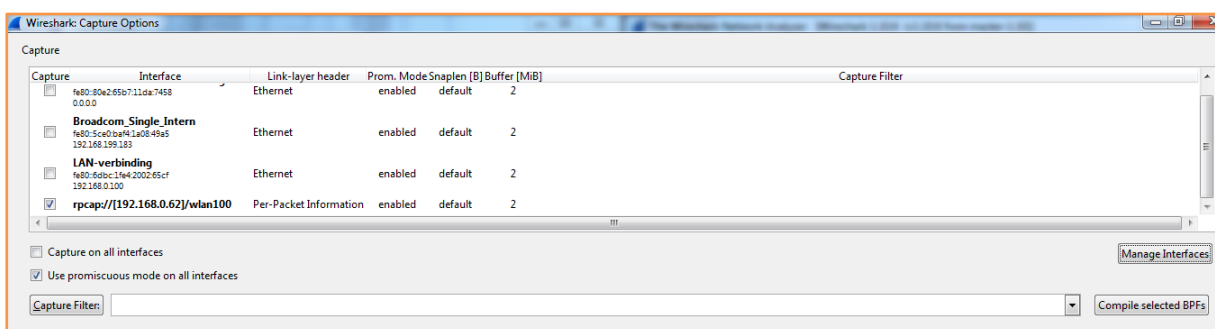


Figuur 5: Remote Interface

Wireshark zal nu een verbinding maken met het access point en de lijst van interfaces weergeven. Achter elke interface zet u het vinkje "hide" aan behalve bij de "MON" interface. In meeste gevallen hebben deze interfaces de volgende naam: **WLAN100** of **WLAN101** (afhankelijk van de geselecteerde frequentie).

Na het selecteren van de interface klikt u op "**Apply**" en daarna op "**Close**".

Na het sluiten van het scherm komt u terug in het eerste scherm genaamd "Capture Options". In dit scherm vindt u de aangemaakte remote interface terug onder de naam "<IP>/WLAN100" of "<IP>/WLAN101". U selecteert de betreffende interface en klikt op "**Start**" om de capture te starten.



Figuur 6: Capture Options

Nu zult u de pakketten van de access points binnen zien komen en kunt u beginnen met het analyseren van de pakketten.

No.	Time	Source	Destination	Protocol	Length	Info
2229	51.3105530	SenaNet_02:e0:a2	Broadcast	802.11	300	Beacon frame, SN=342, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare
2230	51.3629370	Ruckuswi_32:74:98	Broadcast	802.11	291	Beacon frame, SN=1961, FN=0, Flags=.....C, BI=100, SSID=zoneflexR_2.4
2231	51.3678600	Technico_96:31:4b	Broadcast	802.11	305	Beacon frame, SN=1714, FN=0, Flags=.....C, BI=100, SSID=TNCAP96314B
2232	51.4037420	Ruckuswi_0b:a7:b8	Broadcast	802.11	278	Beacon frame, SN=1575, FN=0, Flags=.....C, BI=100, SSID=SCG_22
2233	51.4129440	SenaNet_06:e0:a2	Broadcast	802.11	366	Beacon frame, SN=543, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare
2234	51.4653350	Ruckuswi_32:74:98	Broadcast	802.11	291	Beacon frame, SN=1962, FN=0, Flags=.....C, BI=100, SSID=zoneflexR_2.4
2235	51.4702740	Technico_96:31:4b	Broadcast	802.11	305	Beacon frame, SN=1715, FN=0, Flags=.....C, BI=100, SSID=TNCAP96314B
2236	51.5061390	Ruckuswi_0b:a7:b8	Broadcast	802.11	278	Beacon frame, SN=1576, FN=0, Flags=.....C, BI=100, SSID=SCG_22
2237	51.5153480	SenaNet_06:e0:a2	Broadcast	802.11	366	Beacon frame, SN=544, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare
2238	51.5677470	Ruckuswi_32:74:98	Broadcast	802.11	291	Beacon frame, SN=1963, FN=0, Flags=.....C, BI=100, SSID=zoneflexR_2.4
2239	51.5726560	Technico_96:31:4b	Broadcast	802.11	305	Beacon frame, SN=1716, FN=0, Flags=.....C, BI=100, SSID=TNCAP96314B
2240	51.6094890	Ruckuswi_4b:a7:b8	Broadcast	802.11	268	Beacon frame, SN=2793, FN=0, Flags=.....C, BI=100, SSID=...
2241	51.6177570	SenaNet_06:e0:a2	Broadcast	802.11	366	Beacon frame, SN=545, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare
2242	51.6701360	Ruckuswi_32:74:98	Broadcast	802.11	291	Beacon frame, SN=1964, FN=0, Flags=.....C, BI=100, SSID=zoneflexR_2.4
2243	51.7118890	Ruckuswi_4b:a7:b8	Broadcast	802.11	268	Beacon frame, SN=2794, FN=0, Flags=.....C, BI=100, SSID=...
2244	51.7201440	SenaNet_06:e0:a2	Broadcast	802.11	366	Beacon frame, SN=546, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare
2245	51.7725440	Ruckuswi_32:74:98	Broadcast	802.11	291	Beacon frame, SN=1965, FN=0, Flags=.....C, BI=100, SSID=zoneflexR_2.4
2246	51.7774440	Technico_96:31:4b	Broadcast	802.11	305	Beacon frame, SN=1718, FN=0, Flags=.....C, BI=100, SSID=TNCAP96314B
2247	51.8133350	Ruckuswi_0b:a7:b8	Broadcast	802.11	278	Beacon frame, SN=1579, FN=0, Flags=.....C, BI=100, SSID=SCG_22
2248	51.8225420	SenaNet_06:e0:a2	Broadcast	802.11	366	Beacon frame, SN=547, FN=0, Flags=.....C, BI=100, SSID=EnGenius EnShare

Figuur 7: Packet Capture

3.1 Wireshark Filters

Zoals eerder aangegeven is het ook mogelijk om in Wireshark verschillende filters te maken. Op deze manier kunt u gemakkelijk filteren op de pakketten die u wilt zien, of juist niet wilt zien. Hieronder zullen wij een tabel maken met een aantal filter mogelijkheden.

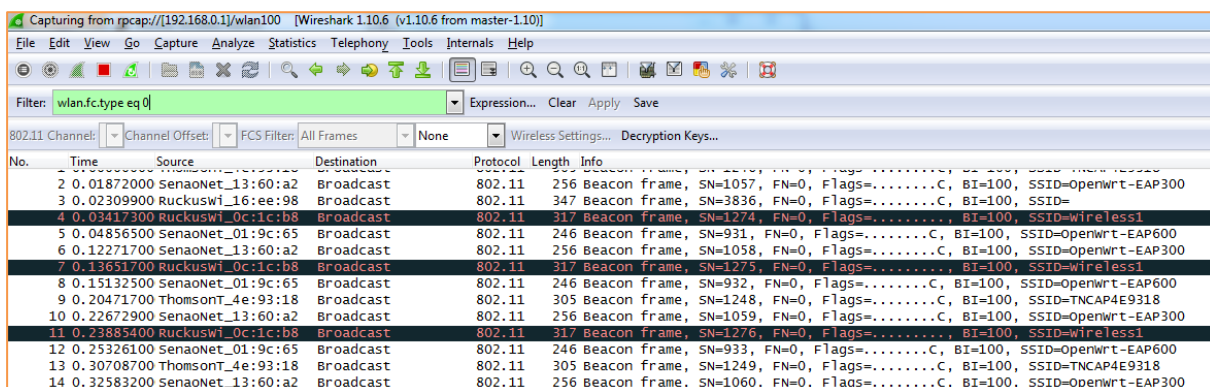
Frame Type	Filter Commando
Management Frames	wlan.fc.type eq 0
Control Frames	wlan.fc.type eq 1
Data Frames	wlan.fc.type eq 2
Association Request	wlan.fc.type_subtype eq 0
Association Response	wlan.fc.type_subtype eq 1
Probe Request	wlan.fc.type_subtype eq 4
Probe Response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12

Hieronder vindt u een screenshot waarin afgebeeld staat waar u de bovenstaande filter opties kan invoeren:



Figuur 8: Filter Command Options

Hieronder geven wij voorbeelden weer van de verschillende filters die in de tabel beschreven zijn:



Figuur 9: Alleen Management Frames

No.	Time	Source	Destination	Protocol	Length	Info
105	1.93718200		Ruckuswi_5b:4d:e8 (802.11)	802.11	98	Acknowledgement, Flags=.....C
109	1.97843700		ThomsonT_4e:93:18 (802.11)	802.11	98	Acknowledgement, Flags=.....C
112	1.98288300		Ruckuswi_0c:1c:b8 (802.11)	802.11	98	Acknowledgement, Flags=.....C
124	2.08757900		Ruckuswi_56:ee:98 (802.11)	802.11	98	Acknowledgement, Flags=.....C
126	2.08916000		Ruckuswi_16:ee:98 (802.11)	802.11	98	Acknowledgement, Flags=.....C
128	2.09164600		Ruckuswi_0c:1c:b8 (802.11)	802.11	98	Acknowledgement, Flags=.....C
132	2.10306900		ThomsonT_4e:93:18 (802.11)	802.11	98	Acknowledgement, Flags=.....C
138	2.14235900		Ruckuswi_96:ee:98 (802.11)	802.11	98	Acknowledgement, Flags=.....C
202	3.17510500		SenaoNet_13:60:a2 (802.11)	802.11	98	Acknowledgement, Flags=.....C
204	3.17903600		SenaoNet_01:9c:65 (802.11)	802.11	98	Acknowledgement, Flags=.....C
205	3.18971200		ThomsonT_4e:93:18 (802.11)	802.11	98	Acknowledgement, Flags=.....C
288	4.50923900		SenaoNet_13:60:a2 (802.11)	802.11	98	Acknowledgement, Flags=.....C
291	4.51438200		Ruckuswi_56:ee:98 (802.11)	802.11	98	Acknowledgement, Flags=.....C

Figur 10: Alleen Control Frames

No.	Time	Source	Destination	Protocol	Length	Info
2077	37.1584820	Technico_85:a0:1e	Broadcast	802.11	164	Data, SN=1272, FN=0, Flags=p...F.C
9200	117.592214	Apple_5b:5d:60	Ruckuswi_57:31:f8	EAPOL	243	Key (Message 2 of 4)
9202	117.596089	Apple_5b:5d:60	Ruckuswi_57:31:f8	EAPOL	221	Key (Message 4 of 4)
16988	220.527855	MurataMa_e1:17:f6	Ruckuswi_17:cd:08	EAPOL	221	Key (Message 4 of 4)
20568	312.678368	169.254.193.148	Broadcast	ARP	148	Gratuitous ARP for 169.254.193.148 (Request)
20582	313.310697	169.254.193.148	igmp.mcast.net	IGMPv3	160	Membership Report / Leave group 239.255.255.250

Figur 11: Alleen Data Frames

No.	Time	Source	Destination	Protocol	Length	Info
9180	117.387501	Apple_5b:5d:60	Ruckuswi_57:31:f8	802.11	248	Association Request, SN=84, FN=0, Flags=.....C, SSID=-DPSK

Figur 12: Alleen Association Request Frames

No.	Time	Source	Destination	Protocol	Length	Info
107	1.97264500	CameoCom_4f:2a:79	Broadcast	802.11	130	Probe Request, SN=980, FN=0, Flags=.....C, SSID=Broadcast
118	2.06836200	CameoCom_4f:2a:79	Broadcast	802.11	130	Probe Request, SN=982, FN=0, Flags=.....C, SSID=Broadcast
120	2.07218100	CameoCom_4f:2a:79	Broadcast	802.11	162	Probe Request, SN=983, FN=0, Flags=.....C, SSID=...
134	2.12729800	CameoCom_4f:2a:79	Broadcast	802.11	130	Probe Request, SN=984, FN=0, Flags=.....C, SSID=Broadcast
199	3.16585900	Ruckuswi_0b:a7:b8	Broadcast	802.11	177	Probe Request, SN=1232, FN=0, Flags=.....C, SSID=SCG_22
200	3.16981400	Ruckuswi_0b:a7:b8	Broadcast	802.11	171	Probe Request, SN=1233, FN=0, Flags=.....C, SSID=Broadcast
283	4.50255900	CameoCom_4f:2a:79	Broadcast	802.11	130	Probe Request, SN=1008, FN=0, Flags=.....C, SSID=Broadcast
289	4.50979700	CameoCom_4f:2a:79	Broadcast	802.11	162	Probe Request, SN=1009, FN=0, Flags=.....C, SSID=...

Figur 13: Alleen Probe Request Frames

No.	Time	Source	Destination	Protocol	Length	Info
93	1.84846500	Senaonet_01:9c:65	CameoCom_4f:2a:79	802.11	240	Probe Response, SN=949, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP600
94	1.85151200	Senaonet_13:60:a2	CameoCom_4f:2a:79	802.11	250	Probe Response, SN=1075, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300
101	1.91461800	Senaonet_13:60:a2	CameoCom_4f:2a:79	802.11	250	Probe Response, SN=1077, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300
102	1.91641700	Senaonet_01:9c:65	CameoCom_4f:2a:79	802.11	240	Probe Response, SN=951, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP600
103	1.91961900	Ruckuswi_1d:6d:88	CameoCom_4f:2a:79	802.11	375	Probe Response, SN=2869, FN=0, Flags=...R...C, BI=100, SSID=Passpoint Demo
104	1.92611100	Ruckuswi_1d:6d:88	CameoCom_4f:2a:79	802.11	375	Probe Response, SN=2869, FN=0, Flags=...R...C, BI=100, SSID=Passpoint Demo
108	1.97813000	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1266, FN=0, Flags=.....C, BI=100, SSID=TNCP4E9318
111	1.98283500	Ruckuswi_0c:1c:b8	CameoCom_4f:2a:79	802.11	311	Probe Response, SN=117, FN=0, Flags=....., BI=100, SSID=Wireless1
119	2.07155600	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1268, FN=0, Flags=.....C, BI=100, SSID=TNCP4E9318
121	2.07528500	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1268, FN=0, Flags=...R...C, BI=100, SSID=TNCP4E9318
125	2.08889700	Ruckuswi_16:ee:98	CameoCom_4f:2a:79	802.11	341	Probe Response, SN=1437, FN=0, Flags=...R...C, BI=100, SSID=
127	2.09159800	Ruckuswi_0c:1c:b8	CameoCom_4f:2a:79	802.11	311	Probe Response, SN=118, FN=0, Flags=....., BI=100, SSID=Wireless1
129	2.09484600	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1268, FN=0, Flags=...R...C, BI=100, SSID=TNCP4E9318
131	2.10275400	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1268, FN=0, Flags=...R...C, BI=100, SSID=TNCP4E9318
133	2.10688700	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1268, FN=0, Flags=...R...C, BI=100, SSID=TNCP4E9318
135	2.13041400	ThomsonT_4e:93:18	CameoCom_4f:2a:79	802.11	431	Probe Response, SN=1269, FN=0, Flags=...R...C, BI=100, SSID=TNCP4E9318
136	2.13221500	Senaonet_13:60:a2	CameoCom_4f:2a:79	802.11	250	Probe Response, SN=1081, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300

Figur 14: Alleen Probe Response Frames

No.	Time	Source	Destination	Protocol	Length	Info
100	1.89070300	Senaonet_01:9c:65	Broadcast	802.11	246	Beacon frame, SN=950, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP600
106	1.96420300	Senaonet_13:60:a2	Broadcast	802.11	256	Beacon frame, SN=1078, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300
110	1.97864800	Ruckuswi_0c:1c:b8	Broadcast	802.11	317	Beacon frame, SN=1293, FN=0, Flags=....., BI=100, SSID=Wireless1
113	1.99305000	Senaonet_01:9c:65	Broadcast	802.11	246	Beacon frame, SN=953, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP600
114	1.99558100	Ruckuswi_56:ee:98	Broadcast	802.11	350	Beacon frame, SN=3854, FN=0, Flags=.....C, BI=100, SSID= -DPSK
115	1.99678200	Ruckuswi_96:ee:98	Broadcast	802.11	330	Beacon frame, SN=3811, FN=0, Flags=.....C, BI=100, SSID= Gasten
116	2.04788000	ThomsonT_4e:93:18	Broadcast	802.11	305	Beacon frame, SN=1267, FN=0, Flags=.....C, BI=100, SSID=TNCP4E9318
117	2.06679100	Senaonet_13:60:a2	Broadcast	802.11	256	Beacon frame, SN=1080, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300
122	2.07653900	Ruckuswi_16:ee:98	Broadcast	802.11	347	Beacon frame, SN=3856, FN=0, Flags=.....C, BI=100, SSID=
123	2.08099300	Ruckuswi_0c:1c:b8	Broadcast	802.11	317	Beacon frame, SN=1294, FN=0, Flags=....., BI=100, SSID=Wireless1
130	2.09661900	Senaonet_01:9c:65	Broadcast	802.11	246	Beacon frame, SN=954, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP600
142	2.16902600	Senaonet_13:60:a2	Broadcast	802.11	256	Beacon frame, SN=1082, FN=0, Flags=.....C, BI=100, SSID=Openwrt-EAP300
144	2.17916600	Ruckuswi_56:ee:98	Broadcast	802.11	350	Beacon frame, SN=3856, FN=0, Flags=.....C, BI=100, SSID= -DPSK
145	2.18041600	Ruckuswi_96:ee:98	Broadcast	802.11	330	Beacon frame, SN=3813, FN=0, Flags=.....C, BI=100, SSID= Gasten

Figur 15: Alleen Beacon Frames

No.	Time	Source	Destination	Protocol	Length	Info
9176	117.384984	Apple_5b:5d:60	Ruckuswi_57:31:f8	802.11	129	Authentication, SN=83, FN=0, Flags=.....C
9178	117.385675	Ruckuswi_57:31:f8	Apple_5b:5d:60	802.11	118	Authentication, SN=0, FN=0, Flags=.....C
13227	155.183428	Ruckuswi_57:cd:08	Apple_a8:da:93	802.11	118	Authentication, SN=0, FN=0, Flags=.....C
16557	215.140970	169.254.193.148	Ruckuswi_97:cd:08	802.11	118	Authentication, SN=26, FN=0, Flags=.....C
16985	220.504282	MurataMa_e1:17:f6	Ruckuswi_17:cd:08	802.11	129	Authentication, SN=75, FN=0, Flags=.....C
16986	220.504944	Ruckuswi_17:cd:08	MurataMa_e1:17:f6	802.11	118	Authentication, SN=0, FN=0, Flags=.....C

Figur 16: Alleen Authentication Frames

4 Additionele Informatie

Hieronder vindt u additionele informatie over de Ruckus CLI en het gebruik van Wireshark.

Wireshark Website:

[Wireshark](#)

Wireshark – Display Filters:

[Wireshark Display Filters](#)

Wireshark – Capture Filters:

[Wireshark Capture Filters](#)

Ruckus AP CLI Guide:

[Ruckus AP CLI Guide](#)