RUCKUS 802.11 PACKET ANALYSIS

Technote (English translation)

Versie:	1.0
Auteur:	Herwin de Rijke
Datum:	20-11-2019

Index

1 Introduction

This document describes how to use your Ruckus Wireless access point to capture 802.11 WLAN packages. You can use these captures to analyse Wi-Fi issues, to better understand why issues occur.
The purpose of this document is therefore to explain in a simple way how you can make packet captures using the Ruckus access points.

To capture packets using your Ruckus wireless access points, at least you need the following equipment:

- Ruckus access point
- Ruckus ZoneDirector (optional, not required)
- Device running Wireshark

Basic knowledge of the ZoneDirector is required to configure this option on ZoneDirector. Knowing the difference between the different tabs and where the different configuration options are located. In addition, it is good to be comfortable with the CLI of a Ruckus access point. Some knowledge about the use of Wireshark is also good to have.

The instructions given in this document are based on an English-language web interface from the ZoneDirector. If you have set the web interface to another language, the steps will be the same, but the names of the menus will differ.

The instructions given in this document are based on firmware version 9.7.0.0.220. If you have a lower firmware, then you have the chance that some functionalities are not yet available. If you have a higher firmware version, then the steps will be almost the same.

2 Configuration

The chapters below explain the steps that must be followed to set up a "packet" capture via a Ruckus access point. There are two ways to set up a "packet capture". You can configure this via the ZoneDirector's web interface, or you can configure this via the CLI of the Ruckus access point. If you want to do a “packet capture” quickly, we recommend you do this via the ZoneDirector. If you would like to configure more options, we recommend that you configure the "packet capture" via the CLI.

2.1 SSH

With the help of a terminal program such as Putty you can set up an SSH session with the Ruckus access point. It is important that you have the correct IP address and that you have the correct login details.

After successful login using SSH there are two option to capture packets using your Ruckus Wireless access point. You can choose between “**stream mode”** or **“save mode”.**

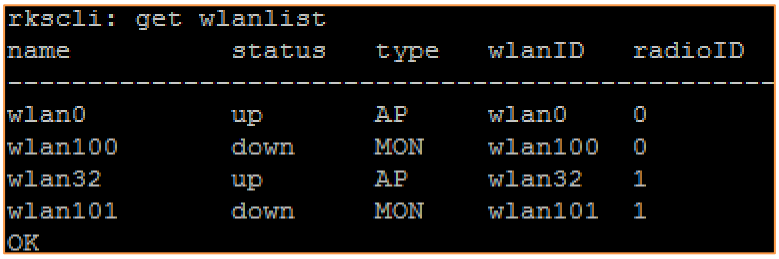
Stream mode: using this option the access point sends the collected packages directly to Wireshark.

Save mode: using this option the access point stores the collected packages locally. The packages can then be sent using TFTP.

Before you can collect packages via the access point you must first know which interface of the access point you can use for this. Some access points have multiple interfaces. With the command below you can get an overview of the interfaces that are present at the access point:

```
rkscli: get wlanlist
```

Only interfaces indicated as type “**MON”** can be used for capturing packets. As you can see on the screenshot below, for the used type of access point only two interfaces can be used to capture packets. One interface for 2,4GHz and one interface for 5GHz.

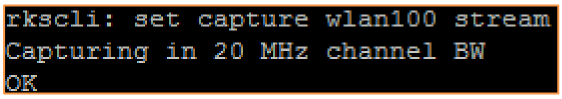


```
rkscli: get wlanlist
name          status   type    wlanID    radioID
-------------------------------------------------
wlan0         up       AP      wlan0     0
wlan100       down     MON     wlan100   0
wlan32        up       AP      wlan32    1
wlan101       down     MON     wlan101   1
OK
```

Figure 1*: WLAN List*

You now have an overview of the interfaces that you can use to collect packages. Now we can start configuring the interface so that it will be in "streaming mode". To start the "packet capture" in "streaming mode", execute the following command:

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



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

Figure 2*: Set Capture*

Now the interface is configured in streaming mode. As we indicated earlier, it is possible to provide extra options via the CLI. You can use these options to immediately exclude certain information that is not needed in a "packet capture". Via the options below you can determine yourself what you do and do not want to see:

- -nob : This option will hide beacon information.
- -noc : This option will hide control data.

You can set the option described when setting the interface to capture packets using command below:

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

If you would like to use more option you can set it as described below,

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

when using this command, both beacons and control data will be excluded from the packet capture.

Using options is not mandatory and mostly used when saving to disk and would like to save diskspace used. Further on in the document it is explained how you can make filters in Wireshark.

If your access point is configured in standalone mode, you can also set the radio to a specific channel. You can configure the channel using the command below:

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

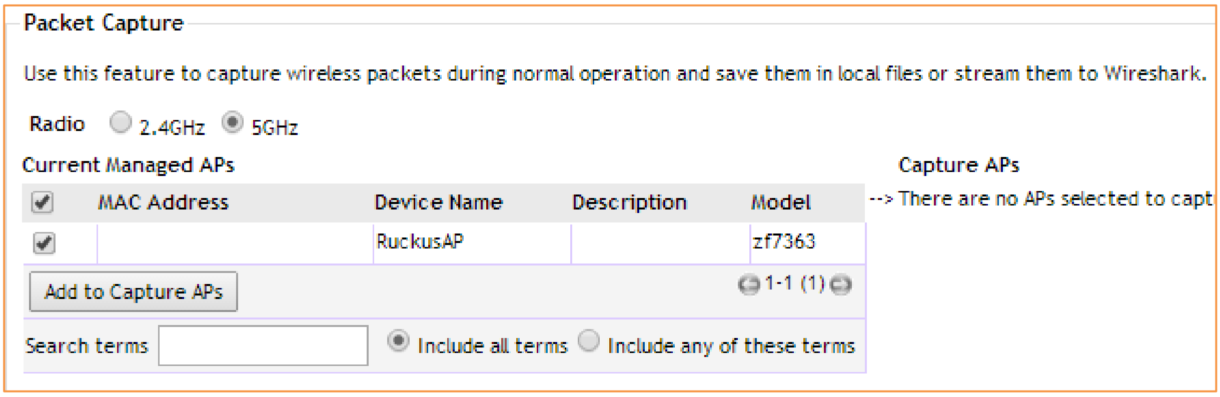
You can request the current used channel using the command below:

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

2.2 ZD Web interface

This chapter explains how to make a "**packet capture**" using the ZoneDirector's web interface. To make a "**packet capture**", navigate to **Administer -> Diagnostics**. On this page you navigate to the Packet Capture category.

In this category you select on which frequency you want to collect packages. You have a choice between 2.4 GHz and 5 GHz. Then select the access point that you want to use for collecting the packages. If you have selected the correct access point, click **Add to Capture APs**. Now the selected access point will be displayed in the list of access points that will capture packets.



Packet Capture

Use this feature to capture wireless packets during normal operation and save them in local files or stream them to Wireshark.

Radio ○ 2.4GHz ● 5GHz

Current Managed APs

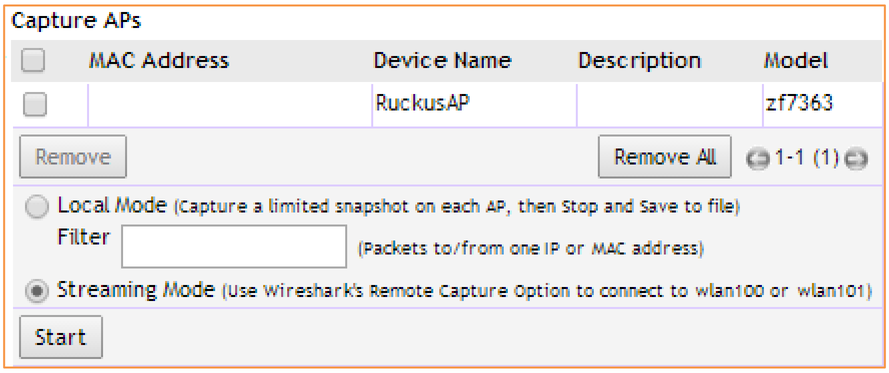
☑	MAC Address	Device Name	Description	Model
☑		RuckusAP		zf7363

Capture APs

--> There are no APs selected to capt

Figure 3: *Packet Capture Configuration*

Once you have added the access point you can set in which mode you want to capture packets. You can choose between **Local Mode** and **Streaming Mode** here. In this technote we used the Streaming mode option.



Capture APs

□	MAC Address	Device Name	Description	Model
□		RuckusAP		zf7363

○ Local Mode (Capture a limited snapshot on each AP, then Stop and Save to file)

Filter (Packets to/from one IP or MAC address)

● Streaming Mode (Use Wireshark's Remote Capture Option to connect to wlan100 or wlan101)

Figure 4: *Local/Streaming Mode*

After setting the correct option and mode you can start the “packet capture” using the **start** button.

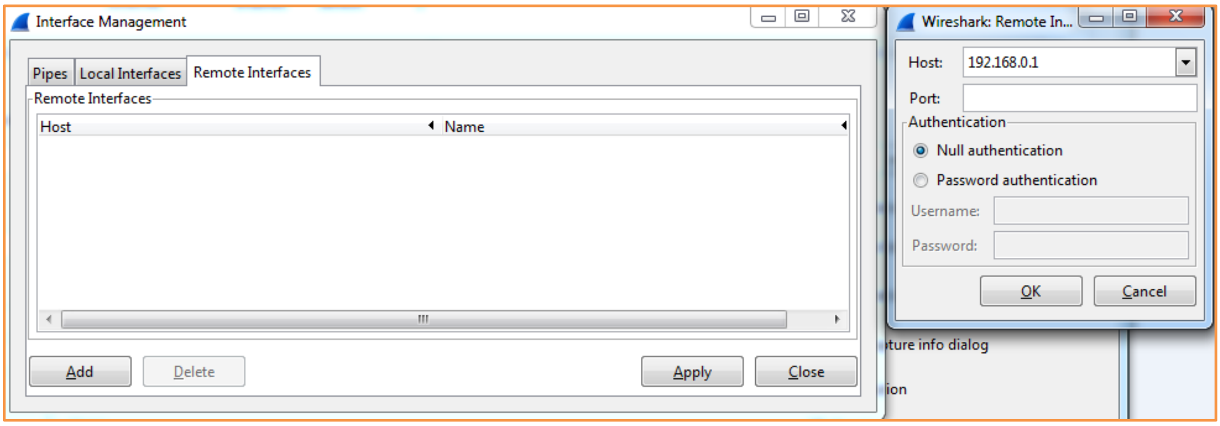
3 Wireshark

Once the access point is set to capture packets in streaming mode, the stream can be opened using Wireshark. In this chapter we will describe how to configure Wireshark to receive packets from the access point.

After starting Wireshark click "**Capture Options**" or use the key combination **Ctrl-K** to open "Capture Options".

After starting "**Capture Options**" click on "**Manage Interfaces**". In this screen navigate to "**Remote Interfaces**". Here you can add a remote interface by clicking "**Add**".

In the screen opened you must enter the IP address of the access point. All other displayed settings can be as default. After setting the IP address you must click "**OK**".



Interface Management

Pipes | Local Interfaces | Remote Interfaces

Remote Interfaces

Host	Name

Add | Delete | Apply | Close

Wireshark: Remote In...

Host: 192.168.0.1

Port:

Authentication

● Null authentication

○ Password authentication

Username:

Password:

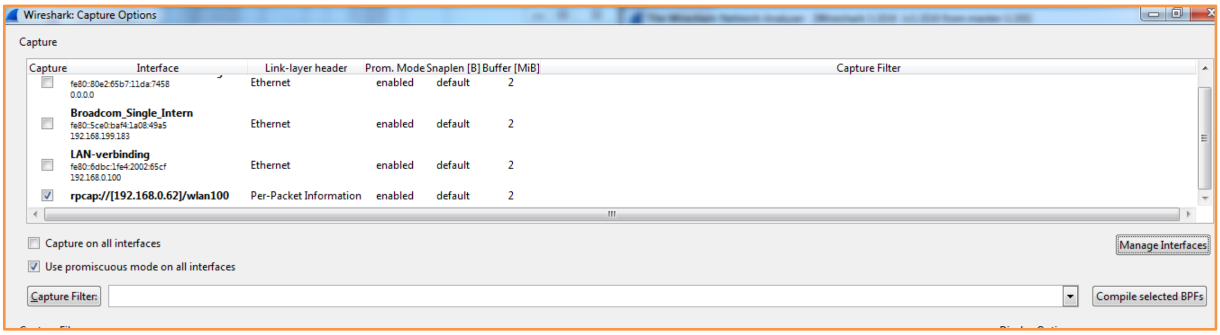
OK | Cancel

Figure 5: *Remote Interface*

Wireshark will now connect to the access point and display the list of available interfaces. Behind each interface you enable the "hide" check mark except for the "MON" interface. In most cases, these interfaces have the following name: WLAN100 or WLAN101 (depending on the selected frequency).

After selecting the interface, you must click "**Apply**" and then "**Close**".

After you closed the screen you will return to the first screen named "Capture Options". In this screen you will find the remote interface by "<IP>/WLAN100" or "<IP>/WLAN101". You can start the capture by clicking "**Start**".



Wireshark: Capture Options

Capture

Capture	Interface	Link-layer header	Prom. Mode	Snaplen [B]	Buffer [MiB]	Capture Filter
☐	fe80::80e2:65b7:11da:7458 0.0.0.0	Ethernet	enabled	default	2	
☐	**Broadcom_Single_Intern** fe80::5ce0:baf4:1a08:49a5 192.168.199.183	Ethernet	enabled	default	2	
☐	**LAN-verbinding** fe80::6dbc:1fe4:2002:65cf 192.168.0.100	Ethernet	enabled	default	2	
☑	**rpcap://[192.168.0.62]/wlan100**	Per-Packet Information	enabled	default	2	

☐ Capture on all interfaces

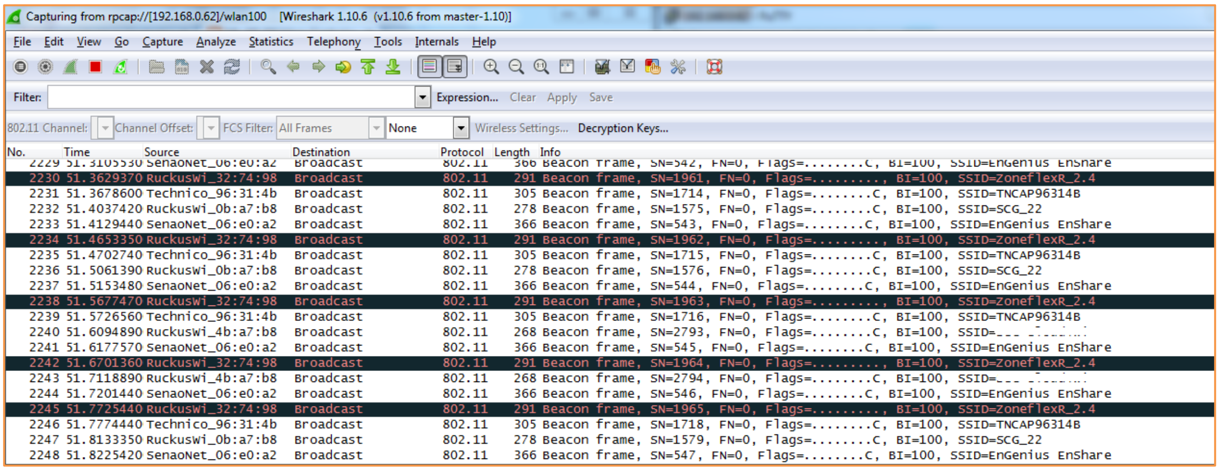
☑ Use promiscuous mode on all interfaces

Manage Interfaces

Capture Filter: | Compile selected BPFs

Figure 6: *Capture Options*

After correctly completing the steps described in the chapters “configuration” and “Wireshark” you will see packets in the main capture window, and you are ready to analyse the packets.


Capturing from rpcap://[192.168.0.62]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
802.11 Channel:
Channel Offset:
FCS Filter: All Frames
None
Wireless Settings...
Decryption Keys...

```
No.   Time       Source               Destination  Protocol Length Info
 2229 51.3105530 SenaoNet_06:e0:a2    Broadcast    802.11   366 Beacon frame, SN=542, 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=........., 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 SenaoNet_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=........., 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 SenaoNet_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=........., 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=[redacted]
 2241 51.6177570 SenaoNet_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=........., 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=[redacted]
 2244 51.7201440 SenaoNet_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=........., 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 SenaoNet_06:e0:a2    Broadcast    802.11   366 Beacon frame, SN=547, FN=0, Flags=........C, BI=100, SSID=EnGenius EnShare
```

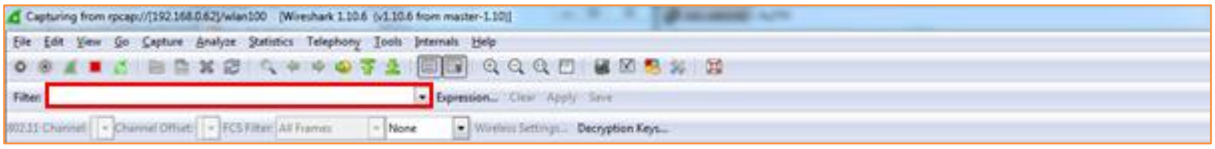
Figure 7: *Packet Capture*

3.1 Wireshark Filters

As indicated earlier, it is also possible to make different display filters in Wireshark. In this way you can easily filter on the packages that you want to see or do not want to see. Below we will make a table with several filter options.

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

Enter the filter in the section marked red below:



Capturing from rpcap://[192.168.0.62]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

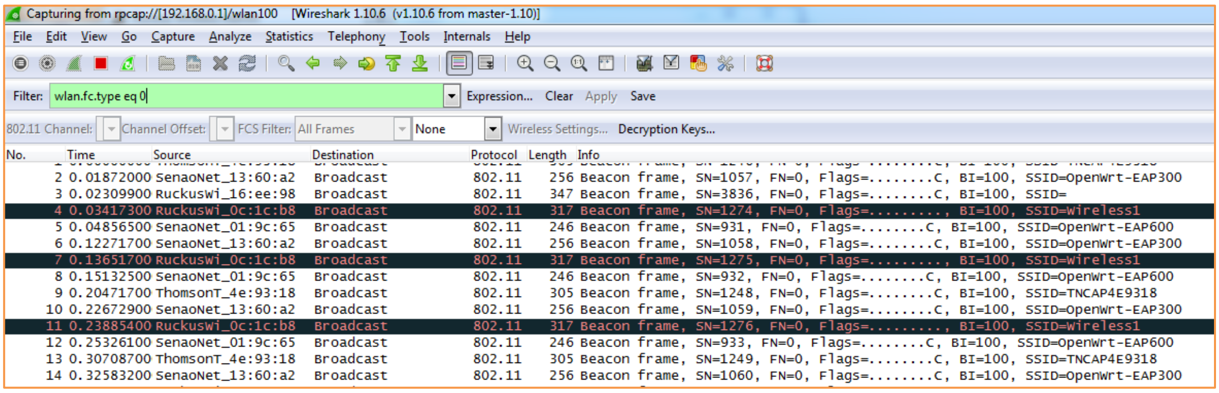
Filter:

802.11 Channel: Channel Offset: FCS Filter: All Frames None

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

Figure 8: *Filter Command Options*

Below some examples of some filters used in Wireshark and their results.



Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

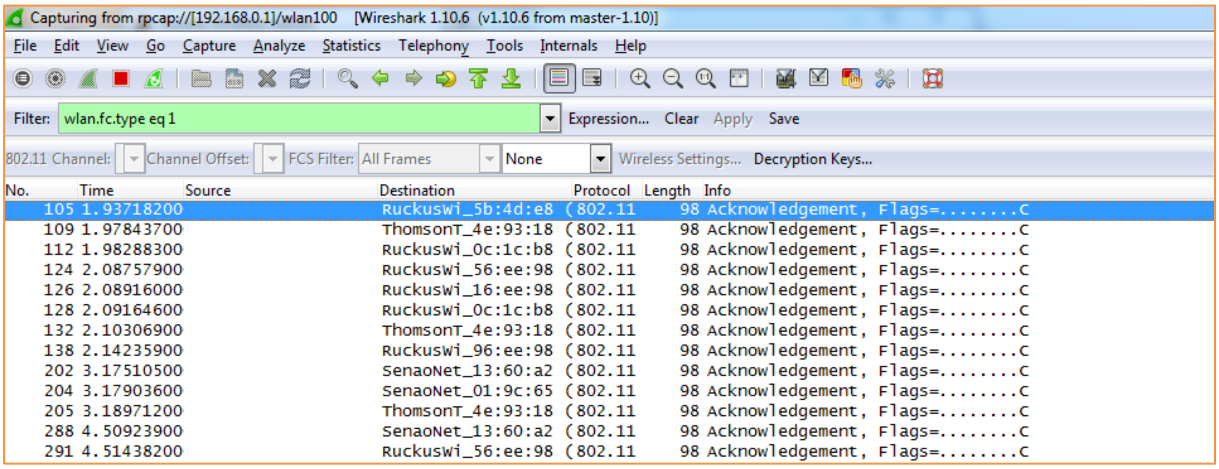
Filter: wlan.fc.type eq 0

802.11 Channel: Channel Offset: FCS Filter: All Frames None

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

```
No.    Time       Source              Destination   Protocol Length Info
     2 0.01872000 SenaoNet_13:60:a2   Broadcast     802.11   256 Beacon frame, SN=1057, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP300
     3 0.02309900 RuckusWi_16:ee:98   Broadcast     802.11   347 Beacon frame, SN=3836, FN=0, Flags=........C, BI=100, SSID=
     4 0.03417300 RuckusWi_0c:1c:b8   Broadcast     802.11   317 Beacon frame, SN=1274, FN=0, Flags=........., BI=100, SSID=wireless1
     5 0.04856500 SenaoNet_01:9c:65   Broadcast     802.11   246 Beacon frame, SN=931, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP600
     6 0.12271700 SenaoNet_13:60:a2   Broadcast     802.11   256 Beacon frame, SN=1058, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP300
     7 0.13651700 RuckusWi_0c:1c:b8   Broadcast     802.11   317 Beacon frame, SN=1275, FN=0, Flags=........., BI=100, SSID=wireless1
     8 0.15132500 SenaoNet_01:9c:65   Broadcast     802.11   246 Beacon frame, SN=932, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP600
     9 0.20471700 ThomsonT_4e:93:18   Broadcast     802.11   305 Beacon frame, SN=1248, FN=0, Flags=........C, BI=100, SSID=TNCAP4E9318
    10 0.22672900 SenaoNet_13:60:a2   Broadcast     802.11   256 Beacon frame, SN=1059, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP300
    11 0.23885400 RuckusWi_0c:1c:b8   Broadcast     802.11   317 Beacon frame, SN=1276, FN=0, Flags=........., BI=100, SSID=wireless1
    12 0.25326100 SenaoNet_01:9c:65   Broadcast     802.11   246 Beacon frame, SN=933, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP600
    13 0.30708700 ThomsonT_4e:93:18   Broadcast     802.11   305 Beacon frame, SN=1249, FN=0, Flags=........C, BI=100, SSID=TNCAP4E9318
    14 0.32583200 SenaoNet_13:60:a2   Broadcast     802.11   256 Beacon frame, SN=1060, FN=0, Flags=........C, BI=100, SSID=OpenWrt-EAP300
```

Figure 9: only display management frames

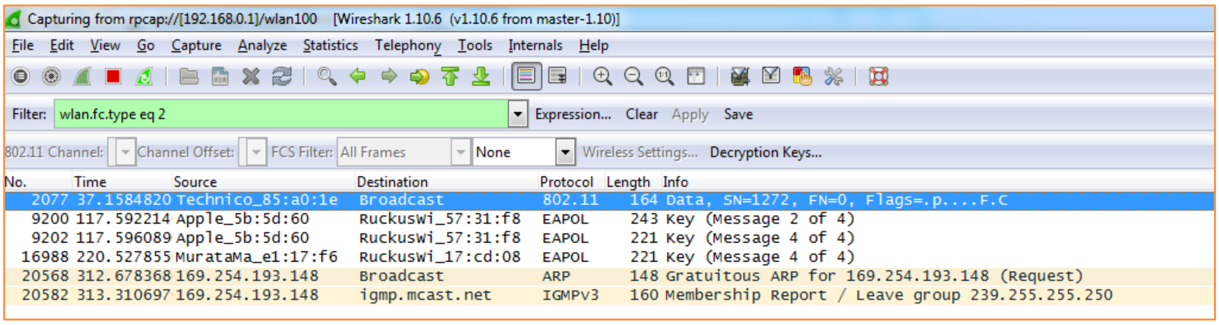

Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type eq 1

Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

```
No.   Time          Source          Destination        Protocol  Length  Info
  105 1.93718200                    RuckusWi_5b:4d:e8 (802.11      98 Acknowledgement, Flags=........C
  109 1.97843700                    ThomsonT_4e:93:18 (802.11      98 Acknowledgement, Flags=........C
  112 1.98288300                    RuckusWi_0c:1c:b8 (802.11      98 Acknowledgement, Flags=........C
  124 2.08757900                    RuckusWi_56:ee:98 (802.11      98 Acknowledgement, Flags=........C
  126 2.08916000                    RuckusWi_16:ee:98 (802.11      98 Acknowledgement, Flags=........C
  128 2.09164600                    RuckusWi_0c:1c:b8 (802.11      98 Acknowledgement, Flags=........C
  132 2.10306900                    ThomsonT_4e:93:18 (802.11      98 Acknowledgement, Flags=........C
  138 2.14235900                    RuckusWi_96:ee:98 (802.11      98 Acknowledgement, Flags=........C
  202 3.17510500                    SenaoNet_13:60:a2 (802.11      98 Acknowledgement, Flags=........C
  204 3.17903600                    SenaoNet_01:9c:65 (802.11      98 Acknowledgement, Flags=........C
  205 3.18971200                    ThomsonT_4e:93:18 (802.11      98 Acknowledgement, Flags=........C
  288 4.50923900                    SenaoNet_13:60:a2 (802.11      98 Acknowledgement, Flags=........C
  291 4.51438200                    RuckusWi_56:ee:98 (802.11      98 Acknowledgement, Flags=........C
```

Figure 10: Only display control frames

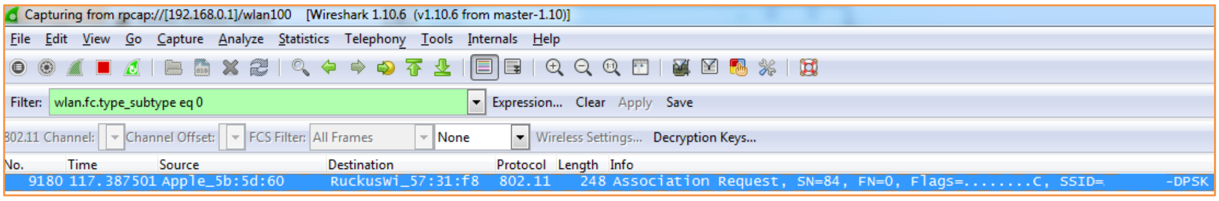

Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type eq 2

Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

```
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
```

Figure 11: only display Data frames

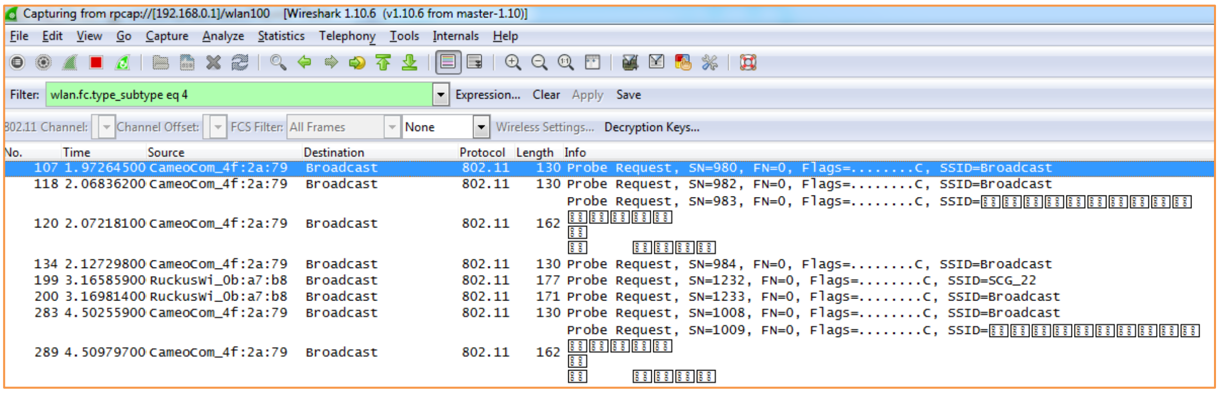

Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type_subtype eq 0

Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

```
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
```

Figure 12: only display Association Request frames

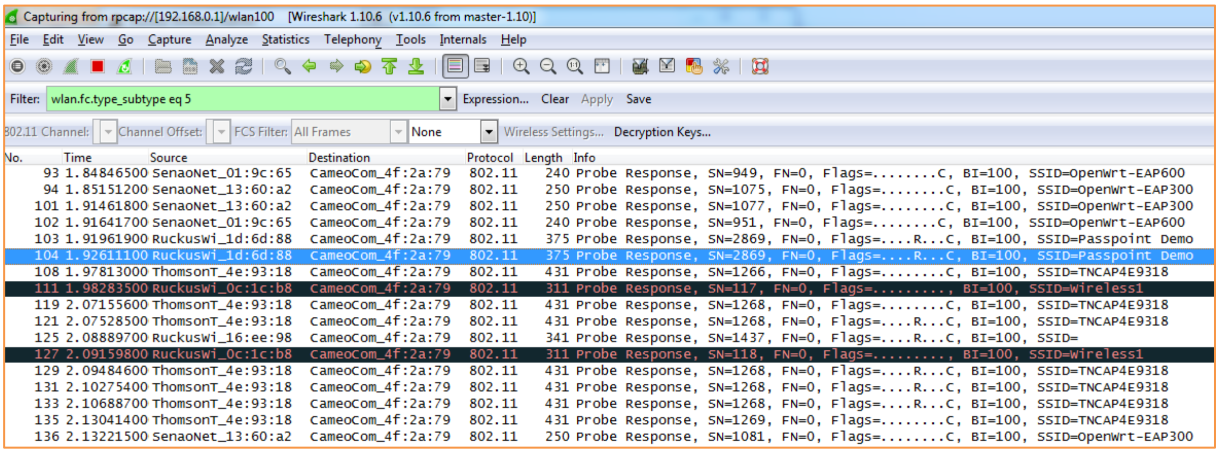

Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: wlan.fc.type_subtype eq 4

Expression... Clear Apply Save
802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

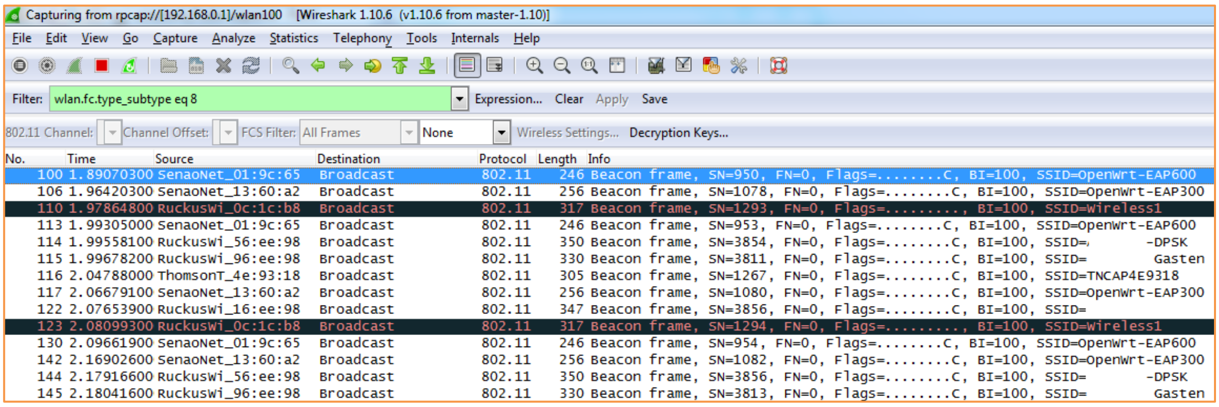
```
No.   Time        Source             Destination  Protocol  Length  Info
  107 1.97264500  CameoCom_4f:2a:79  Broadcast    802.11     130 Probe Request, SN=980, FN=0, Flags=........C, SSID=Broadcast
  118 2.06836200  CameoCom_4f:2a:79  Broadcast    802.11     130 Probe Request, SN=982, FN=0, Flags=........C, SSID=Broadcast
                                                                 Probe Request, SN=983, FN=0, Flags=........C, SSID=□□□□□□□□□□
  120 2.07218100  CameoCom_4f:2a:79  Broadcast    802.11     162 □□□□□
                                                                 □
                                                                 □     □□□□
  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
                                                                 Probe Request, SN=1009, FN=0, Flags=........C, SSID=□□□□□□□□□□
  289 4.50979700  CameoCom_4f:2a:79  Broadcast    802.11     162 □□□□□
                                                                 □
                                                                 □     □□□□
```

Figure 13: Only display Probe Request frames


Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

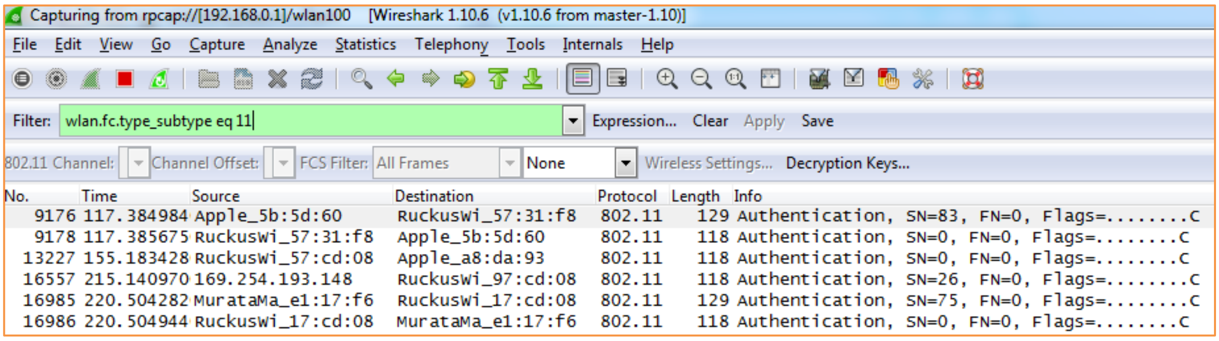
```
Filter: wlan.fc.type_subtype eq 5
802.11 Channel:   Channel Offset:   FCS Filter: All Frames   None
No.   Time       Source               Destination         Protocol  Length  Info
   93 1.84846500 SenaoNet_01:9c:65    CameoCom_4f:2a:79   802.11    240 Probe Response, SN=949, FN=0, Flags=........C, 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=TNCAP4E9318
  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=TNCAP4E9318
  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=TNCAP4E9318
  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=TNCAP4E9318
  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=TNCAP4E9318
  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=TNCAP4E9318
  135 2.13041400 ThomsonT_4e:93:18    CameoCom_4f:2a:79   802.11    431 Probe Response, SN=1269, FN=0, Flags=........C, BI=100, SSID=TNCAP4E9318
  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
```

Figure 14: only display probe response frames


Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

```
Filter: wlan.fc.type_subtype eq 8
802.11 Channel:   Channel Offset:   FCS Filter: All Frames   None
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=TNCAP4E9318
  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
```

Figure 15: only display Beacon frames


Capturing from rpcap://[192.168.0.1]/wlan100 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Wireless Settings... Decryption Keys...

```
Filter: wlan.fc.type_subtype eq 11
802.11 Channel:   Channel Offset:   FCS Filter: All Frames   None
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
```

Figure 16: only display Authentication frames

4 Additional Information

Below you will find some information about using Ruckus CLI and Wireshark.

Wireshark Website:
Wireshark

Wireshark – Display Filters:
Wireshark Display Filters

Wireshark – Capture Filters:
Wireshark Capture Filters

Ruckus AP CLI Guide:
Ruckus AP CLI Guide