AN1287: RS9116N Wi-Fi Roaming Application Note

Version 0.4

10/21/2020

Table of Contents

1 Abstract

This Document helps the user with the Bgscan and Roaming features supported by the RS9116N driver. It also describes the procedure to enable Bgscan and Roaming using RS9116N driver.

2 Introduction

RS9116N Open Source Driver (OSD) is a SoftMAC driver which interacts with the Linux wireless MAC layer, i.e., MAC80211. The driver is a group of simple and efficient kernel modules which currently supports RS9116N chipsets and it can be ported to any embedded platform in-addition to x86 platform.

Background scanning helps to get the information about surrounding AP's in the vicinity of STA. This information helps the STA to roam between the APs. The document explains the steps to enable Background scanning & Roaming with OSD driver in STA mode.

3 Terminology (Acronyms/Abbreviations)

1. NL80211 - nl80211 is the new 802.11 netlink interface public header.
2. Bgscan - Background scanning
3. AP - Access Point
4. STA - Station DUT
5. EVB - Evaluation Board
6. EVK – Evaluation Kit

4 Requirements

- RS9116N EVK – Refer to the sample product link of our module given below:
    - https://www.silabs.com/wireless/wi-fi/rs9116-wi-fi-transceiver-modules
- WLAN driver – RS9116N n-Link Open Source Driver. Available at below link.
    - https://www.silabs.com/wireless/wi-fi/rs9116-wi-fi-transceiver-modules
- Linux PC (kernel version v2.6.38 – v5.3)
- At least two Access points

5 Background Scanning

In the earlier days, the data transfer between the STA and AP is limited to particular range based upon type of standard. If the STA crosses beyond the range, there may be a loss of data and immediate connection to another nearest AP is not possible because there is no background scanning. In order to avoid the loss of data / reduce data loss during the STA is in mode of mobility, background scan was implemented.

Functional Description: The mobility of station makes the signal strength weak and it may sometimes leads to disconnection from AP. In order to avoid data loss, STA must have nearby network report to connect to better AP prior to disconnect from existing AP. This is called BG SCANNING.

Scanning: There are two types of scanning.

1. Active scanning
2. Passive scanning

Active scanning will be done in normal channels and passive scanning should be done in DFS channels of 5GHz due to meet regulatory rules.

Note:

Background scan is implemented in firmware and is controlled by the driver with an IOCTL called "set_bgscan_params". The arguments that are given in the command line, starts the scanning procedure and station may scan available APs before they make decision to roam.

6 Roaming

Roaming, in the context of an 802.11 wireless network, is the process of a client moving an established Wi-Fi network association from one access point to another access point within the same Extended Service Set (ESS) without losing connectivity.

Driver will monitor the RSSI of connected AP and Changes the connection to AP, if connected AP's RSSI crosses the subjected threshold values.

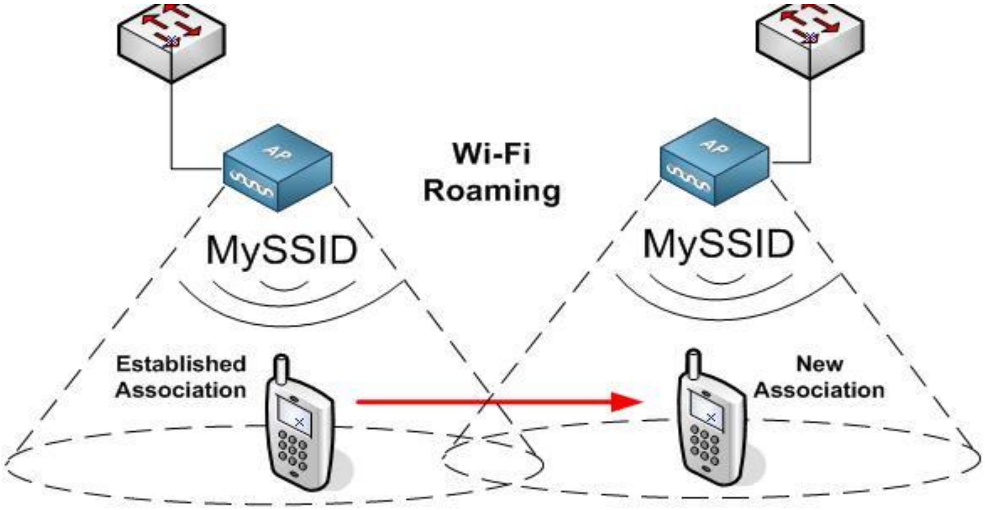


Figure 1: Roaming

It is the legacy roaming in which no roam time optimization method is used.

This process consists of 3 phases:

1. **Scanning**: As the device moves away from the AP to which it is connected and the RSSI (Received Signal Strength Indicator) values begin to drop below certain levels, the client device sends out probe packets to identify AP alternatives. Upon discovery of accessible APs, the device then selects its next AP based on certain criteria, as defined by the device itself.
2. **Authentication**: During this phase, the client device sends an authentication request to the new AP and waits for a response from the AP to approve or reject the request.
3. **Re-association**: Upon approval by the new AP, the client sends a re-association request and waits for a response. Once the re-association is complete, client device connects to new AP.

7 Configuration Steps Required for Roaming

7.1 Configuration Parameters in .config File

Download the supplicant from https://w1.fi/wpa_supplicant/

Extract the supplicant using the following command.

```
# tar xvf wpa_supplicant-2.6.tar.gz
# cd wpa_supplicant-2.6/wpa_supplicant
# cp defconfig .config
```

Make sure the following parameters are enabled in the supplicant configuration file (.config)

```
CONFIG_DRIVER_NL80211=y
CONFIG_BGSCAN_SIMPLE=y
NL80211_CMD_ROAM=y
CONFIG_LIBNL20=y
CONFIG_LIBNL32=y
CONFIG_WPS2=y
CONFIG_BGSCAN=y
```

Save the configuration file and exit.

Compile the supplicant using "make" command in the following path.

```
# cd wpa_supplicant-2.6/wpa_supplicant
# make clean
# make
```

After successful compilation the supplicant executable will be found in the same path. Copy the supplicant executable to the driver release folder.

```
# cp wpa_supplicant RS9116.NB0.NL.GNU.LNX.OSD.a.b.c.d/rsi.
```

7.1.1 Access Point Configuration:

All the AP’s using for Roaming must have below similar configuration’s.

1. Same SSID
2. Same Password
3. Same Security mode
4. Same band(2.4GHz/5GHz)
5. Same Channel width(20Mhz/40Mhz)

7.2 Configuring Bgscan Parameters in sta_settings.conf File

Background scanning and roaming can be verified using wpa_supplicant. It is recommended to use supplicant version greater than 2.6 for better performance in roaming.

To use this facility, user needs to ensure the flag **CONFIG_BGSCAN_SIMPLE** is enabled in the supplicant build configuration file (.config).

> **Note:**
>
> If user does not require bgscan he has to disable bgscan in the supplicant config and should not include above configurations in the wpa_supplicant.conf file. This cannot be done if the user is connected through network manager.

To enable Bgscan and Roaming add **'bgscan="simple: 10:-45:100" '** in the network block of sta_settings.conf file. Wpa_supplicant behavior for background scanning can be specified by configuring a bgscan module. These modules are responsible for requesting background scans for the purpose of roaming within an ESS (i.e., within a single network block with all the APs using the same SSID).

The bgscan parameter uses the below format:

"<bgscan module name> :< module parameters>"

```
bgscan="simple :< short bgscan interval in seconds> :< signal strength threshold>:  <long interval>"
```

This line should be present either inside a network block or outside of all network blocks based on the requirement.

Bgscan parameter has three configurable parameters.

1. short bgscan interval,

2. signal strength threshold,

3. long bgscan interval in seconds.

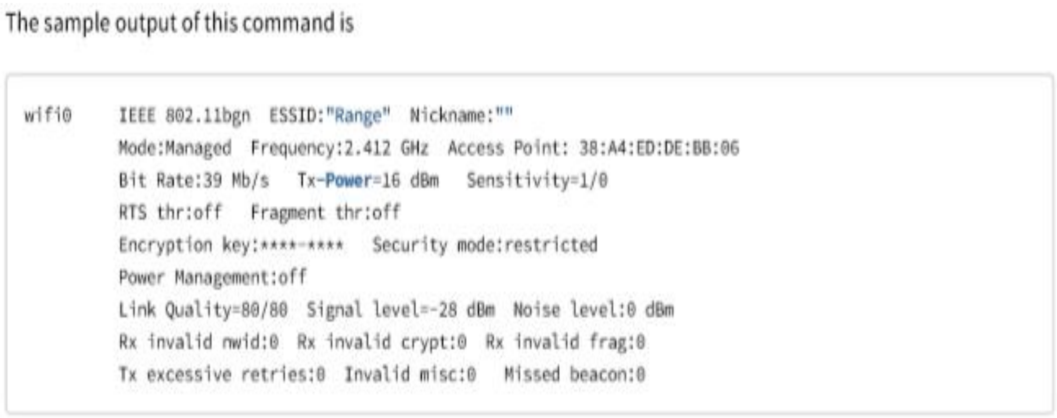
If the signal strength of connected AP is stronger/better than "signal strength threshold" supplicant will perform a bgscan for every "long interval" and if the signal is worse, it will perform a scan every "short bgscan interval".

Please see the example network block:

```
network={
ssid= "Range"
key_mgmt= WPA-PSK
psk=<passphrase specified in the Access Point>
proto=WPA2
pairwise=CCMP
group =CCMP
#bgscan="simple:<short bgscan interval in seconds>:<signal strength
threshold>:<long interval in seconds>"
bgscan="simple:10:-45:100"
priority=1
}
```

After configuring the network block, follow the below steps:

1) Start the RS9116N module in STA mode and connect to AP [For starting RS9116N module in STA mode, please refer section 4. Installing the nlink Driver in RS9116N Open Source Driver Technical Reference Manual
2) Run the supplicant to connect the STA to nearest AP.
   ./wpa_supplicant -i < Interface_name> -D nl80211 -c sta_settings.conf -dddt > log1 &
3) Check the connection of the STA with "**iwconfig**" or " **./wpa_cli -i < interface> status**".
   Example: ./wpa_cli -i wifi0 status



The sample output of this command is

```
wifi0     IEEE 802.11bgn  ESSID:"Range"  Nickname:""
          Mode:Managed  Frequency:2.412 GHz  Access Point: 38:A4:ED:DE:BB:06
          Bit Rate:39 Mb/s   Tx-Power=16 dBm   Sensitivity=1/0
          RTS thr:off   Fragment thr:off
          Encryption key:****-****   Security mode:restricted
          Power Management:off
          Link Quality=80/80  Signal level=-28 dBm  Noise level:0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

7.3 Configuring background scan parameters through debugfs

For Bgscan, f/w requires some of the parameters to be configured. Default values are configured if user doesn't configure them through debugfs. Below commands are used to configure bgscan params.

1) To verify the bgscan status and parameters

```
# cat /sys/kernel/debug/phy<X>/bgscan
```

2) To enable background scan and configure its parameters from debugfs:

```
# echo 1 10 10 20 20 100 1 3 1 6 11 > /sys/kernel/debug/phy<X>/bgscan
```

The input parameters of the background scan command are explained below.

- **<background_enable>:** To enable the background scan.
- **<bgscan_threshold>:** The Background scan threshold is referred to as the RSSI Upper Threshold. At every background scan interval, the n-Link® module decides whether to initiate or not to initiate a background scan based on the connected Access Point's RSSI. The module initiates a background scan if the RSSI of the connected Access Point is below this threshold. The input value should be the absolute value in dBm.
- **<rssi_tolerance_threshold>:** If the difference between the current RSSI value of the connected Access Point and the RSSI value of the Access Point from the previous background scan is greater than the RSSI Tolerance Threshold, then the module performs a background scan. Assigning a large value to this field will eliminate this method of triggering background scans.
- **<periodicity>:** This parameter specifies the interval between the background scans. The unit of this field is seconds. Setting the value of this field as 0 will disable background scans.

- **<active_scan_duration>:** This parameter determines the duration of the active scan in each channel during the Background scan process. The recommended value for this parameter is 20ms for quicker Background scan operation and uninterrupted throughput. The maximum allowed value for this parameter is 255ms.
- **<passive_scan_duration>:** This parameter determines the duration of the passive scan in each DFS channel. If an active scan is enabled in a DFS channel and a beacon or probe response is received during that period, the module converts the passive scan into an active scan and waits through the duration specified by the <active_scan_duration> parameter. During a passive scan, if any beacon is received in a channel, then the recommended value for this parameter will be 100ms. The active scan in DFS channel can be enabled through Background scan probe request. Active scanning will be performed only if channel switch IE (Information Element) is not present in the received beacon or probe response packets. The maximum allowed value for this parameter is 255ms.
- **<two_probe_enable>:** If this feature is enabled, the Client sends two probe requests to the Access Point. This is useful when scanning is carried out in channels with high traffic. The valid values are

  a. 0 – Disable
  b. 1 – Enable

- **<num_of_bgscan_channels>:** Specifies the number of Background scan channels. The n-Link® module supports up to 24 channels.
- **<channels_to_scan>:** The list of channels in which Background scan has to be performed.

The command initializes background scanning in the driver, for the channels specified. It also takes signal strength threshold and periodicity values specified as input. These will decide at what signal strength threshold to start bgscan and at what interval those need to be repeated, irrespective of signal strength threshold

3) To disable background scan which is happening in channels provided through debugfs.

```
# echo 0 > /sys/kernel/debug/phy<X>/bgscan
```

4) For checking the list of bgscan channels configured to device use below command. This will display the list of bgscan channels configured to device with DFS indication also.

```
# cat /sys/kernel/debug/phy<X>/bgscan
```

The command initializes background scanning in the driver, for the channels specified. It also takes signal strength threshold and periodicity values specified as input. These will decide at what signal strength threshold to start bgscan and at what interval those need to be repeated, irrespective of signal strength threshold.

7.4 Configure Connection Quality Monitoring (cqm) rssi and hysteresis using iw Command

To know more about iw tool, refer to the section Configuration Using CFG80211.

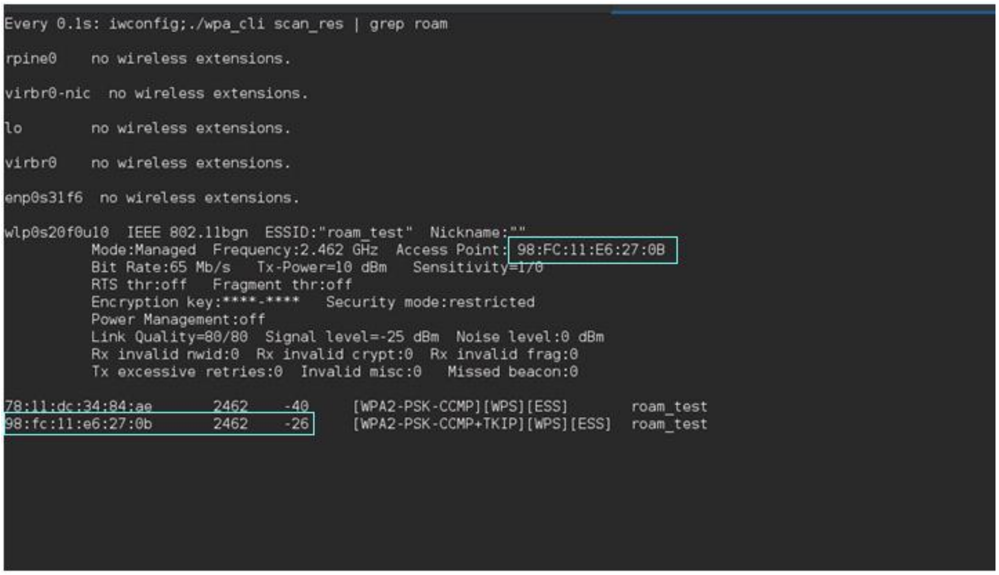
```
$iw dev <devname> cqm rssi <threshold|off> [<hysteresis>]
Set connection quality monitor RSSI threshold.
Example:
$iw dev wlan0 cqm rssi -45 4
```

To know more about Background Scan and Set Parameters configuration, refer to the section **Background Scan & Roaming** in RS9116N Open Source Driver Technical Reference Manual.

Note: Use only open source supplicant for roaming using NL80211. Latest supplicant is recommended (wpa_supplicant 2.6)

7.5 Illustration of Roaming

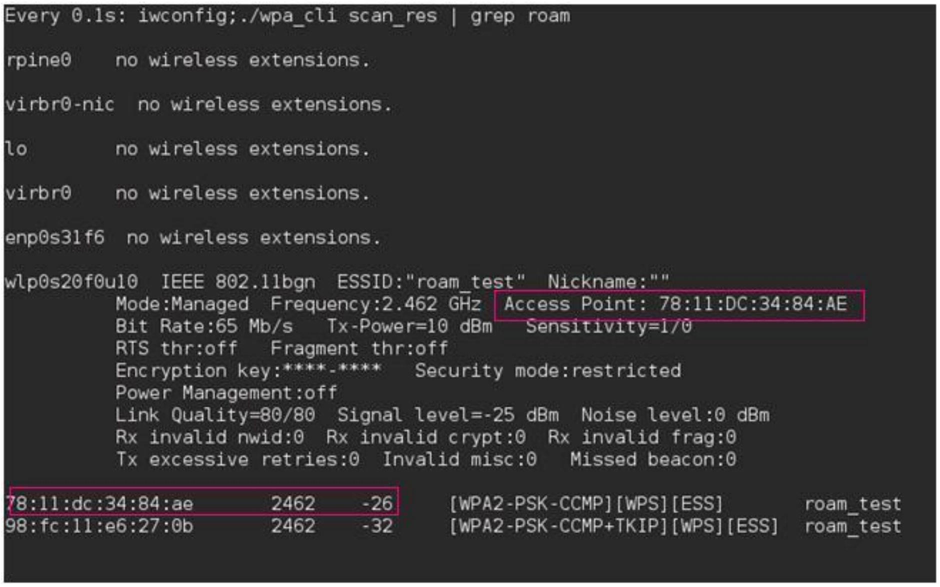
Let us say, two AP's are configured with same SSID, security and password. After executing the bgscan IOCTL, STA is connected to one AP which has better signal strength (In the figure below: AP (98:FC:11:E6:27:0B) with signal strength -26dBm).



```
Every 0.1s: iwconfig;./wpa_cli scan_res | grep roam

rpine0    no wireless extensions.

virbr0-nic  no wireless extensions.

lo        no wireless extensions.

virbr0    no wireless extensions.

enp0s31f6  no wireless extensions.

wlp0s20f0u10  IEEE 802.11bgn  ESSID:"roam_test"  Nickname:""
          Mode:Managed  Frequency:2.462 GHz  Access Point: 98:FC:11:E6:27:0B
          Bit Rate:65 Mb/s   Tx-Power=10 dBm   Sensitivity=1/0
          RTS thr:off   Fragment thr:off
          Encryption key:****-****   Security mode:restricted
          Power Management:off
          Link Quality=80/80  Signal level=-25 dBm  Noise level:0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

78:11:dc:34:84:ae       2462    -40     [WPA2-PSK-CCMP][WPS][ESS]       roam_test
98:fc:11:e6:27:0b       2462    -26     [WPA2-PSK-CCMP+TKIP][WPS][ESS]  roam_test
```

Figure 2: Connected to AP-1

When the signal strength of the AP is weaker, STA will try to connect to another AP which has better signal strength (In the figure below: AP (78:11:dc:34:84:ae) with signal strength -26dBm).



```
Every 0.1s: iwconfig;./wpa_cli scan_res | grep roam

rpine0    no wireless extensions.

virbr0-nic  no wireless extensions.

lo        no wireless extensions.

virbr0    no wireless extensions.

enp0s31f6  no wireless extensions.

wlp0s20f0u10  IEEE 802.11bgn  ESSID:"roam_test"  Nickname:""
          Mode:Managed  Frequency:2.462 GHz  Access Point: 78:11:DC:34:84:AE
          Bit Rate:65 Mb/s   Tx-Power=10 dBm   Sensitivity=1/0
          RTS thr:off   Fragment thr:off
          Encryption key:****-****   Security mode:restricted
          Power Management:off
          Link Quality=80/80  Signal level=-25 dBm  Noise level:0 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

78:11:dc:34:84:ae       2462    -26     [WPA2-PSK-CCMP][WPS][ESS]       roam_test
98:fc:11:e6:27:0b       2462    -32     [WPA2-PSK-CCMP+TKIP][WPS][ESS]  roam_test
```

Figure 3: Connected to AP-2 with Better Signal Strength

8 Test Procedure

8.1 Block Diagram

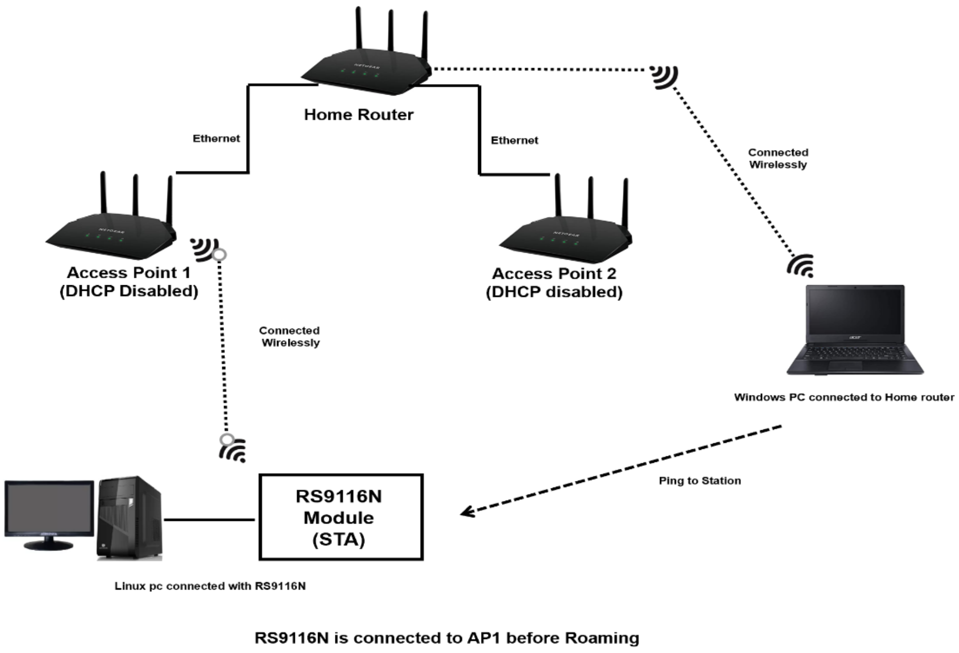

Home Router
Ethernet
Ethernet
Connected Wirelessly
Access Point 1 (DHCP Disabled)
Access Point 2 (DHCP disabled)
Connected Wirelessly
Windows PC connected to Home router
Ping to Station
RS9116N Module (STA)
Linux pc connected with RS9116N
RS9116N is connected to AP1 before Roaming

Figure 4: Before Roaming (STA Connected to AP1)

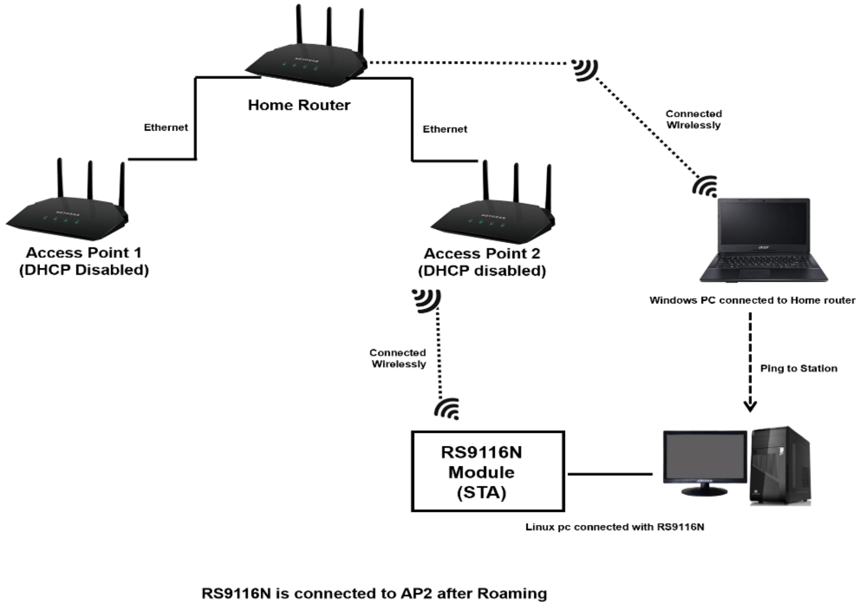

Home Router
Ethernet
Ethernet
Connected Wirelessly
Access Point 1 (DHCP Disabled)
Access Point 2 (DHCP disabled)
Windows PC connected to Home router
Connected Wirelessly
Ping to Station
RS9116N Module (STA)
Linux pc connected with RS9116N
RS9116N is connected to AP2 after Roaming

Figure 5: After Roaming (STA Connected to AP2)

8.2 Description

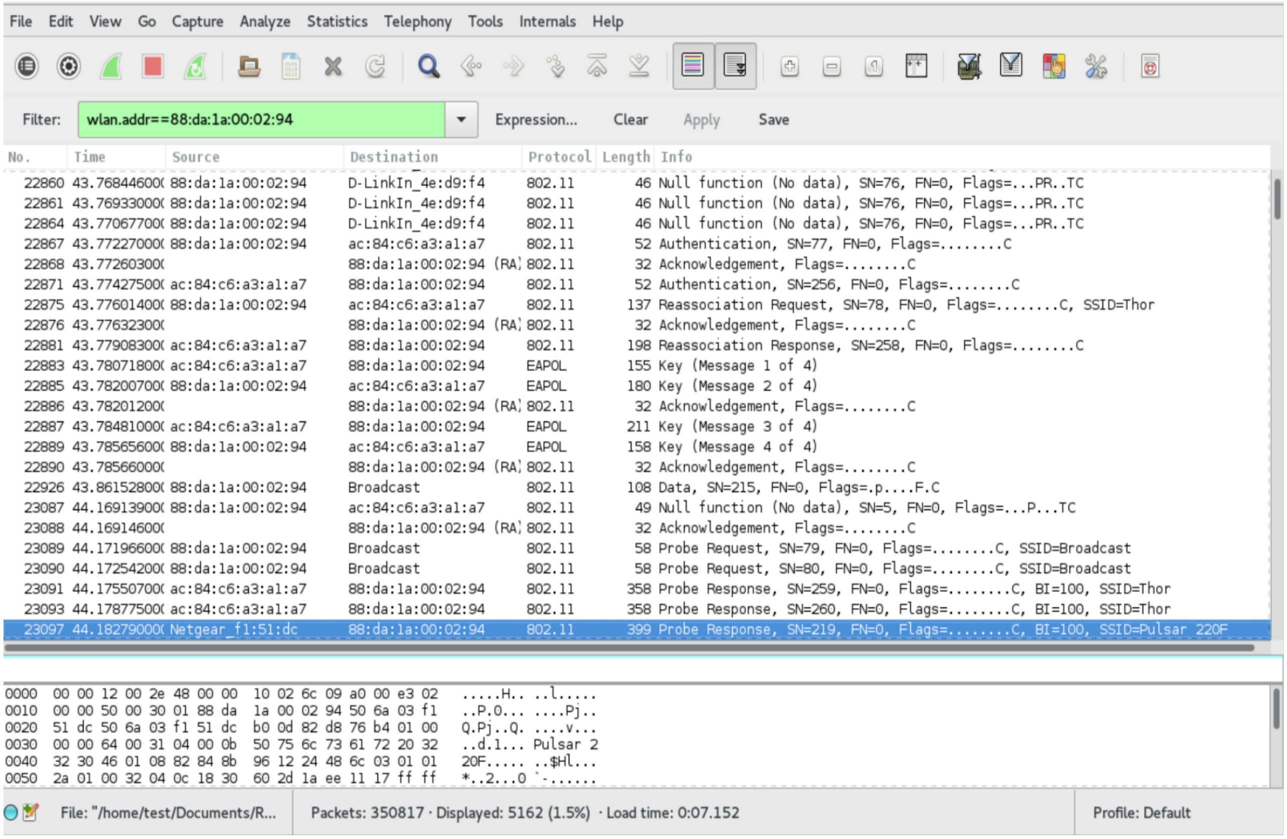
This test procedure is used to calculate the switchover time of Roaming.

8.3 Procedure

1. Connect the both Access points, AP1 and AP2 to Home router with ethernet cables.
2. Disable the DHCP server in both AP1 and AP2.
3. Configure the both access points with same SSID's, Password, Security, Band and channel width.
4. Now, connect RS9116N module to Linux PC and configure it in STA(client) mode.
5. Establish the connection between STA and AP1, configure the background scan as mentioned in the above section (Follow the procedure for Roaming mentioned in the section 7 Configuration steps required for roaming:).
6. Obtain IP address to STA, by dhclient command and start ping from Windows PC connected wirelessly to home router to STA.
7. When STA switches from AP1 to AP2, roaming is happened and the ping will continue with some timeouts.
8. Now, calculate the switchover time from AP1 to AP2.

8.4 Results

- Switchover time from AP1 to AP2 is ~100ms.



Filter: wlan.addr==88:da:1a:00:02:94

```
No.   Time        Source             Destination            Protocol Length Info
22860 43.76844600( 88:da:1a:00:02:94 D-LinkIn_4e:d9:f4      802.11    46 Null function (No data), SN=76, FN=0, Flags=...PR..TC
22861 43.76933000( 88:da:1a:00:02:94 D-LinkIn_4e:d9:f4      802.11    46 Null function (No data), SN=76, FN=0, Flags=...PR..TC
22864 43.77067700( 88:da:1a:00:02:94 D-LinkIn_4e:d9:f4      802.11    46 Null function (No data), SN=76, FN=0, Flags=...PR..TC
22867 43.77227000( 88:da:1a:00:02:94 ac:84:c6:a3:a1:a7      802.11    52 Authentication, SN=77, FN=0, Flags=........C
22868 43.77260300(                   88:da:1a:00:02:94 (RA) 802.11    32 Acknowledgement, Flags=........C
22871 43.77427500( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      802.11    52 Authentication, SN=256, FN=0, Flags=........C
22875 43.77601400( 88:da:1a:00:02:94 ac:84:c6:a3:a1:a7      802.11   137 Reassociation Request, SN=78, FN=0, Flags=........C, SSID=Thor
22876 43.77632300(                   88:da:1a:00:02:94 (RA) 802.11    32 Acknowledgement, Flags=........C
22881 43.77908300( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      802.11   198 Reassociation Response, SN=258, FN=0, Flags=........C
22883 43.78071800( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      EAPOL    155 Key (Message 1 of 4)
22885 43.78200700( 88:da:1a:00:02:94 ac:84:c6:a3:a1:a7      EAPOL    180 Key (Message 2 of 4)
22886 43.78201200(                   88:da:1a:00:02:94 (RA) 802.11    32 Acknowledgement, Flags=........C
22887 43.78481000( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      EAPOL    211 Key (Message 3 of 4)
22889 43.78565600( 88:da:1a:00:02:94 ac:84:c6:a3:a1:a7      EAPOL    158 Key (Message 4 of 4)
22890 43.78566000(                   88:da:1a:00:02:94 (RA) 802.11    32 Acknowledgement, Flags=........C
22926 43.86152800( 88:da:1a:00:02:94 Broadcast              802.11   108 Data, SN=215, FN=0, Flags=.p....F.C
23087 44.16913900( 88:da:1a:00:02:94 ac:84:c6:a3:a1:a7      802.11    49 Null function (No data), SN=5, FN=0, Flags=...P...TC
23088 44.16914600(                   88:da:1a:00:02:94 (RA) 802.11    32 Acknowledgement, Flags=........C
23089 44.17196600( 88:da:1a:00:02:94 Broadcast              802.11    58 Probe Request, SN=79, FN=0, Flags=........C, SSID=Broadcast
23090 44.17254200( 88:da:1a:00:02:94 Broadcast              802.11    58 Probe Request, SN=80, FN=0, Flags=........C, SSID=Broadcast
23091 44.17550700( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      802.11   358 Probe Response, SN=259, FN=0, Flags=........C, BI=100, SSID=Thor
23093 44.17877500( ac:84:c6:a3:a1:a7 88:da:1a:00:02:94      802.11   358 Probe Response, SN=260, FN=0, Flags=........C, BI=100, SSID=Thor
23097 44.18279000( Netgear_f1:51:dc  88:da:1a:00:02:94      802.11   399 Probe Response, SN=219, FN=0, Flags=........C, BI=100, SSID=Pulsar 220F
```

```
0000  00 00 12 00 2e 48 00 00  10 02 6c 09 a0 00 e3 02   .....H.. ..l.....
0010  00 00 50 00 30 01 88 da  1a 00 02 94 50 6a 03 f1   ..P.0... ....Pj..
0020  51 dc 50 6a 03 f1 51 dc  b0 0d 82 d8 76 b4 01 00   Q.Pj..Q. ....v...
0030  00 00 64 00 31 04 00 0b  50 75 6c 73 61 72 20 32   ..d.1... Pulsar 2
0040  32 30 46 01 08 82 84 8b  96 12 24 48 6c 03 01 01   20F..... ..$Hl...
0050  2a 01 00 32 04 0c 18 30  60 2d 1a ee 11 17 ff ff   *..2...0 `-......
```

File: "/home/test/Documents/R... | Packets: 350817 · Displayed: 5162 (1.5%) · Load time: 0:07.152 | Profile: Default

9 Troubleshooting

- Make sure you are enabling bgscan in STA mode only.
- Make sure all the AP's SSID, password, band, channel width and security mode should be same in case of roaming.
- The parameters given in the example command are only for reference. You can change the values based on your application.
- Make sure of the COEX and DRIVER modes for corresponding STA mode that you intended to use.
    - COEX MODE =1 - Wi-Fi ALONE
    - COEX MODE =5 - Wi-Fi STA+BT classic
    - COEX MODE =9 - Wi-Fi STA+BT LE
    - COEX MODE =13 - Wi-Fi STA+BT classic +BT LE (All possible modes for STA)
  - Make sure, "CFG80211 and MAC 80211" and "Bluetooth subsystem" is enabled in the Target platform's kernel. Please refer our RS9116N Open Source Driver Technical Reference Manual.
  - Use latest wpa supplicant version 2.6 or above.

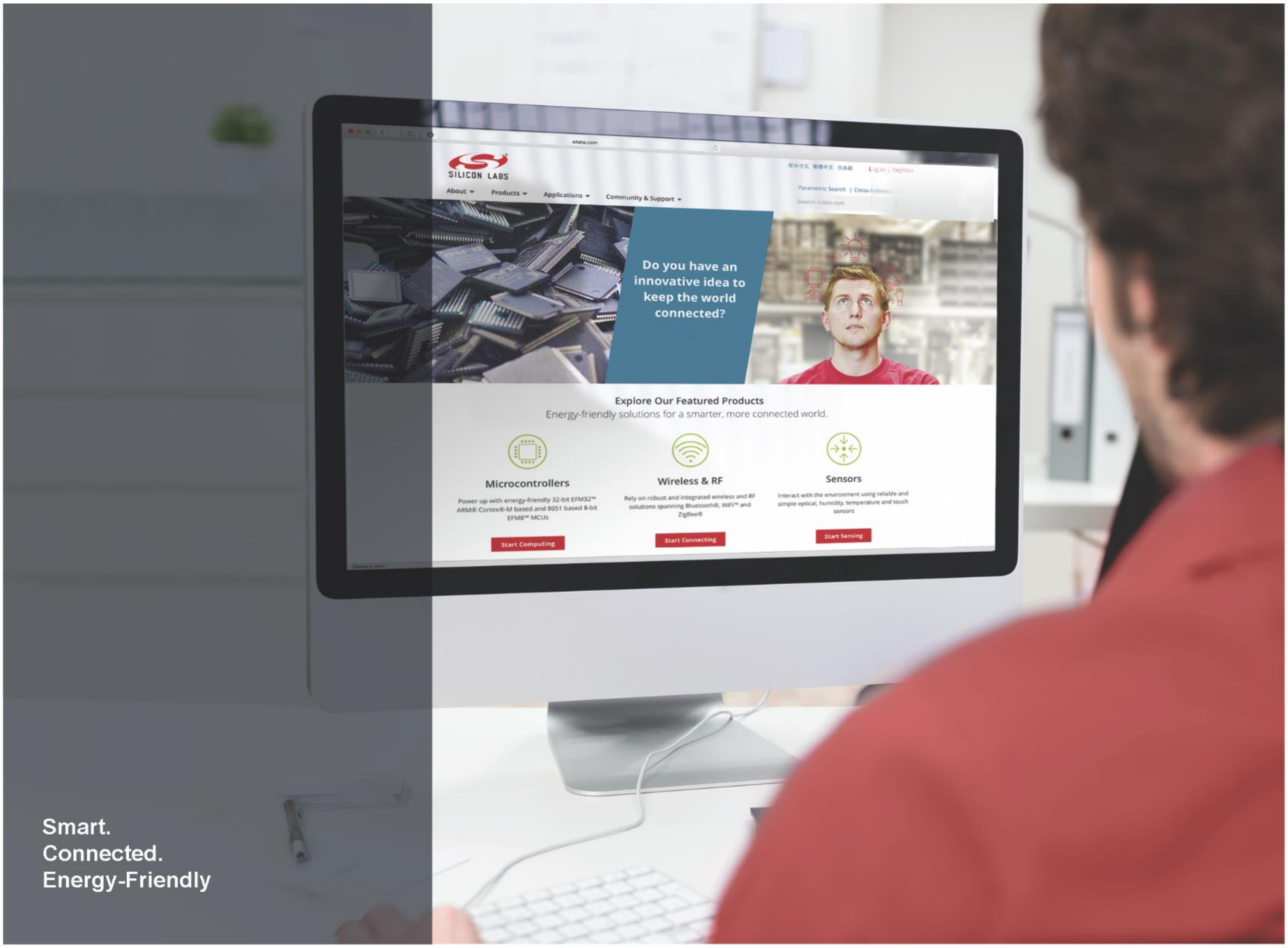
10 References and Related Documentation

- Refer to our RS9116N Open Source Driver Technical Reference Manual which is part of our driver source package available at the link below:

  https://www.silabs.com/wireless/wi-fi/rs9116-wi-fi-transceiver-modules

11 Revision History

Revision No	Version No	Date	History/Comments
1	Initial Version	February, 2019	Initial document
2	Secondary version	August, 2020	Changed the Driver link
3	0.1	August 7, 2020	Initial Review.
4	0.2	August 13, 2020	Review#2
5	0.3	September 6, 2020	Review#3
6	0.4	October 16, 2020	Updated OSD related changes. Updated references.


silabs.com
SILICON LABS
About
Products
Applications
Community & Support
Log in | Register
Parametric Search | Cross-Reference
Search silabs.com
Do you have an innovative idea to keep the world connected?
Explore Our Featured Products
Energy-friendly solutions for a smarter, more connected world.
Microcontrollers
Power up with energy-friendly 32-bit EFM32™ ARM® Cortex®-M based and 8051 based 8-bit EFM8™ MCUs
Start Computing
Wireless & RF
Rely on robust and integrated wireless and RF solutions spanning Bluetooth®, WiFi™ and ZigBee®
Start Connecting
Sensors
Interact with the environment using reliable and simple optical, humidity, temperature and touch sensors
Start Sensing

Smart.
Connected.
Energy-Friendly

Products
www.silabs.com/products

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

Disclaimer

Silicon Laboratories intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Laboratories products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Laboratories reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Laboratories shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products must not be used within any Life Support System without the specific written consent of Silicon Laboratories. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Laboratories products are generally not intended for military applications. Silicon Laboratories products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information

Silicon Laboratories Inc., Silicon Laboratories, Silicon Labs, SiLabs and the Silicon Labs logo, CMEMS®, EFM, EFM32, EFR, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZMac®, EZRadio®, EZRadioPRO®, DSPLL®, ISOmodem ®, Precision32®, ProSLIC®, SiPHY®, USBXpress® and others are trademarks or registered trademarks of Silicon Laboratories Inc. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com