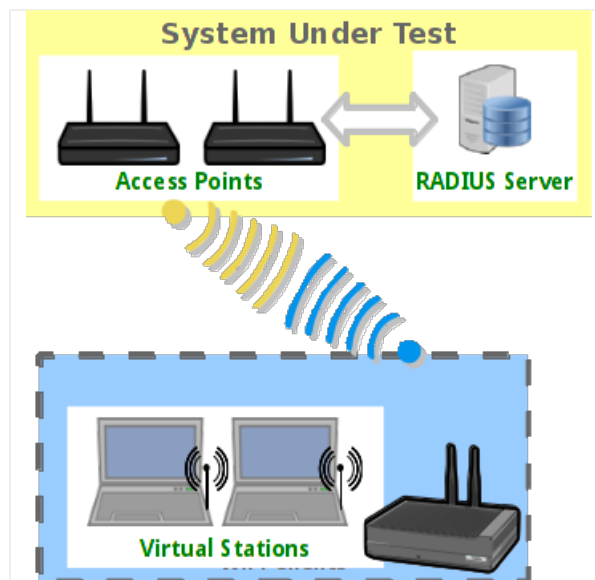


## LANforge WiFi testing Roaming and HotSpot 2.0

**Goal:** Use automated script to reconnect stations to an AP and report results. Requires LANforge 5.2.11 or later. Configure Stations to use HotSpot 2.0 (802.1x, 802.1u, etc) and associate them with a HotSpot 2.0 AP. Use the 'WiFi Mobility' LANforge-GUI Plugin to automate re-connecting to the AP and querying ANQP. The plugin will create graphs and other reports that can be saved to HTML. This example uses a LANforge CT520 system but the procedure should work on all CT521, CT522, CT523, CT525 and similar systems. The AP in this test is another LANforge machine, but it could be any AP that supports HotSpot 2.0. A similar test could roam between multiple APs. If the APs are all on the same channel there are no restrictions, but if the APs are on different channels, then only a single station can be configured per LANforge radio. In that case, multiple 3-radio CT523 or other high-density systems may be a good choice.



1. Configure stations to connect to an AP configured for HotSpot 2.0.
  - A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create desired number of Station interfaces.

- B. The new stations should appear in the Port-Mgr table. Double-click to modify one of them. Configure IP Address information, set SSID to [BLANK] and select WPA2:

sta1 (ath9k-119) Configure Settings

Port Status Information

Current: LINK-UP GRO Authorized

Driver Info: Port Type: WIFI-STA Parent: wiphy0

Port Configurables

Standard Configuration

Advanced Configuration

Enable

☒ Set IP Info

☒ Set IP6 Info

☐ Set IF Down

☐ Set MAC

☐ Set TX Q Len

☐ Set MTU

☐ Set Offload

☐ Set PROMISC

Services

☐ HTTP

☐ FTP

Low Level

☐ PROMISC

☐ TSO Enabled

☐ UFO Enabled

☐ GSO Enabled

☐ LRO Enabled

☒ GRO Enabled

General Interface Settings

☐ DHCP-IPv6

☒ DHCP Release

☐ Down

☐ Aux-Mgt

☒ DHCP-IPv4

Secondary-IPs

DHCP Client ID: None

DNS Servers: 10.97.1.1

Peer IP: NA

IP Address: 9.9.9.2

Global IPv6: AUTO

IP Mask: 255.255.255.0

Link IPv6: AUTO

Gateway IP: 0.0.0.0

IPv6 GW: AUTO

Alias:

MTU: 1500

MAC Addr: 00:ab:cd:ef:01:02

TX Q Len: 1000

Rpt Timer: medium (8 s)

WiFi Bridge: NONE

WiFi Settings

SSID: [BLANK]

AP: DEFAULT

Key/Phrase:

Mode: 802.11abgn

Freq/Channel: 5180/36

Rate: OS Default

RTS: -1

Tx-Power: 17 dBm

AMPDU-Factor: OS Default

AMPDU-Density: OS Default

Max-AMSDU: OS Default

Bridge-IP: 0.0.0.0

☐ Use WPA

☒ Use WPA2

☐ Use WEP

☐ Disable HT40

☐ Disable SGI

☐ Scan Hidden

☐ Allow Migration

Print

View Details

Probe

Display Scan

Sync

Apply

OK

Cancel

- C. Select the **Advanced Configuration** tab in the Port-Modify window and configure the Key Management, EAP Method, passwords, select **Use 802.1x**, **Enable 802.11u** and **HotSpot 2.0**. If you want to report on DHCP negotiation times, be sure to select the **Restart DHCP on Connect** checkbox. If you want to get packet-drop statistics during roam, Un-select **Restart DHCP on Connect**:

**sta1 (ath9k-119) Configure Settings**

**Port Status Information**  
Current: LINK-UP GRO Authenticated  
Driver Info: Port Type: WIFI-STA Parent: wiphy0

**Port Configurables**

**Standard Configuration** **Advanced Configuration**

**Advanced WiFi Settings**

Select 'WPA2' on the Standard Configuration screen to enable 802.1x and enable 802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: WPA-EAP HESSID: 00:00:00:00:00:00  
Pairwise Ciphers: CCMP TKIP Realm: lanforge.org  
Group Ciphers: All Client Cert:  
WPA PSK:  
EAP Methods: EAP-TTLS Milenage:  
EAP Identity: testuser Domain: lanforge.org  
EAP Anon Identity:  
EAP Password: testpasswd Consortium:  
EAP Pin: Phase-1:  
Private Key: Phase-2: auth=MSCHAPV2  
CA Cert File: PK Password:  
Network Auth: PAC File:  
☒ Use 802.1x ☐ PC/SC & SIM/USIM ☒ Enable 802.11u ☒ HotSpot 2.0 ☐ Enable PKC  
☐ Custom WPA Cfg WPA Cfg:  
☒ Restart DHCP on Connect

Print View Details Probe Display Scan Sync Apply OK Cancel

- D. Once the single station is connecting properly, use Batch-Modify to configure the rest of the stations to match the first.

For more information see [LANforge User's Guide: Ports \(Interfaces\)](#) , [WiFi Station Cookbook](#) , [WiFi HotSPot 2.0 Cookbook](#)

2. Start the WiFi Migration script.

- A. Go to the Port Manager tab, select the stations you wish to roam, right-click and choose the **WiFi Mobility** menu option.

WiFi Mobility

Refresh Interval (ms):

5000

Pause Between Commands (ms):

50

Pause after Show-Port (ms):

1000

Auto-Verify timer (ms):

1000

Maximum roam-time in graphs (ms):

250

☐ Skip Roam to current AP

☒ Run Script in Loop

☐ Clear Counters on Start

WiFi Stations

Ports in Use

1.3.5 sta2  
1.3.6 sta3  
1.3.7 sta4  
1.3.8 sta5  
1.3.9 sta6  
1.3.10 sta7

← Add Station

Remove Station →

Free Ports

1.1.4 wlan0  
1.1.5 wlan1  
1.3.2 sta0  
1.3.4 sta1  
1.3.11 sta8  
1.3.12 sta9  
1.3.13 sta10  
1.3.14 sta11  
1.3.15 sta12  
1.3.16 sta13

Before roaming, you should first scan the proper frequencies. Otherwise, the supplicant process may do an internal scan which may significantly affect the connection time:

```
do_cli scan 1 Resource STA NA 'trigger freq F1 F2'
```

To roam to a new Access Point, add a line in the text area with the following format:

```
roam Resource STA BSSID
```

- Resource: Station's resource ID number, often '1'
- STA: name of the station to roam: 'sta11'
- BSSID: the BSSID address of the AP: 00:01:02:03:04:05
- F1: the first frequency to scan: 5180
- F2: Optional second frequency to scan: 5300

After issuing ROAM commands, a pause should be added to let the stations adjust (in seconds, floating-point allowed):

```
sleep 20
```

To issue a generic LANforge CLI command, begin command with:

```
do_cli
```

Example:

```
do_cli scan 1 1 sta1 NA 'trigger freq 5180 5300'
sleep 1
roam 1 sta1 dc:a5:f4:ff:4f:ae
sleep 20
do_cli scan 1 1 sta1 NA 'trigger freq 5180 5300'
sleep 1
roam 1 sta1 dc:a5:f4:f3:ce:9e
sleep 20
```

```
# When roaming to self, anqp is not normally done
# so this script forces an ANQP query so that we
# get some ANQP query report times to display.

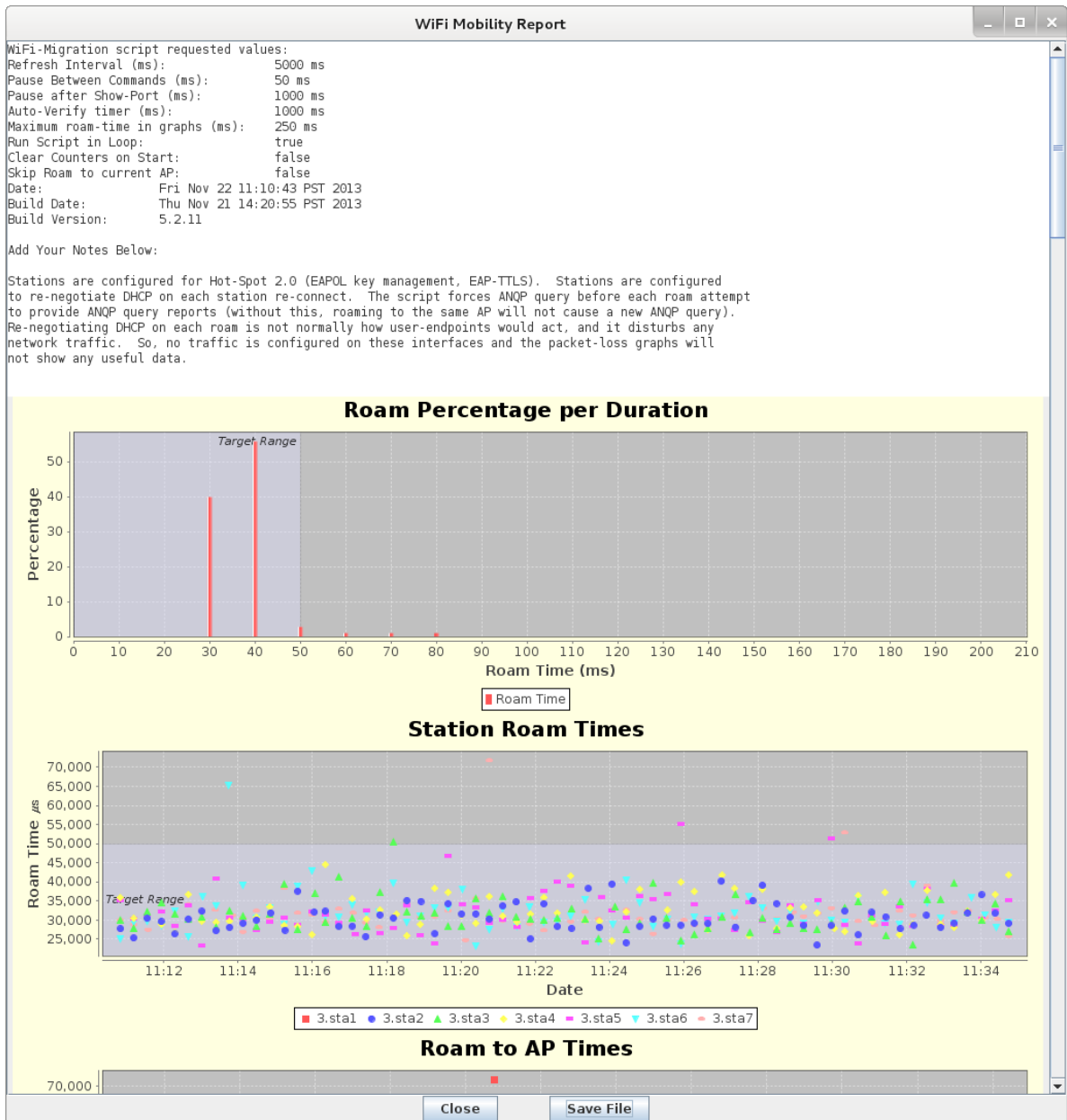
do_cli scan 1 3 sta1 NA 'trigger freq 5180 5300'
sleep 1
do_cli wifi_cli_cmd 1 3 sta1 'fetch_anqp'
roam 3 sta1 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta2 'fetch_anqp'
roam 3 sta2 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta3 'fetch_anqp'
roam 3 sta3 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta4 'fetch_anqp'
roam 3 sta4 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta5 'fetch_anqp'
roam 3 sta5 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta6 'fetch_anqp'
roam 3 sta6 80:01:02:03:04:05
do_cli wifi_cli_cmd 1 3 sta7 'fetch_anqp'
roam 3 sta7 80:01:02:03:04:05
sleep 20
```

Start

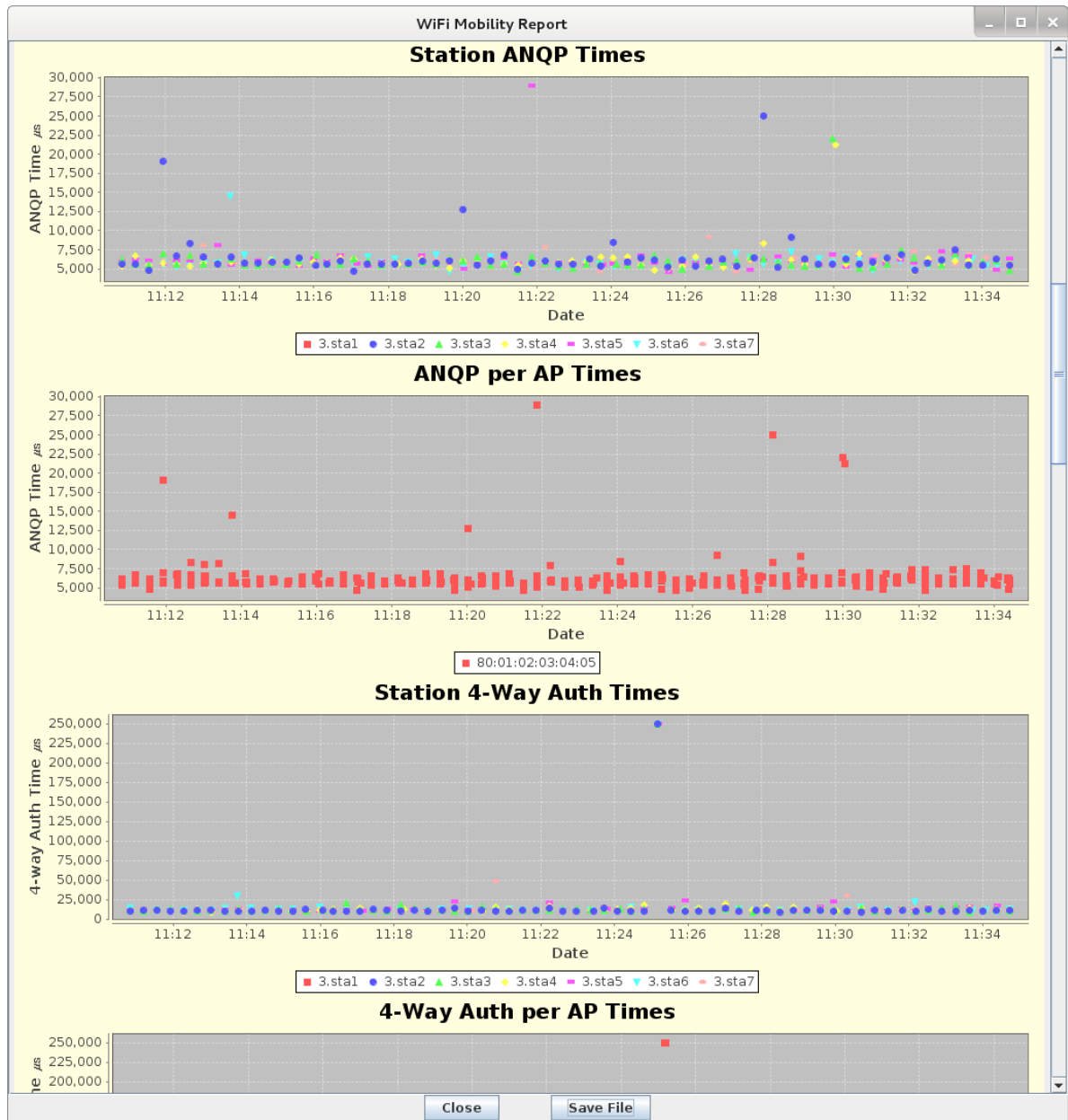
Close

- B. The options at the top default to common values and most do not need to be changed. For this example, you must unselect **Skip Roam to current AP** because the script is requesting exactly that. The ports will be automatically configured based on the selection on the Port Manager tab, and may be adjusted before starting the script. The **Ports in Use** should normally include all stations used in the script. The configuration requiring the most work from the user is the roaming script itself. There is a help section on the left, and a script-entry field on the right. Once the script is written, it should be saved in a text file on the user's PC so that it can easily be pasted into future WiFi Mobility scripts. Some key points are that you must scan about 1 second before roaming or the roam logic in the supplicant process will either fail or do its own roaming. Either way, the results may be worse than if you do the roam properly in the script. It can take a bit of time for LANforge to get all of the data it needs to report on the roam attempt, so it is suggested that stations not roam more often than about once every 10-20 seconds. If reporting is less important, then the stations can roam more often.

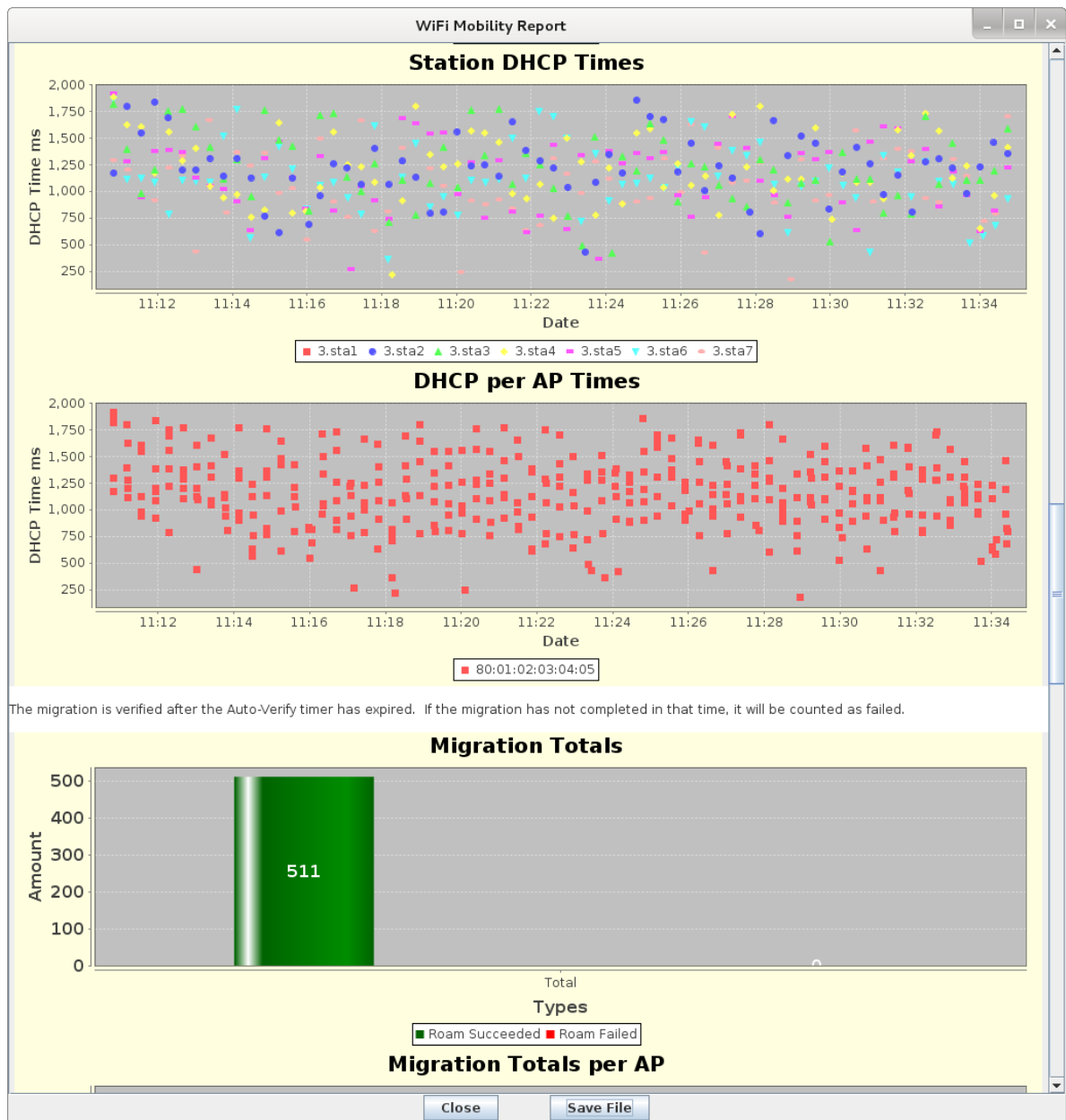
- C. Once the script is properly configured, click Start to start the roaming. A window will pop up that has live-updating graphs of various reports. A text log is at the bottom for more detailed analysis, and the whole thing can be saved as HTML. The graphs can be scaled and configured through right-click menus if desired. It will take 1-2 complete roam attempts before the graphs are able to show any useful information.



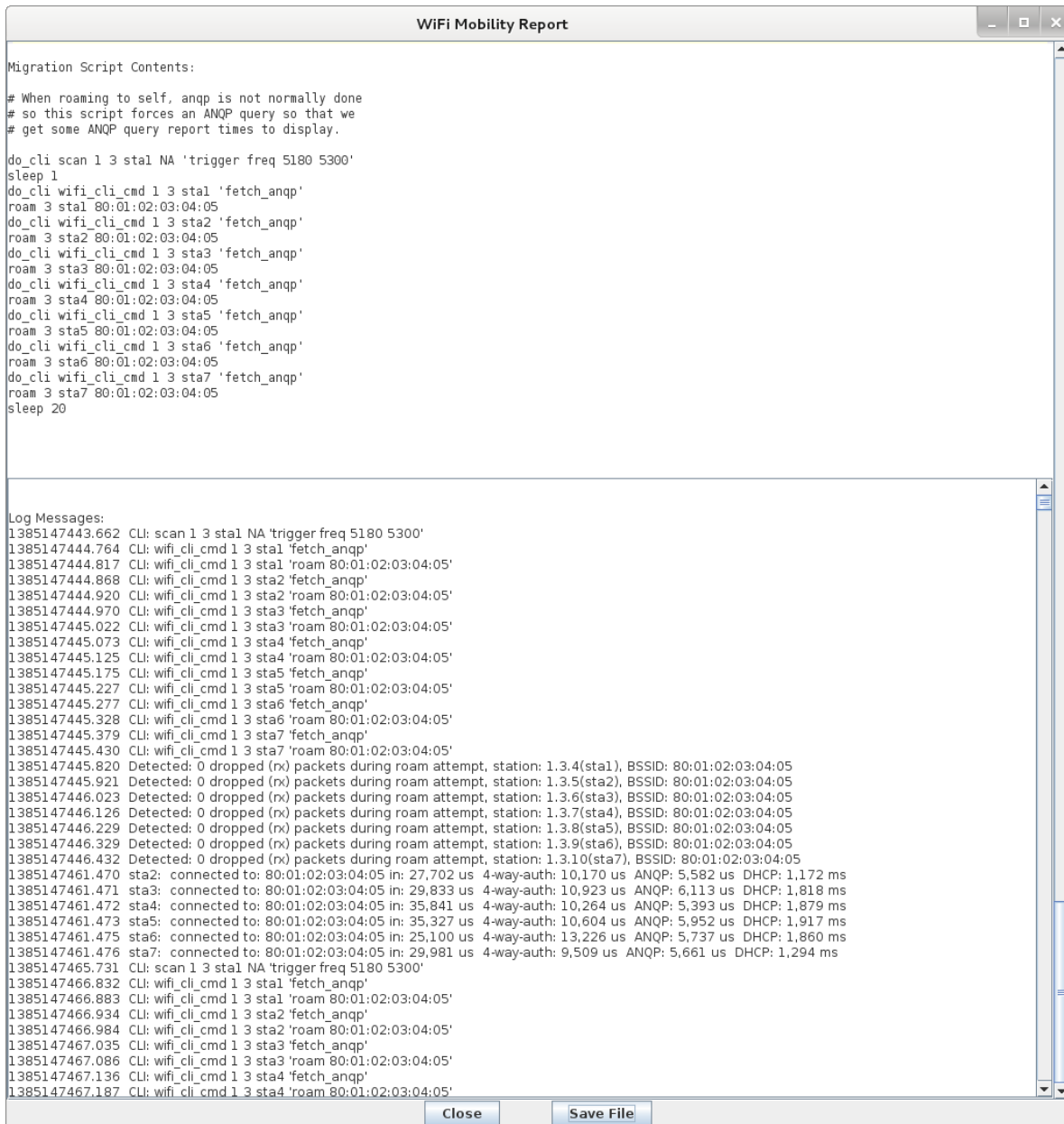
D. ANQP and 4-Way Authentication graphs.



E. DHCP Negotiation and Migration Totals graphs.



F. Text log with timestamps. Can be correlated with wpa\_supplicant logs and other log files to debug specific roam attempts.



For more information see [Complete report for this test case](#)

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA  
www.candelatech.com | sales@candelatech.com | +1.360.380.1618