

LANforge WiFi testing with HotSpot 2.0

Goal: Authenticate using HotSpot 2.0, 802.11u, and 802.1x EAP-TTLS.

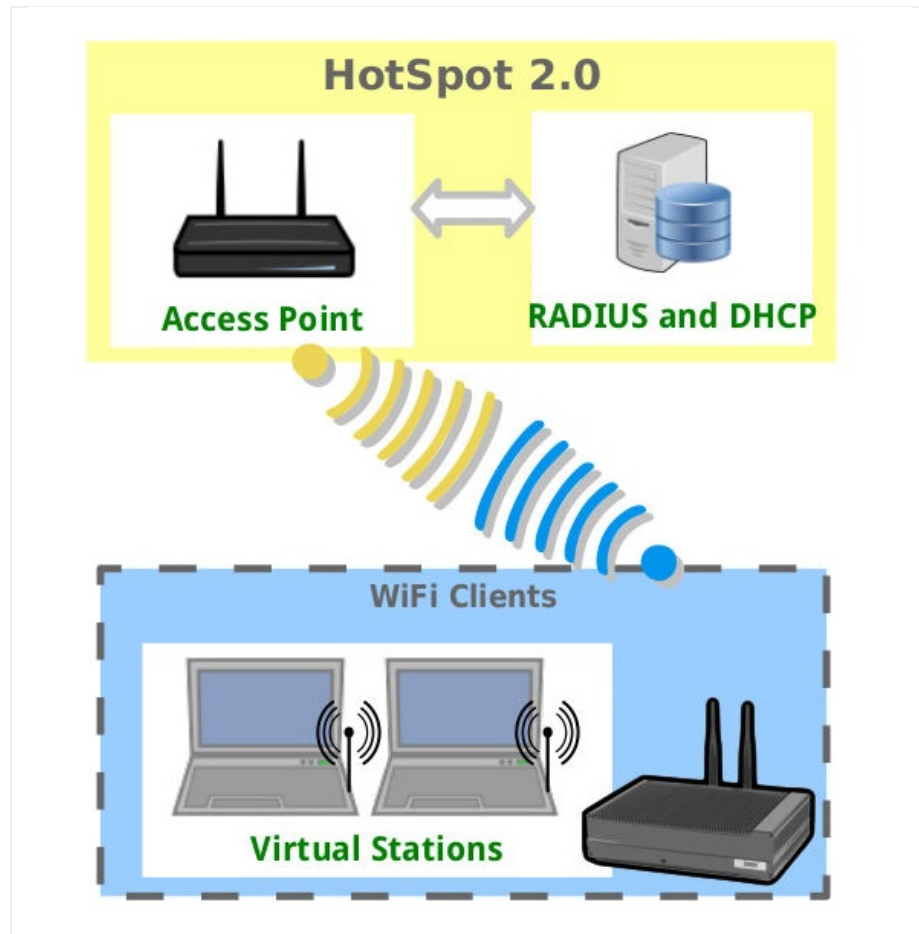
Simplest HotSpot 2.0 example using EAP-TTLS where the client only needs a username and password to authenticate.

There are four main components to setting up this test:

1. One or more Access Points
2. A RADIUS Server
3. A DHCP Server
4. One or more Clients

In this example, one LANforge system will fulfill the roles of APs, RADIUS and DHCP servers while another LANforge system will fulfill the role of Client devices.

Any one of the four main components can be replaced by 3rd party devices as required.



-
1. Configure Access Point 1

A. Standard Configuration tab:

vap0 (lf0350-6b3c) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy0 [wiphy0...](#)

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Enable

☐ Set MAC
☐ Set TX Q Len
☐ Set MTU
☐ Set Offload
☐ Set PROMISC

Services

☐ HTTP
☐ FTP
☐ DNS
☐ IPSEC-Client
☐ IPsec-Upstream

Low Level

☐ PROMISC
☒ TSO Enabled
☐ UFO Enabled
☒ GSO Enabled
☐ LRO Enabled
☒ GRO Enabled

General Interface Settings

☐ Down ☐ Aux-Mgt DHCP Hostname:
☐ DHCP-IPv6 ☒ DHCP Release DHCP Vendor ID:
☒ DHCP-IPv4 [Secondary-IPs](#) DHCP Client ID:
DNS Servers: Peer IP:
IP Address: Global IPv6:
IP Mask: Link IPv6:
Gateway IP: IPv6 GW:
Alias: MTU:
MAC Addr: TX Q Len:
Rpt Timer: WiFi Bridge:
IPSec GW: IPSec Password:
IPSec Local ID.: IPSec Remote ID.:

WiFi Settings

SSID: AP:
Key/Phrase: [?] Mode:
Freq/Channel: Rate:
DTIM-Period: Max-STA:
Beacon:
☐ WPA ☒ WPA2 ☐ WPA3 ☐ OSEN ☐ WEP ☐ Verbose Debug
☐ Disable HT40 ☐ Disable HT80 ☐ Enable VHT160 ☐ Disable SGI

[Print](#) [Display](#) [Logs](#) [Probe](#) [Display Scan](#) [Sync](#) [Apply](#) [OK](#) [Cancel](#)

B. Advanced Configuration tab:

vap0 (lf0350-6b3c) Configure Settings

Port Status Information

Current: LINK-UP GRO NONE

Driver Info: Port Type: WIFI-AP Parent: wiphy0 wiphy0...

Port Configurables

Standard Configuration

Advanced Configuration

Misc Configuration

Custom WiFi

Advanced WiFi Settings

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

Pairwise Ciphers: DEFAULT

Group Ciphers: DEFAULT

Ignore Probes: zero (0%)

HESSID: 04:f0:21:d1:e7:79

Ignore Auth-Assoc: zero (0%)

Realm: 0.vap0.localdomain,21[5:7]

Ignore Assoc: zero (0%)

IMSI:

Ignore Re-Assoc: zero (0%)

Milenage:

Corrupt GTK: zero (0%)

Domain: vap0.localdomain

HS20 Capabilities

Consortium:

HS20 Oper Class

RADIUS IP 127.0.0.1

HS20 WAN Metrics

RADIUS Port 1812

ieee80211w: Disabled (0)

RADIUS Secret lanforge

Venue Group: Unspecified (0)

Venue Type: Unspecified (0)

Network Type: Private (0)

Address Types: Not Available (0)

Network Auth:

3GPP Cell Net:

☒ Use 80211d
☒ Use 80211h
☐ BSS-Load
☐ Neighbor Reports
☐ BSS Transition

☒ Advanced/802.1x
☐ Short-Preamble
☒ HotSpot 2.0
☐ Disable DGAF

☒ Enable 802.11u
☐ 802.11u Internet
☐ 802.11u ASRA
☐ 802.11u ESR
☐ 802.11u UESA

Print

Display

Logs

Probe

Display Scan

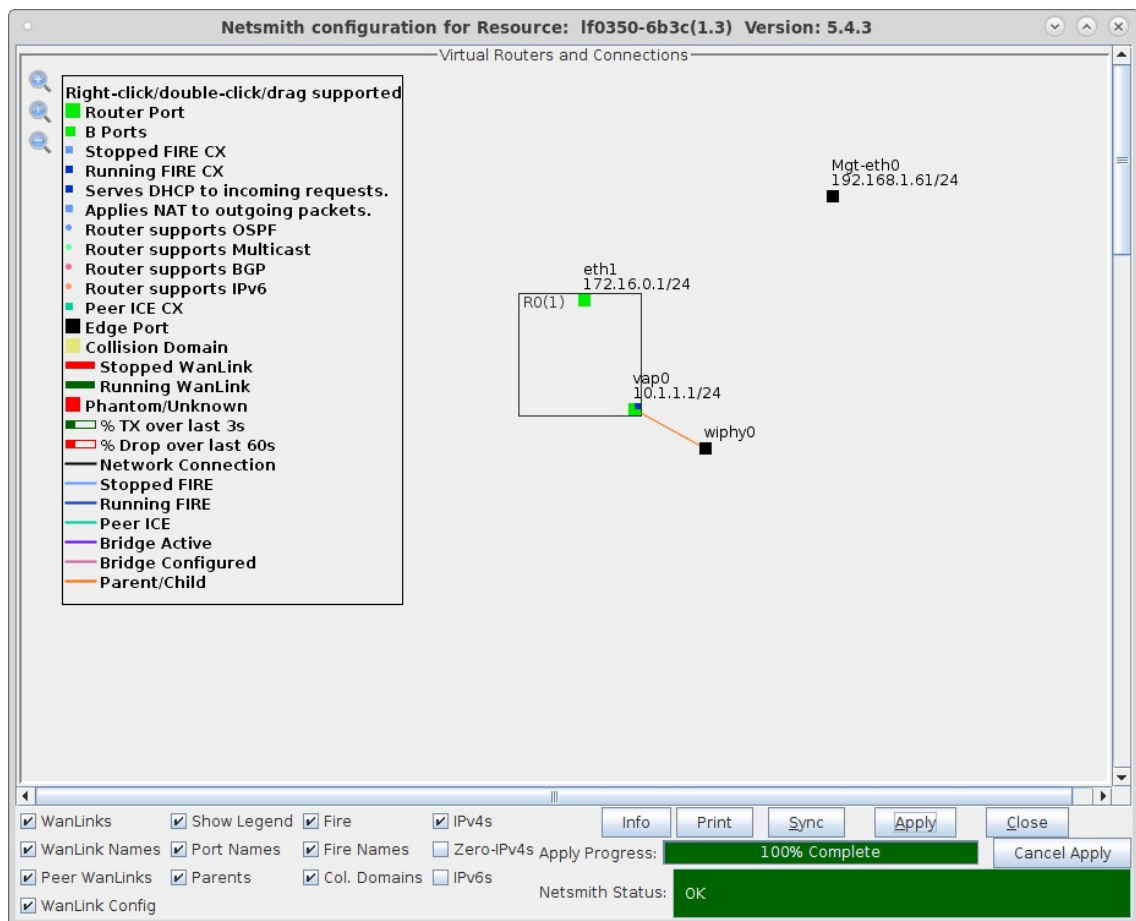
Sync

Apply

OK

Cancel

C. Create a Virtual-Router for DHCP Service:



For more information see

[LANforge User's Guide: Ports \(Interfaces\)](#) ,

[VAP Bridge Mode Cookbook](#) ,

[Virtual Router with DHCP Cookbook](#)

2. Configure Access Point 2

A. Standard Configuration tab:

vap1 (lf0350-6b3c) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy1 [wiphy1...](#)

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Enable

☐ Set MAC
☐ Set TX Q Len
☐ Set MTU
☐ Set Offload
☐ Set PROMISC

Services

☐ HTTP
☐ FTP
☐ DNS
☐ IPSEC-Client
☐ IPsec-Upstream

Low Level

☐ PROMISC
☒ TSO Enabled
☐ UFO Enabled
☒ GSO Enabled
☐ LRO Enabled
☒ GRO Enabled

General Interface Settings

☐ Down ☐ Aux-Mgt DHCP Hostname:
☐ DHCP-IPv6 ☒ DHCP Release DHCP Vendor ID:
☒ DHCP-IPv4 [Secondary-IPs](#) DHCP Client ID:
DNS Servers: Peer IP:
IP Address: Global IPv6:
IP Mask: Link IPv6:
Gateway IP: IPv6 GW:
Alias: MTU:
MAC Addr: TX Q Len:
Rpt Timer: WiFi Bridge:
IPSec GW: IPSec Password:
IPSec Local ID.: IPSec Remote ID.:

WiFi Settings

SSID: AP:
Key/Phrase: [?] Mode:
Freq/Channel: Rate:
DTIM-Period: Max-STA:
Beacon:
☐ WPA ☒ WPA2 ☐ WPA3 ☐ OSEN ☐ WEP ☐ Verbose Debug
☐ Disable HT40 ☐ Disable HT80 ☐ Enable VHT160 ☐ Disable SGI

[Print](#) [Display](#) [Logs](#) [Probe](#) [Display Scan](#) [Sync](#) [Apply](#) [OK](#) [Cancel](#)

B. Advanced Configuration tab:

vap1 (lf0350-6b3c) Configure Settings

Port Status Information

Current: LINK-UP GRO NONE

Driver Info: Port Type: WIFI-AP Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration

Advanced Configuration

Misc Configuration

Custom WiFi

Advanced WiFi Settings

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

Pairwise Ciphers: DEFAULT

Group Ciphers: DEFAULT

Ignore Probes: zero (0%)

HESSID: 00:0e:8e:b9:8e:26

Ignore Auth-Assoc: zero (0%)

Realm: 0.vap1.localdomain,21[5:7]

Ignore Assoc: zero (0%)

IMSI:

Ignore Re-Assoc: zero (0%)

Milenage:

Corrupt GTK: zero (0%)

Domain: vap1.localdomain

HS20 Capabilities:

Consortium:

HS20 Oper Class:

RADIUS IP: 127.0.0.1

HS20 WAN Metrics:

RADIUS Port: 1812

ieee80211w: Disabled (0)

RADIUS Secret: lanforge

Venue Group: Unspecified (0)

Venue Type: Unspecified (0)

Network Type: Private (0)

Address Types: Not Available (0)

Network Auth:

3GPP Cell Net:

Use 80211d

Use 80211h

BSS-Load

Neighbor Reports

BSS Transition

Advanced/802.1x

Short-Preamble

HotSpot 2.0

Disable DGAF

Enable 802.11u

802.11u Internet

802.11u ASRA

802.11u ESR

802.11u UESA

Print

Display

Logs

Probe

Display Scan

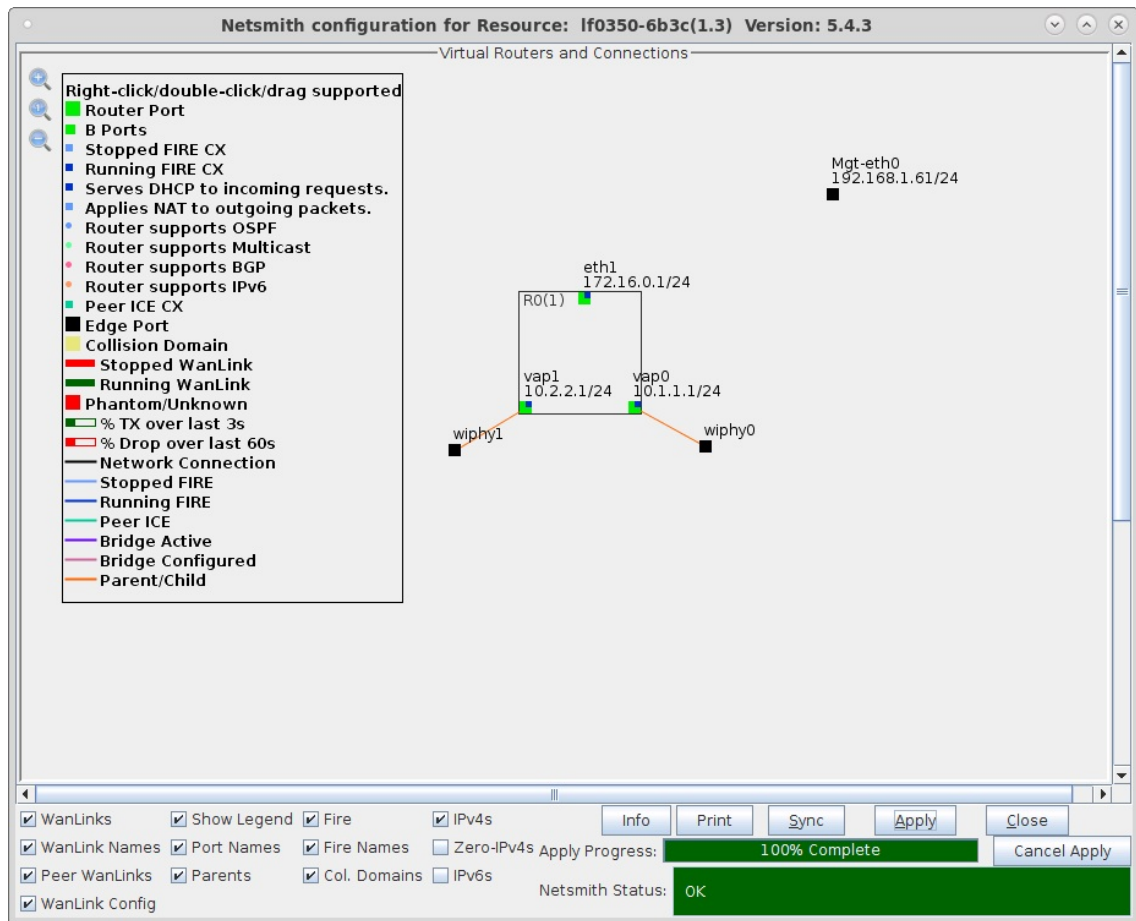
Sync

Apply

OK

Cancel

C. Add DHCP Service for the second AP:

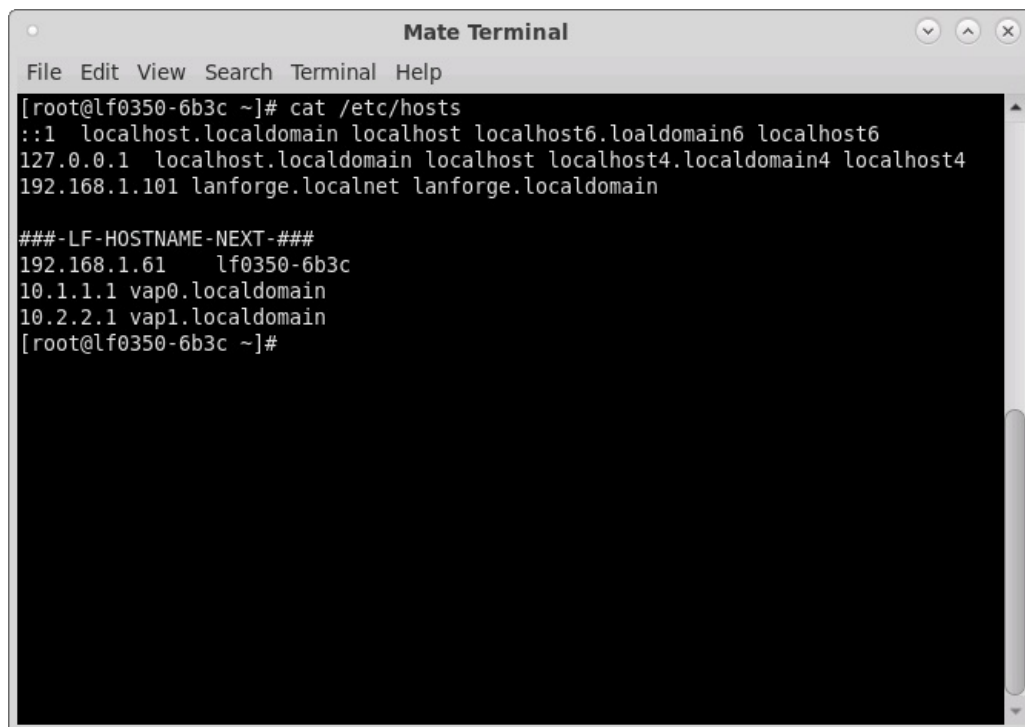


3. Verify FreeRadius is running and setup /etc/hosts file.

A. FreeRadius is installed on the LANforge system by default with the TTLS user/pass credentials
testuser / testpasswd.

```
Mate Terminal
File Edit View Search Terminal Help
[root@lf0350-6b3c ~]# pgrep radiusd
1125
[root@lf0350-6b3c ~]# radtest testuser testpasswd 127.0.0.1:1812 0 lanforge
Sent Access-Request Id 90 from 0.0.0.0:14347 to 127.0.0.1:1812 length 78
  User-Name = "testuser"
  User-Password = "testpasswd"
  NAS-IP-Address = 192.168.1.61
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "testpasswd"
Received Access-Accept Id 90 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
[root@lf0350-6b3c ~]#
```

- B. Edit /etc/hosts to add local domain names for each AP.



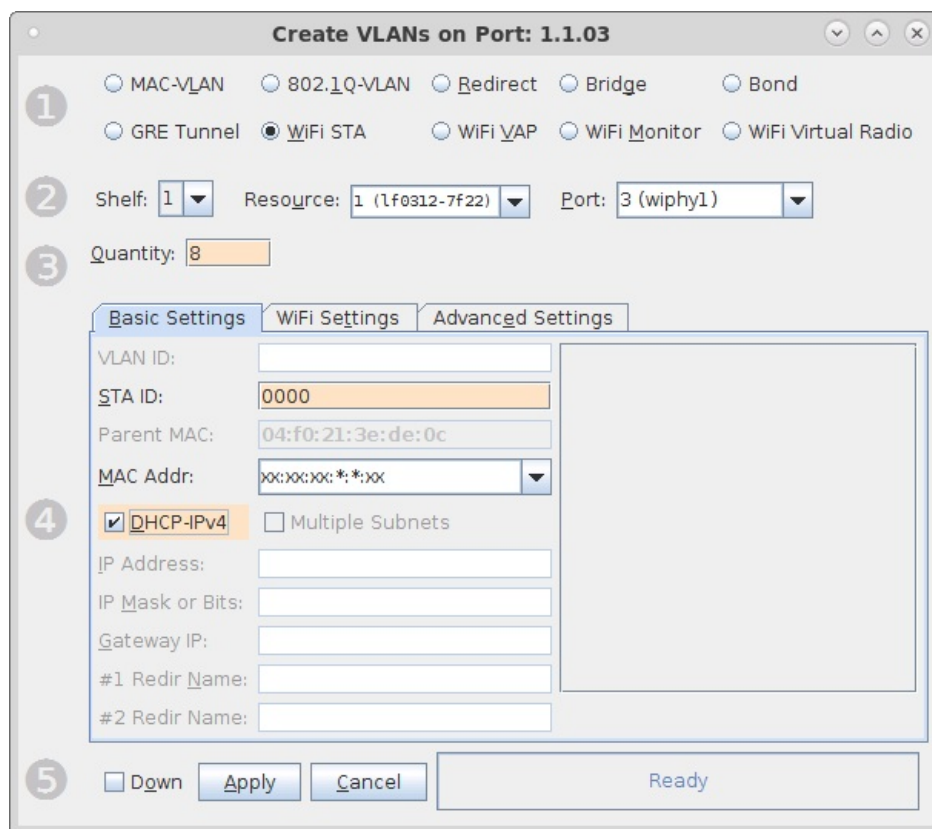
A screenshot of a Mate Terminal window titled "Mate Terminal". The terminal shows the command `cat /etc/hosts` and its output. The output lists several host entries, including `localhost.localdomain`, `localhost6.localdomain6`, `127.0.0.1`, `192.168.1.101`, `lanforge.localnet`, `lanforge.localdomain`, and a section for the host `lf0350-6b3c` with its IP `192.168.1.61` and various virtual interface addresses like `vap0.localdomain` and `vap1.localdomain`.

```
[root@lf0350-6b3c ~]# cat /etc/hosts
::1 localhost.localdomain localhost localhost6.localdomain6 localhost6
127.0.0.1 localhost.localdomain localhost localhost4.localdomain4 localhost4
192.168.1.101 lanforge.localnet lanforge.localdomain

###-LF-HOSTNAME-NEXT-###
192.168.1.61 lf0350-6b3c
10.1.1.1 vap0.localdomain
10.2.2.1 vap1.localdomain
[root@lf0350-6b3c ~]#
```

4. Create EAP-TTLS (802.1X username + password authentication) for one or more clients.

- A. Create stations.



A screenshot of the "Create VLANs on Port: 1.1.03" dialog box. The dialog is divided into several sections. Section 1 shows radio buttons for `MAC-VLAN`, `802.1Q-VLAN`, `Redirect`, `Bridge`, `Bond`, `GRE Tunnel`, `WiFi STA` (selected), `WiFi VAP`, `WiFi Monitor`, and `WiFi Virtual Radio`. Section 2 shows dropdowns for `Shelf: 1`, `Resource: 1 (1f0312-7f22)`, and `Port: 3 (wiphy1)`. Section 3 shows a `Quantity: 8` input field. Section 4 shows tabs for `Basic Settings`, `WiFi Settings`, and `Advanced Settings`. Under `Basic Settings`, there are fields for `VLAN ID:`, `STA ID: 0000`, `Parent MAC: 04:f0:21:3e:de:0c`, and `MAC Addr: xx:xx:xx:*:*:xx`. There are checkboxes for `DHCP-IPv4` (checked) and `Multiple Subnets`. Below these are fields for `IP Address:`, `IP Mask or Bits:`, `Gateway IP:`, `#1 Redir Name:`, and `#2 Redir Name:`. Section 5 shows a `Down` checkbox, `Apply`, `Cancel`, and `Ready` buttons.

B. The SSID and Key/Password do not need to be configured when using HotSpot 2.0:

sta0000 (If0312-7f22) Configure Settings

Port Status Information
Current: DOWN LINK-DOWN GRO NONE
Driver Info: Port Type: WIFI-STA Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Corruptions | Custom WiFi

Enable

☐ Set MAC
☐ Set TX Q Len
☐ Set MTU
☐ Set Offload
☐ Set PROMISC

Services

☐ HTTP
☐ FTP
☐ DNS
☐ RADIUS
☐ IPSEC-Client
☐ IPsec-Upstream

Low Level

☐ PROMISC
☒ TSO Enabled
☐ UFO Enabled
☐ GSO Enabled
☐ LRO Enabled
☒ GRO Enabled

General Interface Settings

☒ Down ☐ Aux-Mgt
☐ DHCP-IPv6 ☒ DHCP Release
☒ DHCP-IPv4 Secondary-IPs
DNS Servers: BLANK Peer IP: NA
IP Address: 0.0.0.0 Global IPv6: AUTO
IP Mask: 0.0.0.0 Link IPv6: AUTO
Gateway IP: 0.0.0.0 IPv6 GW: AUTO
Alias: MTU: 1500
MAC Addr: 04:f0:21:02:17:0c TX Q Len: 1000
Rpt Timer: faster (1 s) WiFi Bridge: NONE
IPSec GW: 0.0.0.0 IPSec Password:
IPSec Local ID.: IPSec Remote ID.:

WiFi Settings

SSID: [BLANK] AP: DEFAULT
Key/Phrase: [?] Mode: 802.11abgn-AC
Freq/Channel: 0/0 Rate: OS Default
☐ WPA ☒ WPA2 ☐ WPA3 ☐ OSEN ☐ WEP
☐ Disable HT40 ☐ Enable VHT160 ☐ Disable SGI

Print Display Probe Display Scan Sync Apply OK Cancel

- C. Select the **Advanced Configuration** tab in the Port-Modify window and configure the 802.1x, 802.11u, HotSpot 2.0 and other information. The **EAP Identity** and **EAP Password** must match the configuration on your RADIUS server.

sta0000 (If0312-7f22) Configure Settings

Port Status Information
Current: DOWN LINK-DOWN GRO NONE
Driver Info: Port Type: WIFI-STA Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

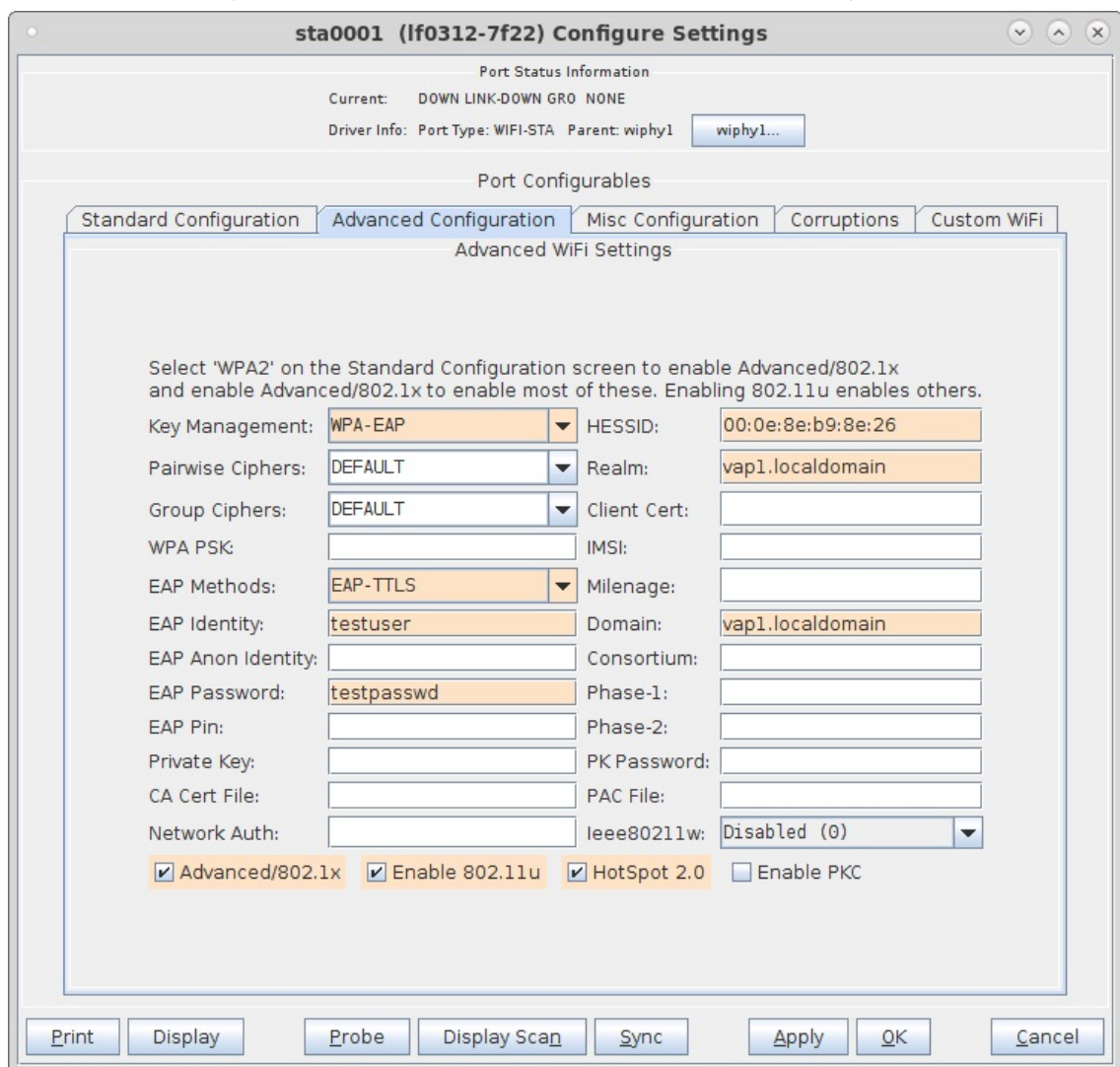
Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management:	WPA-EAP	HESSID:	04:f0:21:d1:e7:79
Pairwise Ciphers:	DEFAULT	Realm:	vap0.localdomain
Group Ciphers:	DEFAULT	Client Cert:	
WPA PSK:		IMSI:	
EAP Methods:	EAP-TTLS	Milenage:	
EAP Identity:	testuser	Domain:	vap0.localdomain
EAP Anon Identity:		Consortium:	
EAP Password:	testpasswd	Phase-1:	
EAP Pin:		Phase-2:	
Private Key:		PK Password:	
CA Cert File:		PAC File:	
Network Auth:		Ieee80211w:	Disabled (0)

☒ Advanced/802.1x ☒ Enable 802.11u ☒ HotSpot 2.0 ☐ Enable PKC

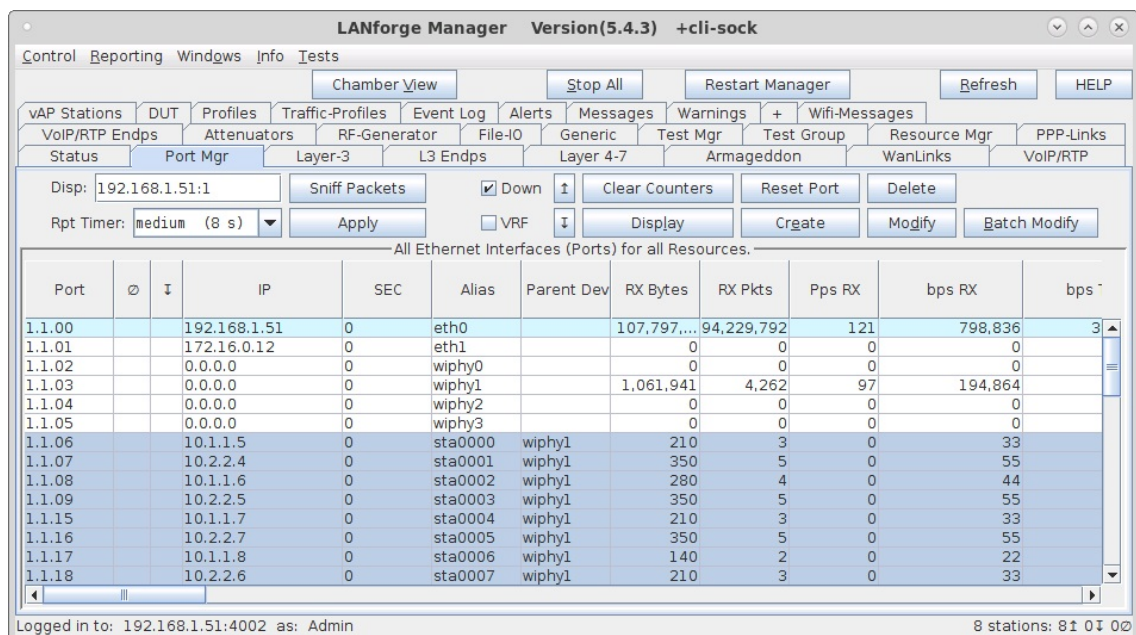
Print Display Probe Display Scan Sync Apply OK Cancel

D. The next station is setup with the HESSID and Realm/Domain of the second access point.



The image shows the 'sta0001 (If0312-7f22) Configure Settings' window. It has a 'Port Status Information' section at the top showing 'Current: DOWN LINK-DOWN GRO NONE' and 'Driver Info: Port Type: WIFI-STA Parent: wiphy1'. Below this are tabs for 'Standard Configuration', 'Advanced Configuration', 'Misc Configuration', 'Corruptions', and 'Custom WiFi'. The 'Advanced Configuration' tab is selected, showing 'Advanced WiFi Settings'. A note states: 'Select "WPA2" on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.' The settings include: Key Management: WPA-EAP, HESSID: 00:0e:8e:b9:8e:26, Pairwise Ciphers: DEFAULT, Realm: vap1.localdomain, Group Ciphers: DEFAULT, Client Cert: (empty), WPA PSK: (empty), IMSI: (empty), EAP Methods: EAP-TTLS, Milenage: (empty), EAP Identity: testuser, Domain: vap1.localdomain, EAP Anon Identity: (empty), Consortium: (empty), EAP Password: testpasswd, Phase-1: (empty), EAP Pin: (empty), Phase-2: (empty), Private Key: (empty), PK Password: (empty), CA Cert File: (empty), PAC File: (empty), Network Auth: (empty), IEEE80211w: Disabled (0). At the bottom are checkboxes for 'Advanced/802.1x' (checked), 'Enable 802.11u' (checked), 'HotSpot 2.0' (checked), and 'Enable PKC' (unchecked). Action buttons at the bottom include Print, Display, Probe, Display Scan, Sync, Apply, OK, and Cancel.

E. Verify stations connect and obtain DHCP IP address configuration.



The image shows the 'LANforge Manager Version(5.4.3) +cli-sock' window. It has a top menu bar with 'Control', 'Reporting', 'Windows', 'Info', and 'Tests'. Below this are various tabs for configuration and monitoring. The 'Port Manager' tab is selected, showing a table of 'All Ethernet Interfaces (Ports) for all Resources.' The table has columns: Port, IP, SEC, Alias, Parent Dev, RX Bytes, RX Pkts, Pps RX, bps RX, and bps T. The data is as follows:

Port	IP	SEC	Alias	Parent Dev	RX Bytes	RX Pkts	Pps RX	bps RX	bps T
1.1.00	192.168.1.51	0	eth0		107,797,...	94,229,792	121	798,836	3
1.1.01	172.16.0.12	0	eth1		0	0	0	0	
1.1.02	0.0.0.0	0	wiphy0		0	0	0	0	
1.1.03	0.0.0.0	0	wiphy1		1,061,941	4,262	97	194,864	
1.1.04	0.0.0.0	0	wiphy2		0	0	0	0	
1.1.05	0.0.0.0	0	wiphy3		0	0	0	0	
1.1.06	10.1.1.5	0	sta0000	wiphy1	210	3	0	33	
1.1.07	10.2.2.4	0	sta0001	wiphy1	350	5	0	55	
1.1.08	10.1.1.6	0	sta0002	wiphy1	280	4	0	44	
1.1.09	10.2.2.5	0	sta0003	wiphy1	350	5	0	55	
1.1.15	10.1.1.7	0	sta0004	wiphy1	210	3	0	33	
1.1.16	10.2.2.7	0	sta0005	wiphy1	350	5	0	55	
1.1.17	10.1.1.8	0	sta0006	wiphy1	140	2	0	22	
1.1.18	10.2.2.6	0	sta0007	wiphy1	210	3	0	33	

At the bottom, it says 'Logged in to: 192.168.1.51:4002 as: Admin' and '8 stations: 81 01 00'.

For more information see [WiFi Station Cookbook](#)