

LANforge WiFi testing with HotSpot 2.0

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

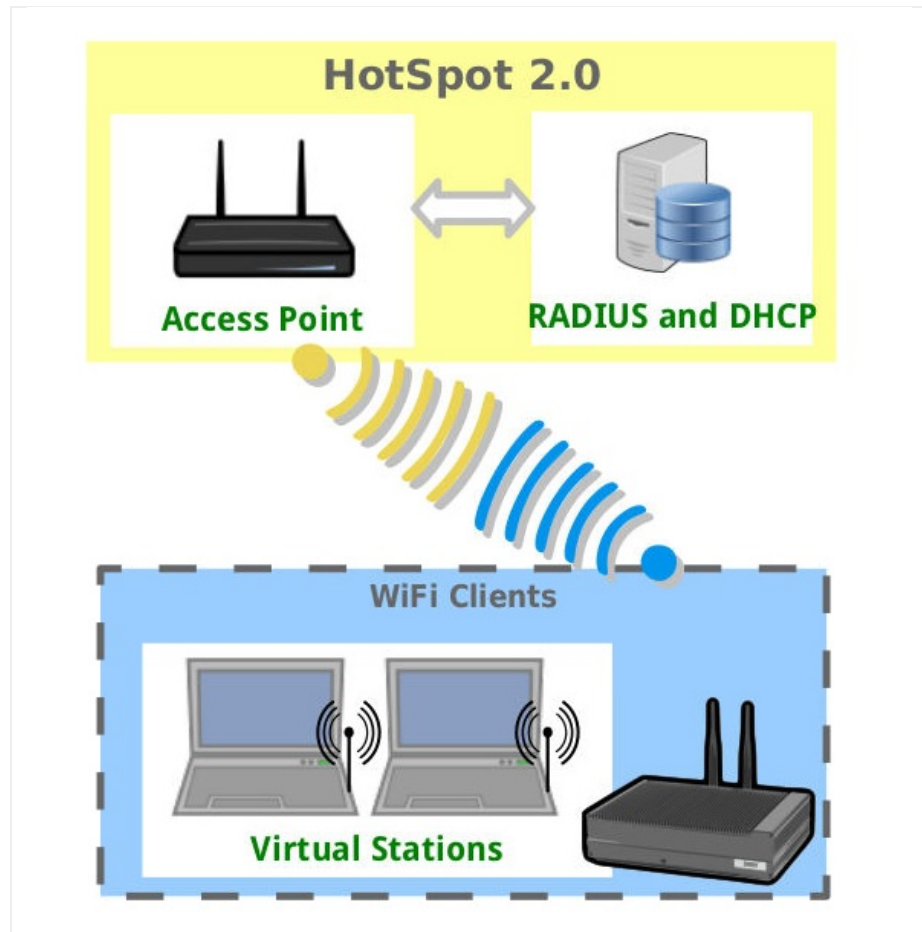
Simplest HotSpot 2.0 example using EAP-TTLS where the client only needs a username and password to authenticate.

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 (If0350-6b3c) 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: 5745/149 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 (If0350-6b3c) 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
leee80211w:	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:	

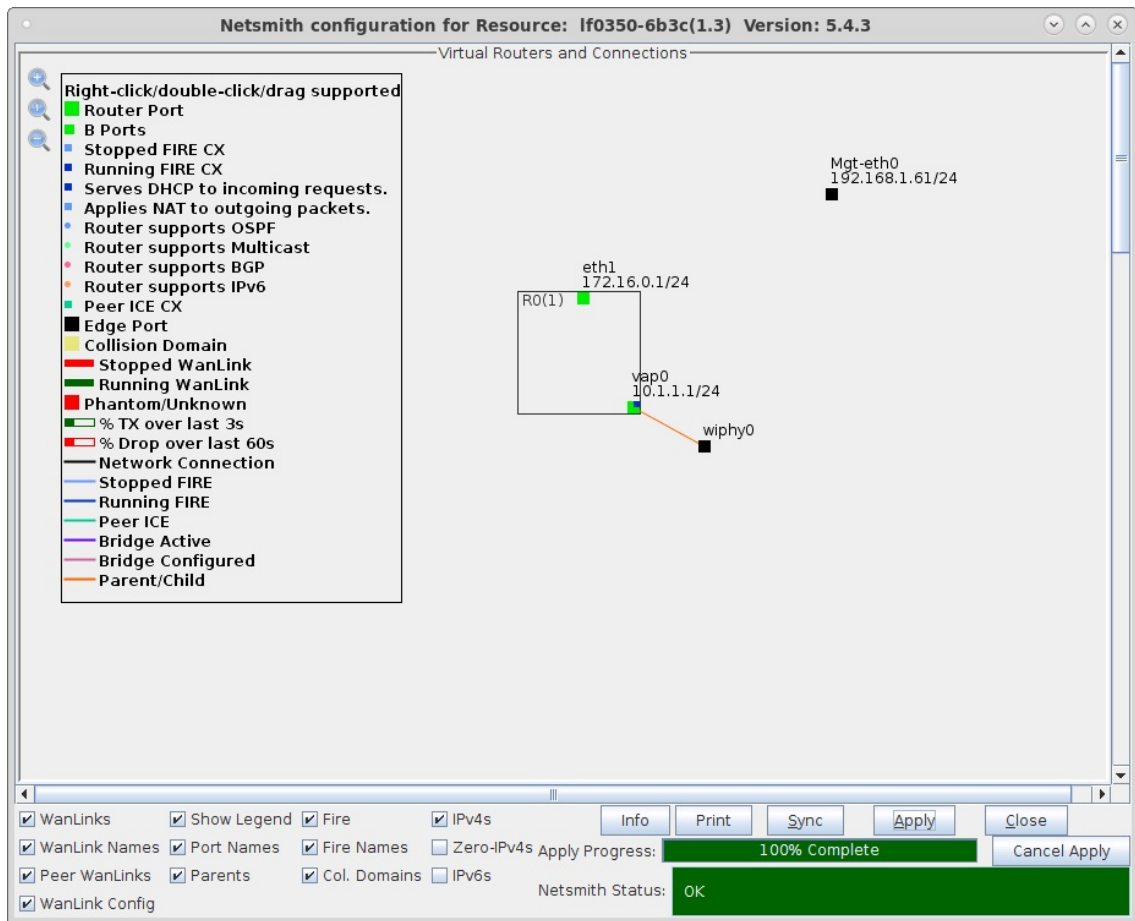
Use 80211d Use 80211h BSS-Load Neighbor Reports BSS Transition

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 (If0350-6b3c) 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-IPv6 DHCP Release

DHCP-IPv4 Secondary-IPs

DNS Servers:

IP Address:

IP Mask:

Gateway IP:

Alias:

MAC Addr:

Rpt Timer: ▼

IPSec GW:

IPSec Local ID.:

DHCP Hostname: ▼

DHCP Vendor ID: ▼

DHCP Client ID: ▼

Peer IP:

Global IPv6:

Link IPv6:

IPv6 GW:

MTU:

TX Q Len:

WiFi Bridge: ▼

IPSec Password:

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
leee80211w:	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:	

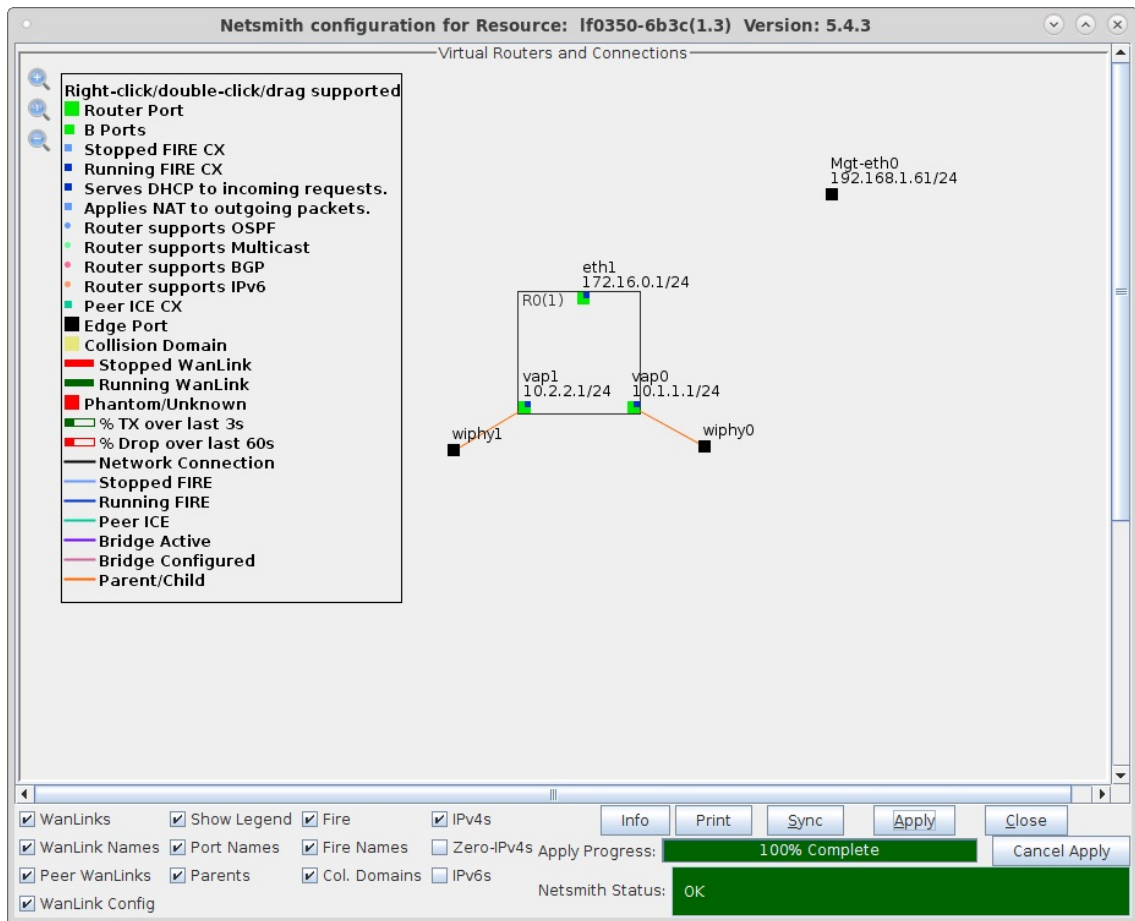
Use 80211d Use 80211h BSS-Load Neighbor Reports BSS Transition

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:

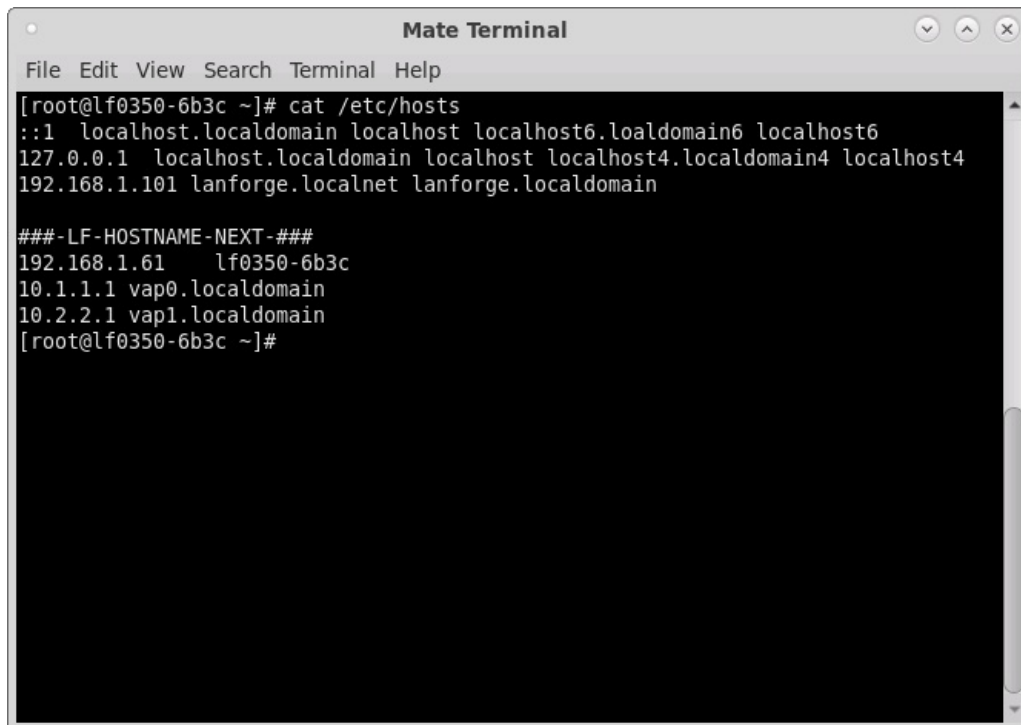


3. Verify FreeRadius is running and setup /etc/hosts file.

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

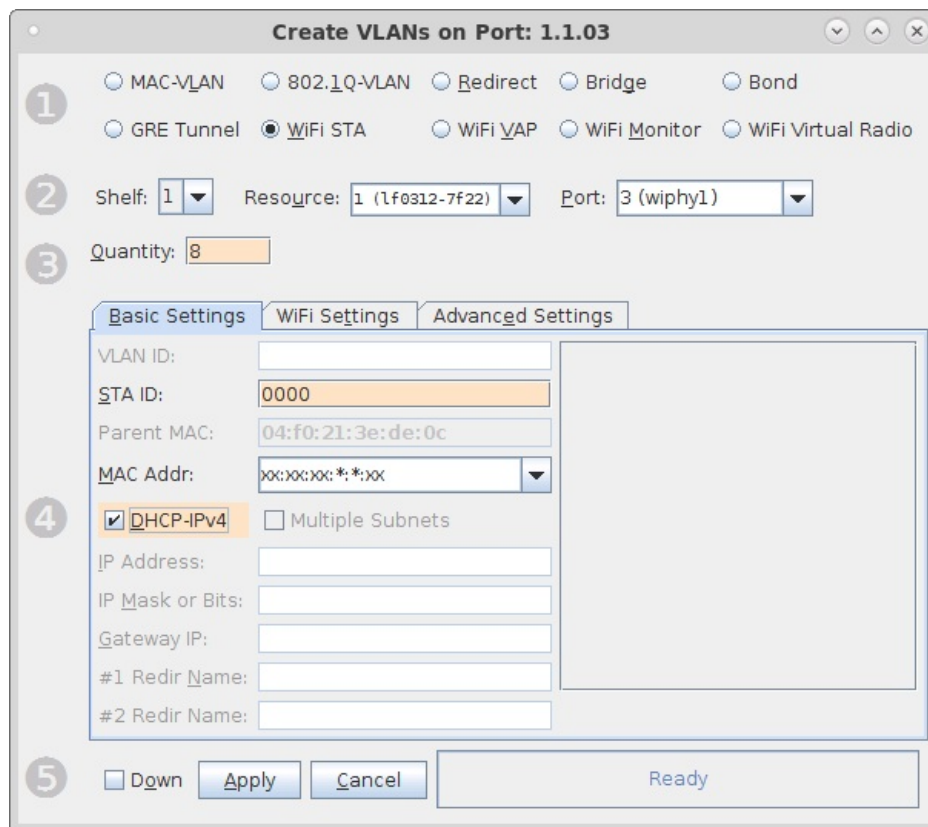
```
Mate Terminal
File Edit View Search Terminal Help
[root@lf0350-6b3c ~]# pgrep radiusd
1125
[root@lf0350-6b3c ~]# radtest testuser testpasswd 127.0.0.1:1812 0 lanforge
Sent Access-Request Id 90 from 0.0.0.0:14347 to 127.0.0.1:1812 length 78
  User-Name = "testuser"
  User-Password = "testpasswd"
  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.



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

A. Create stations.



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
- IP Address: 0.0.0.0
- IP Mask: 0.0.0.0
- Gateway IP: 0.0.0.0
- Alias:
- MAC Addr: 04:f0:21:02:17:0c
- Rpt Timer: faster (1 s)
- IPSec GW: 0.0.0.0
- IPSec Local ID.:
- DHCP Hostname: None
- DHCP Vendor ID: None
- DHCP Client ID: None
- Peer IP: NA
- Global IPv6: AUTO
- Link IPv6: AUTO
- IPv6 GW: AUTO
- MTU: 1500
- TX Q Len: 1000
- WiFi Bridge: NONE
- IPSec Password:
- IPSec Remote ID.:

WiFi Settings

- SSID: [BLANK] AP: DEFAULT
- Key/Phrase: [?] Mode: 802.11abgn-AC
- Freq/Channel: 0/0 Rate: 0S 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

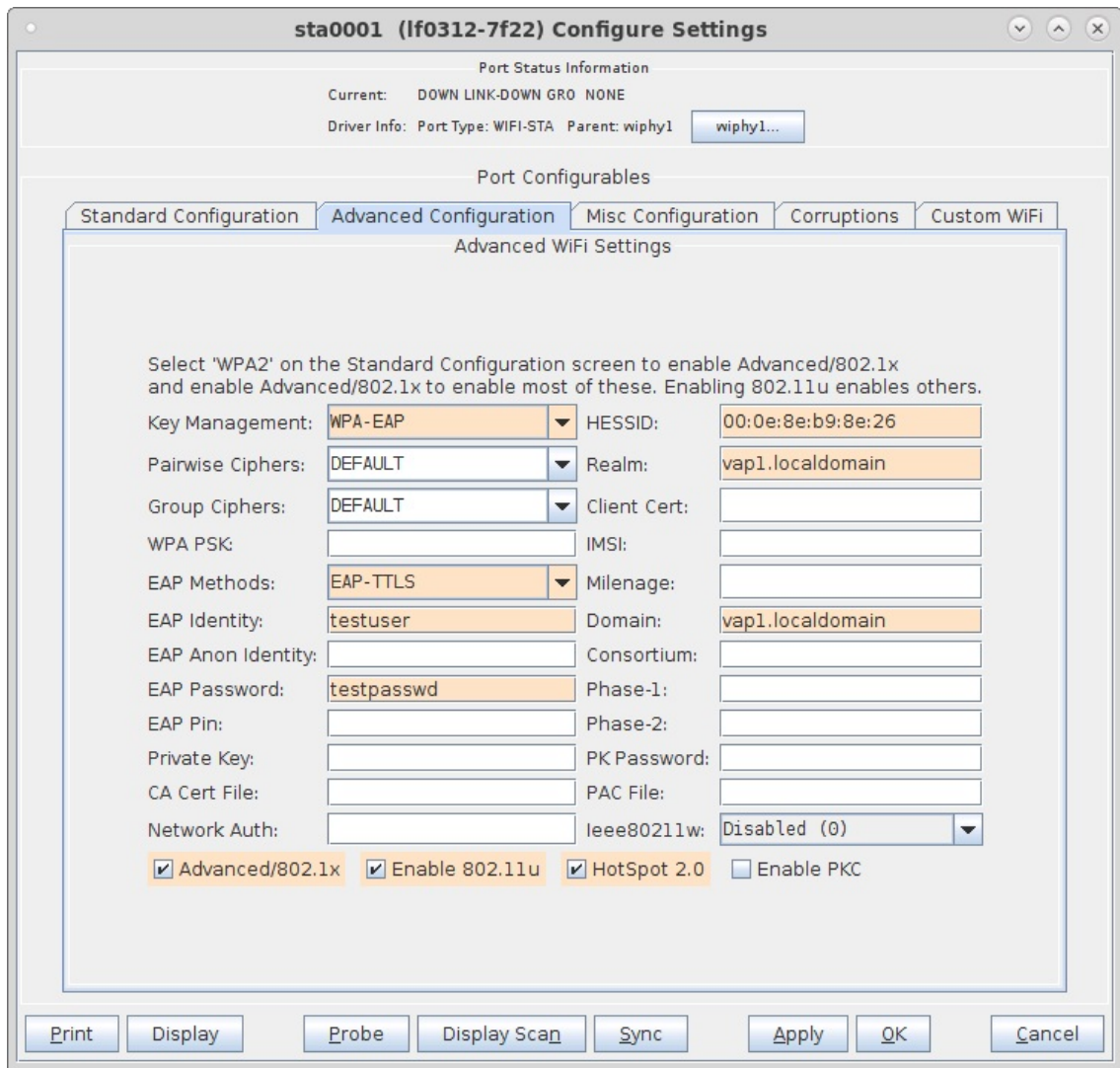
Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

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)

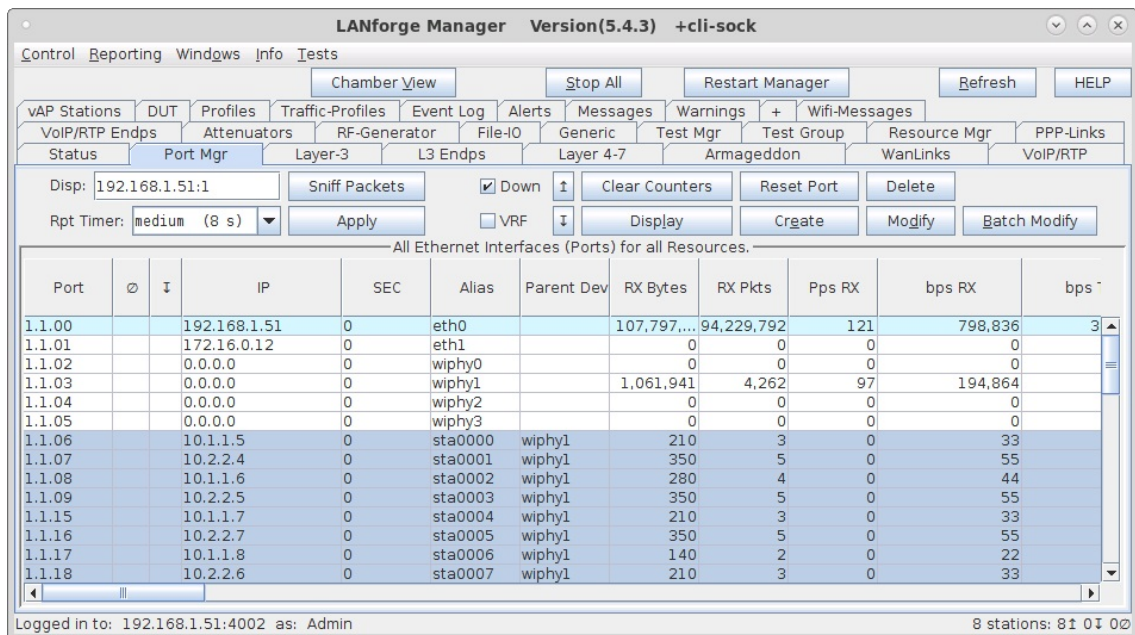
Advanced/802.1x Enable 802.11u HotSpot 2.0 Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

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



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



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