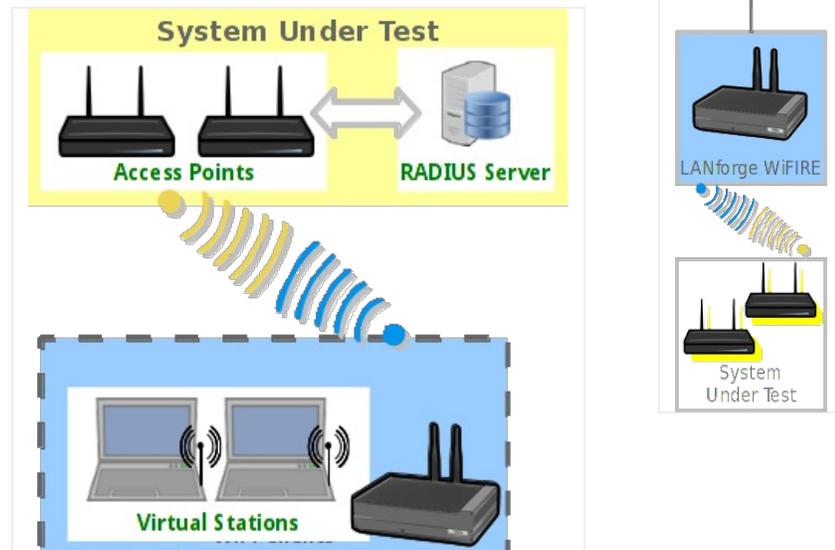


LANforge WiFi testing with HotSpot 2.0

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

Requires LANforge 5.2.10 or later. Create a Virtual AP configured for HotSpot 2.0 and RADIUS (802.1x) authentication. Create two Station interfaces, one connecting with EAP-TLS and one with EAP-TTLS. This example uses two LANforge CT520 systems but the procedure should work on all CT521, CT522, CT523, CT525 and similar systems.



1. Create a virtual AP on wiphy0 of Resource 1. (Skip this if you are using your own AP)
 - A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create basic Virtual AP interface.

- B. The new VAP should appear in the Port-Mgr table. Double-click to modify. Configure IP Address information, SSID and select WPA2:

vap1 (If0301-1n-f17-32) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy0

Port Configurables

Standard Configuration | **Advanced Configuration** | Misc Configuration

Enable

- 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: BLANK Peer IP: NA
- IP Address: 10.97.1.1 Global IPv6: AUTO
- IP Mask: 255.255.0.0 Link IPv6: AUTO
- Gateway IP: 0.0.0.0 IPv6 GW: AUTO
- Alias: MTU: 1500
- MAC Addr: 00:0e:8e:c3:19:79 TX Q Len: 1000
- Rpt Timer: medium (8 s) WiFi Bridge: NONE

WiFi Settings

- SSID: ABCD-1234 AP: DEFAULT
- Key/Phrase: Mode: 802.11abgn
- Freq/Channel: 5745/149 Rate: OS Default
- DTIM-Period: 2 Max-STA: 2007
- Beacon: 240
- Use WPA Use WPA2 Use WEP Disable HT40 Disable SGI
- Verbose Debug

Print View Details Logs 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, RADIUS and other information. The RADIUS server can be the LANforge machine when freeradius is installed via `lf_install.pl --do_radius ...` then just copy the `client.p12` and `ca.pem` from the `/home/lanforge/` directory on the RADIUS LANforge machine to the Station machine(s) and configure the stations to use those key files. Or, use your own RADIUS server and copy key files as appropriate:

vap1 (If0301-1n-f17-32) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy0

Port Configurables

Standard Configuration | **Advanced Configuration** | Misc Configuration

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.

- Ignore Probes: zero (0%) HESSID: 00:00:00:00:00:01
- Ignore Auth-Assoc: zero (0%) Realm: 0,lanforge.com,13[5:6],21[2:4][5:7]
- Ignore Assoc: zero (0%) IMSI:
- Ignore Re-Assoc: zero (0%) Milenage:
- Corrupt GTK: zero (0%) Domain: lanforge.com
- HS20 Capabilities Consortium:
- HS20 Oper Class: 517C RADIUS IP: 127.0.0.1
- HS20 WAN Metrics: 01:8000:1000:80:240:3000 RADIUS Port: 1812
- IEEE80211w: Disabled (0) RADIUS Secret: lanforge
- Venue Group: Business (2) Venue Type: Private Residence (1)
- Network Type: Personal (4) Address Types: Public IPv4 (4)
- Network Auth: 00 3GPP Cell Net: 244,91;310,026;234,56
- Use 80211d Use 80211h Short-Preamble
- Advanced/802.1x HotSpot 2.0 Disable DGAF
- Enable 802.11u 802.11u Internet 802.11u ASRA 802.11u ESR 802.11u UESA

Print View Details Logs Probe Display Scan Sync Apply OK Cancel

- D. Use NetSmith to create Virtual-Router. Add the vapX interface to the Virtual router, configure the Virtual Router port object to serve DHCP. Optionally, add external Ethernet interface to virtual router so that it can route to upstream networks. You could also set up the VAP in bridge mode and use external DHCP server if preferred.

For more information see [LANforge User's Guide: Ports \(Interfaces\)](#) , [VAP Bridge Mode Cookbook](#) , [Virtual Router with DHCP Cookbook \(Skip the WanLink portion\)](#)

2. Create EAP-TLS (key certificate authentication) Station on wiphy0 of the second LANforge Resource.
- A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create a basic Virtual Station interface.
- B. The new Station should appear in the Port-Mgr table. Double-click to modify. Select WPA2. The SSID and Key/Password do not need to be configured when using HotSpot 2.0:

wlan0 (ct523-3n-f20) Configure Settings

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

Port Configurables

Standard Configuration | **Advanced Configuration** | **Misc Configuration**

Enable

- 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: **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: **00:0e:8e:30:9d:69** 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: **5745/149** Rate: **OS Default**
- Use WPA Use WPA2 Use WEP Disable HT40 Disable SGI

Print **View Details** **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** is required, but it may not matter what value you enter unless your RADIUS server has specific requirements. The LANforge RADIUS server does not care. The **Private Key** and **CA Cert File** should come from the /home/lanforge directory on the RADIUS machine if using LANforge for the RADIUS server, or from your own RADIUS server's machine if using your own RADIUS.

wlan0 (ct523-3n-f20) Configure Settings

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

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration

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: 00:00:00:00:00:00
 Pairwise Ciphers: CCMP TKIP Realm: lanforge.com
 Group Ciphers: All Client Cert:
 WPA PSK: IMSI:
 EAP Methods: EAP-TLS Milenage:
 EAP Identity: lanforge Domain: lanforge.com
 EAP Anon Identity: Consortium:
 EAP Password: Phase-1:
 EAP Pin: Phase-2:
 Private Key: /home/lanforge/client.p12 PK Password: lanforge
 CA Cert File: /home/lanforge/ca.pem PAC File:
 Network Auth: leee80211w: Disabled (0)

Advanced/802.1x Enable 802.11u HotSpot 2.0 Enable PKC

Print View Details Probe Display Scan Sync Apply OK Cancel

- D. Verify Station connects and obtains DHCP IP Address configuration.

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

3. Create EAP-TTLS (802.1x username + password authentication) Station on wiphy0 of the second LANforge Resource.
- A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create another basic Virtual Station interface.

- B. The new Station should appear in the Port-Mgr table. Double-click to modify. Select WPA2. The SSID and Key/Password do not need to be configured when using HotSpot 2.0:

The screenshot shows the configuration window for wlan1. The 'Port Status Information' section indicates the port is 'LINK-UP GRO Authorized' with 'Driver Info: Port Type: WIFI-STA Parent: wiphy1'. The 'Port Configurables' section has three tabs: 'Standard Configuration', 'Advanced Configuration', and 'Misc Configuration'. The 'Standard Configuration' tab is active, showing a list of checkboxes for 'Enable' (Set IF Down, Set MAC, Set TX Q Len, Set MTU, Set Offload, Set PROMISC), 'Services' (HTTP, FTP), and 'Low Level' (PROMISC, TSO Enabled, UFO Enabled, GSO Enabled, LRO Enabled, GRO Enabled). The 'General Interface Settings' section includes checkboxes for DHCP-IPv6, DHCP Release, Down, and Aux-Mgt. It also has fields for DHCP-IPv4, DNS Servers, IP Address, IP Mask, Gateway IP, Alias, MAC Addr, Rpt Timer, Secondary-IPs, DHCP Client ID, Peer IP, Global IPv6, Link IPv6, IPv6 GW, MTU, TX Q Len, and WiFi Bridge. The 'WiFi Settings' section includes fields for SSID, Key/Phrase, Freq/Channel, AP, Mode, Rate, and checkboxes for Use WPA, Use WPA2, Use WEP, Disable HT40, and Disable SGI.

- 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. LANforge RADIUS defaults to: testuser, testpasswd when freeradius is installed via lf_kinstall.pl --do_radius. Phase-2 must be configured as shown for EAP-TLS with MSCHAPV2.

The screenshot shows the configuration window for wlan1 with the 'Advanced Configuration' tab selected. The 'Advanced WiFi Settings' section contains a text instruction: '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.' Below this are various configuration fields: Key Management (WPA-EAP), Pairwise Ciphers (CCMP TKIP), Group Ciphers (All), WPA PSK, EAP Methods (EAP-TLS), EAP Identity (testuser), EAP Anon Identity, EAP Password (testpasswd), EAP Pin, Private Key, CA Cert File, Network Auth, HESSID (00:00:00:00:00:00), Realm (lanforge.com), Client Cert, IMSI, Milenage, Domain (lanforge.com), Consortium, Phase-1, Phase-2 (auth=MSCHAPV2), PK Password, PAC File, and IEEE80211w (Disabled (0)). At the bottom, there are checkboxes for 'Advanced/802.1x', 'Enable 802.11u', 'HotSpot 2.0', and 'Enable PKC'.

- D. Verify Station connects and obtains DHCP IP Address configuration.

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

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