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;
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 `if_kinstall.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:

![LANforge VAP1 Configuration Settings](image)

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)](example), [VAP Bridge Mode Cookbook](example), [Virtual Router with DHCP Cookbook](example) (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 HolSpot 2.0.
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.

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

For more information see WiFi Station Cookbook

3. Create EAP-TLS (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.

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 Identify and EAP Password must match the configuration on your RADIUS server. LANforge RADIUS defaults to: testuser, testpasswd when freeradius is installed via if_kinstall.pl --do_radius. Phase-2 must be configured as shown for EAP-TLS with MSCHAPV2.
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