LANforge WiFi AP and Stations with HS20 and EAP-SIM

**Goal:** Use LANforge to create AP, RADIUS server, and Station that supports HotSpot 2.0 (HS20) and EAP-SIM authentication.

Requires LANforge 5.2.11 or later. Create a Virtual AP configured for HotSpot 2.0 and RADIUS (802.1x) authentication. Create a MAC-VLAN interface to act as RADIUS server using hostapd. Configure back-end tools authenticate EAP-SIM. Create and configure LANforge WiFi station to test authentication. This example uses two LANforge CT520 systems but the procedure should work on all CT521, CT522, CT523 and CT525 systems. Information here should be useful for non-LANforge users creating their own AP using the hostapd program.

This example uses LANforge for all components, so it is both the test gear and the system under test. This cookbook is primarily intended to record information on how to set up various components of an HS20 EAP-SIM network for demo purposes. Users may choose to implement sub-sections of this cookbook and replace others with third-party APs, RADIUS servers, etc.

1. Create a virtual AP on wiphy0 of Resource 1.
   
   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. Note that the 3GPP Cell Net entry must correspond to the IMSI we enter as the station’s identity and the IMSI information in the hl_auc_gw config file. Also, note that the Realm must contain the EAP Method Type 18 (EAP-SIM) as described in [http://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml#eap-numbers-4](http://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml#eap-numbers-4).

D. Use NsMith 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.

E. For those doing this manually, the hostapd.conf file looks like this:

```bash
interface=vap1
driver=nl80211
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_vap0.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ssid=ABCD-1234
bssid=00:0e:8e:c3:19:79
country_code=US
ieee80211n=1
ieee80211h=0
ieee80211w=0
hw_mode=a
wmm_enabled=1
wmm_ac_bk_cwmin=4
```

D. Use NsMith 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.

E. For those doing this manually, the hostapd.conf file looks like this:

```bash
interface=vap1
driver=nl80211
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_vap0.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ssid=ABCD-1234
bssid=00:0e:8e:c3:19:79
country_code=US
ieee80211n=1
ieee80211h=0
ieee80211w=0
hw_mode=a
wmm_enabled=1
wmm_ac_bk_cwmin=4
```
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 a MAC-VLAN interface on eth1 of Resource 1 to act as RADIUS server.
   A. Go to the Port Manager tab, select eth1 on the proper resource, click Create, fill out appropriate information and create a basic MAC-VLAN interface.
B. The new interface should appear in the Port-Mgr table. Double-click to modify. Configure IP Address information and select the RADIUS checkbox which will allow a hostapd based RADIUS server on the interface using the config file /home/lanforge/wifi/hostapd_eth1#0.conf:

```
interface=eth1#0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
#dump_file=/home/lanforge/wifi/hostapd_eth1#0.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/hostapd.eap_user
server_id=lf0301.mytest.com
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients
cia_cert=/etc/raddb/certs/ca.pem
server_cert=/etc/raddb/certs/server.pem
private_key=/etc/raddb/certs/server.key
private_key_passwd=lanforge
```

C. We are just using LANforge to start/stop the hostapd process associated with the MAC-VLAN interface. All interesting configuration is in the custom config file, which should appear similar to this:

```
interface=eth1#0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
#dump_file=/home/lanforge/wifi/hostapd_eth1#0.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/hostapd.eap_user
server_id=lf0301.mytest.com
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients
cia_cert=/etc/raddb/certs/ca.pem
server_cert=/etc/raddb/certs/server.pem
private_key=/etc/raddb/certs/server.key
private_key_passwd=lanforge
```

D. Create RADIUS client authentication file on the LANforge machine called /etc/hostapd.radius_clients with contents similar to:

```
192.168.100.0/24 lanforge
127.0.0.1/24 lanforge
```

E. Create the /etc/hostapd.eap_user file, with contents similar to this:

```
"*@mytest.com" TLS
"0"* SIM,TTLS,TLS,PEAP,AKA
"1"* SIM,TTLS,TLS,PEAP,AKA
```

3. Configure back-end authenticator for EAP-SIM.
A. On the LANforge machine, use your favorite editor to create the file /etc/hlr_auc_gw.milenage_db 
   It should have contents similar to:

   # Parameters for Milenage (Example algorithms for AKA).
   # The example Ki, OPC, and AMF values here are from 3GPP TS 35.208 V6.0.0
   # 4.3.20 Test Set 20. SQN is the last used SQN value.
   # These values can be used for both UMTS (EAP-AKA) and GSM (EAP-SIM)
   # authentication. In case of GSM/EAP-SIM, AMF and SQN values are not used, but
   # dummy values will need to be included in this file.
   # IMSI Ki OPC AMF SQN
   # These values are from Test Set 19 which has the AMF separation bit set to 1
   # and as such, is suitable for EAP-AKA test.
   # These values are from Test Set 20 which has the AMF separation bit set to 1
   # and as such, is suitable for EAP-AKA test.

   IMSI Ki OPC AMF SQN
   2320100000000000 90dca4eda45b53cf0f12d7c9c3b6a89 cb9cccc4b9258e6dca476079f82581 61df 000000000000
   3244433222111 5122502143ce723a5dd523fc145fc0 981d464c7c52eb6e5036234984ad0bcf c3ab 16f3b3f70fc1

   NOTE: If the hlr_auc_gw does not start, you may have to remove the file /tmp/hlr_auc_gw.sock first.

B. As root user, start the hlr_auc_gw tool:

   ```
   cd /home/lanforge
   . lanforge.profile
   hlr_auc_gw -m /etc/hlr_auc_gw.milenage_db > /tmp/hlr_auc_gw.log &
   ```

C. In the LANforge GUI, select the MAC-VLAN interface [eth1] [0 in our example] and click Reset to restart the hostapd RADIUS process now that the hlr_auc_gw program is running.

4. Create WiFi Station on second wiphy (and/or second LANforge) to test connectivity
   A. Go to the Port Manager tab, select wiphyX 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. Set the SSID to [BLANK]. 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 Identity and EAP Password must match the configuration on your RADIUS server, and in this case, that means it must match the hir_auc_gw configuration we entered earlier. The HS20 Realm and Domain should be configured to match the HS20 AP.

D. Verify Station connects to the AP and obtains DHCP IP Address configuration. If it does not work, look at the Station’s supplicant logs, the AP logs, the RADIUS server logs, and the hir_auc_gw logs.

E. For those doing this manually, the wpa_supplicant.conf file looks like this:

```plaintext
ctrl_interface=/var/run/wpa_supplicant
fast_reauth=1
concurrent_assoc_ok=1
scan_cur_freq=1
min_scan_gap=5
p2p_disabled=1

# 802.11u / Interworking configuration.
interworking=1
hessid=00:00:00:00:00:33
auto_interworking=1
access_network_type=0

# HotSpot 2.0 configuration
hs2b=1
bss_max_count=2000

network={
    interworking_defaults=1
    disable_ht=0
    disable_vht=1
    disable_ht40=0
    disable_sgi=0
    ht_mcs=""
    disable_max_amsdu=-1
    ampdu_factor=-1
    ampdu_density=-1
}

cred={
    username="1232010000000000@mytest.com"
    password="90dca4eda45b53cf012d7c3b6a89:cb9ccc4b92586edca4760379f82581"
    realm="mytest.com"
    domain="mytest.com"
    eap=SIM
}
```

For more information see WiFi Station Cookbook.