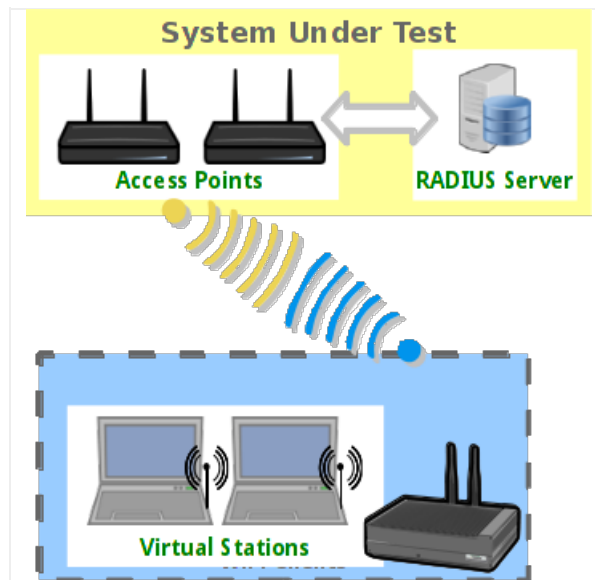


LANforge WiFi AP and Stations with HS20 and EAP-AKA

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

Requires LANforge 5.2.11 or later. Create a Virtual AP configured for HotSpot 2.0 and RADIUS (802.1x) authentication. Create second dummy AP to act as RADIUS server using hostapd. Configure back-end tools authenticate EAP-AKA. 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-AKA 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:

The screenshot shows the 'vap1 (If0301-1n-f17-32) Configure Settings' window. The 'Port Status Information' section shows 'Current: LINK-UP GRO NONE' and 'Driver Info: Port Type: WIFI-AP Parent: wiphy0'. The 'Port Configurables' section has three tabs: 'Standard Configuration', 'Advanced Configuration', and 'Misc Configuration'. The 'Standard Configuration' tab is active, showing 'Enable' options (Set IF Down, Set MAC, Set TX Q Len, Set MTU, Set Offload, Set PROMISC), 'Services' (HTTP, FTP), and 'Low Level' options (PROMISC, TSO Enabled, UFO Enabled, GSO Enabled, LRO Enabled, GRO Enabled). The 'General Interface Settings' section includes 'DHCP-IPv6', 'DHCP-IPv4', 'Secondary-IPs', 'DNS Servers', 'IP Address', 'IP Mask', 'Gateway IP', 'Alias', 'MAC Addr', 'Rpt Timer', 'DHCP Release', 'Down', 'Aux-Mgt', 'DHCP Client ID', 'Peer IP', 'Global IPv6', 'Link IPv6', 'IPv6 GW', 'MTU', 'TX Q Len', and 'WiFi Bridge'. The 'WiFi Settings' section includes 'SSID', 'Key/Phrase', 'Freq/Channel', 'DTIM-Period', 'Beacon', 'AP', 'Mode', 'Rate', 'Max-STA', 'Use WPA', 'Use WPA2', 'Use WEP', 'Disable HT40', 'Disable SGI', and 'Verbose Debug'.

- 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 hlr_auc_gw config file:

The screenshot shows the 'vap1 (If0301-1n-f17-32) Configure Settings' window, now with the 'Advanced Configuration' tab selected. The 'Advanced WiFi Settings' section includes a note: '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 'Ignore Probes', 'Ignore Auth-Assoc', 'Ignore Assoc', 'Ignore Re-Assoc', 'Corrupt GTK', 'HS20 Capabilities', 'HS20 Oper Class', 'HS20 WAN Metrics', 'Ieee80211w', 'Venue Group', 'Network Type', 'Network Auth', 'HESSID', 'Realm', 'IMSI', 'Milenage', 'Domain', 'Consortium', 'RADIUS IP', 'RADIUS Port', 'RADIUS Secret', 'Venue Type', 'Address Types', and '3GPP Cell Net'. The 'Advanced/802.1x', 'HotSpot 2.0', 'Enable 802.11u', '802.11u Internet', '802.11u ASRA', '802.11u ESR', and '802.11u UESA' options are checked.

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

```
interface=vap0
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=ben-138
bssid=80:01:02:03:04:05
country_code=US
ieee80211d=1
hw_mode=a
ieee80211n=1
beacon_int=240
dtim_period=2
max_num_sta=2007
rts_threshold=2347
fragm_threshold=2346
preamble=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
# Enable HT modes if you want 300Mbps+ throughput.
#ht_capab=[HT20][HT40-][HT40+][GF][SHORT-GI-20][SHORT-GI-40]
# [TX-STBC][RX-STBC123][MAX-AMSDU-7935][DSSS_CCK-40][PSMP][LSIG-TXOP-PROT]
ht_capab=[HT20][HT40+][SHORT-GI-40][SHORT-GI-20]
#vht_capab=[HT20][HT80+][HT80-][SHORT-GI-80]
wmm_enabled=1
wmm_ac_bk_cwmin=4
wmm_ac_bk_cwmax=10
wmm_ac_bk_aifs=7
wmm_ac_bk_txop_limit=0
wmm_ac_bk_acm=0
wmm_ac_be_aifs=3
wmm_ac_be_cwmin=4
wmm_ac_be_cwmax=10
wmm_ac_be_txop_limit=0
wmm_ac_be_acm=0
wmm_ac_vi_aifs=2
wmm_ac_vi_cwmin=3
wmm_ac_vi_cwmax=4
wmm_ac_vi_txop_limit=94
wmm_ac_vi_acm=0
wmm_ac_vo_aifs=2
wmm_ac_vo_cwmin=2
wmm_ac_vo_cwmax=3
wmm_ac_vo_txop_limit=47
wmm_ac_vo_acm=0
channel=36
ieee8021x=1
own_ip_addr=127.0.0.1
auth_server_addr=127.0.0.1
auth_server_port=1812
auth_server_shared_secret=lanforge
wpa=2
wpa_pairwise=CCMP
wpa_key_mgmt=WPA-EAP
# 802.11u configuration
interworking=1
access_network_type=4
internet=1
asra=1
```

```

esr=1
uesa=1
venue_group=2
venue_type=1
hessid=00:00:00:00:00:01
roaming_consortium=01010101
venue_name=eng:LANforge Test Venue
network_auth_type=00
ipaddr_type_availability=04
domain_name=lanforge.org
anqp_3gpp_cell_net=055,54
nai_realm=0,lanforge.org,13[5:6],21[2:4][5:7]
# HotSpot 2.0 configuration
hs20=1
hs20_oper_friendly_name=eng:LANforge HotSpot 2.0
hs20_wan_metrics=01:8000:1000:80:240:3000
hs20_operating_class=517C

```

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 dummy virtual AP on wiphy0 of Resource 1 to act as RADIUS server.
 - 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:

vap2 (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: 10.20.1.1 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:84:81:79 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
- DTIM-Period: 2 Max-STA: 2007
- Beacon: 240
- ☐ Use WPA ☒ Use WPA2 ☐ Use WEP ☐ Disable HT40 ☐ Disable SGI
- ☒ Verbose Debug

Buttons: Print View Details Logs Probe Display Scan Sync Apply OK Cancel

- C. Select the **Misc Configuration** tab in the Port-Modify window and select **Custom WPA Cfg** and specify the **WPA Cfg** file name:

The screenshot shows a window titled "vap2 (If0301-1n-f17-32) Configure Settings". At the top, "Port Status Information" shows "Current: LINK-UP GRO NONE" and "Driver Info: Port Type: WIFI-AP Parent: wiphy0". Below this is the "Port Configurables" section with three tabs: "Standard Configuration", "Advanced Configuration", and "Misc Configuration". The "Misc Configuration" tab is active, showing "More WiFi Settings". In this section, "Freq-2.4" and "Freq-5" are both set to "0xffffffff". "X-Coordinate" and "Z-Coordinate" are set to "0". "Y-Coordinate" is set to "0". The "Post IF-UP Script:" field is empty. The "Custom WPA Cfg" checkbox is checked, and the "WPA Cfg:" field contains the path "/home/lanforge/hostapd_vap2_radius.conf". The "Skip Portal on Roam" checkbox is unchecked. At the bottom of the window are buttons for "Print", "View Details", "Logs", "Probe", "Display Scan", "Sync", "Apply", "OK", and "Cancel".

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

```
interface=eth0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_vap2.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=1f138.lanforge.com
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients
```

- E. Create RADIUS client authentication file named **/etc/hostapd.radius_clients** with contents similar to:

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

- F. Create RADIUS eap user file named **/etc/hostapd.eap_user** file, with contents similar to this:

```
"*@lanforge.com" TLS
"0"* AKA
"2"* AKA
"4"* AKA
```

3. Configure back-end authenticator for EAP-AKA.

- 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
232010000000000 90dca4eda45b53cf0f12d7c9c3bc6a89 cb9cccc4b9258e6dca4760379fb82581 61df 000000000000

# 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.
55544333222111 5122250214c33e723a5dd523fc145fc0 981d464c7c52eb6e5036234984ad0bcf c3ab 16f3b3f70fc1
```

- 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 dummy vap (vap2 in our example) and click **Reset** to restart the 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], and Select WPA2. The SSID and Key/Password do not need to be configured when using HotSpot 2.0:

The screenshot shows the 'sta1 (ct523-3n-f20) Configure Settings' window. At the top, it displays 'Port Status Information' with 'Current: LINK-UP GRO Authorized' and 'Driver Info: Port Type: WIFI-STA Parent: wiphy0'. Below this is the 'Port Configurables' section with three tabs: 'Standard Configuration', 'Advanced Configuration', and 'Misc Configuration'. The 'Standard Configuration' tab is selected, showing a list of checkboxes on the left (Set IF Down, Set MAC, Set TX Q Len, Set MTU, Set Offload, Set PROMISC, HTTP, FTP, PROMISC, TSO Enabled, UFO Enabled, GSO Enabled, LRO Enabled, GRO Enabled) and a 'General Interface Settings' panel on the right. The 'General Interface Settings' panel includes fields for DNS Servers, IP Address, IP Mask, Gateway IP, Alias, MAC Addr, Rpt Timer, DHCP-IPv6, DHCP Release, DHCP Client ID, Peer IP, Global IPv6, Link IPv6, IPv6 GW, MTU, TX Q Len, and WiFi Bridge. The 'WiFi Settings' panel at the bottom shows SSID set to '[BLANK]', AP set to 'DEFAULT', Key/Phrase set to an empty field, Mode set to '802.11abgn', Freq/Channel set to '5745/149', Rate set to 'OS Default', and checkboxes for 'Use WPA', 'Use WPA2' (checked), 'Use WEP', 'Disable HT40', and 'Disable SGI'. At the bottom of the window are buttons for 'Print', 'View Details', 'Probe', 'Display Scan', 'Sync', 'Apply', 'OK', and '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, and in this case, that means it must match the hlr_auc_gw configuration we entered earlier. The HS20 Realm and Domain should be configured to match the HS20 AP.

sta1 (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-AKA Milenage:
 EAP Identity: 0555444333222111@lanforge.com Domain: lanforge.com
 EAP Anon Identity: Consortium:
 EAP Password: 5122250214c33e723a5dd523fc145fc0:981d464c7c52eb6e5036234984ad0bcf:16f3b3f70fc1 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 View Details Probe Display Scan Sync Apply OK Cancel

- 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 hlr_auc_gw logs.

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

```
ctrl_interface=/var/run/wpa_supplicant
fast_reauth=1
can_scan_one=1
# 802.11u / Interworking configuration.
interworking=1
auto_interworking=1
access_network_type=0
# HotSpot 2.0 configuration
hs20=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="0555444333222111@wlan.org"
    password="5122250214c33e723a5dd523fc145fc0:981d464c7c52eb6e5036234984ad0bcf:16f3b3f70fc1"
    realm="lanforge.org"
    domain="lanforge.org"
    eap=AKA
}
```

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