LANforge WiFIRE Cookbook

The LANforge WiFIRE Cookbook provides a set of high-level examples of how to setup useful test scenarios in LANforge-FIRE for WiFi traffic generation. Each example intends to give the reader a brief introduction to the test scenario and a set of step-by-step instructions on how to use the LANforge-GUI to configure the test.

All of the following examples will work on Linux systems running the LANforge software with the LANforge kernel and a sufficient license. If you are running another Linux kernel, you will not be able to exactly duplicate some of the examples, but there are usually work-arounds available to assist you. Please contact us at support@candelatech.com if you have any questions.

If you are using the Windows version of LANforge, you will have to modify parts using the Windows utilities.

LANforge WiFIRE WiFi Traffic Generation

Before attempting the examples below, ensure that you have successfully followed these software installation guides:

- LANforge-GUI Installation
- LANforge Server Installation

It is also recommended that you back up your current running LANforge Server database so that you may safely return to your current operating state.

Quick Examples

- LANforge-FIRE Examples
- LANforge WiFIRE Wireless Testing Examples
1. AP Testing: Basic AP Testing
2. AP Testing: Jamming a channel with CT523
3. UE Testing: Create VAP in Bridge Mode
4. UE Testing: Create Routed VAP to Ethernet
5. AP Testing: Station performance for 1, 50, and 128 stations
6. AP Testing: Multicast download test
7. UE Testing: Configuring a Virtual AP with Limited Stations
8. UE Testing: WiFi Station Association Code 17
9. Enterprise: HotSpot 2.0 with EAP-TLS and EAP-TTLS
10. Enterprise: Hotspot 2.0 with EAP-AKA
11. Enterprise: Hotspot 2.0 with EAP-SIM
12. Enterprise: Fast Roaming Stations with 802.11r (FT-EAP)
13. Enterprise: Two Access Point Network with 802.11r (FT-EAP)
14. Enterprise: Four Access Point Network with 802.11r (FT-EAP)
15. Enterprise: Roaming with HotSpot 2.0
16. Enterprise: HotSpot 2.0 Release 2
17. AP Testing: Rate v. Range Test
18. AP Testing: Attenuation vs PDU Size Test
19. AP Testing: WiFi Capacity Test
20. AP Testing: Station Reset Test
21. AP Testing: Emulating Degraded Stations
22. AP Testing: Scripted Attenuation of a WiFi Connection
23. AP Testing: External Traffic Generation
25. Captive Portal: Older Captive Portal Login (if_itup_post)
26. UE Testing: Emulating many vAP with one radio for Station DUT testing
27. UE Testing: Emulating a degraded vAP to test Station DUT management frame retry logic
28. AP Testing: Multiple Stations with a Hunt Script
29. UE Testing: Running UDP Traffic with Android
30. UE Testing: Verifying Android QoS
31. UE Testing: ScriptHunt with Test Groups
32. AP Testing: WPS Association
33. AP Testing: Station MU-MIMO performance for 2x2 and 1x1 stations
34. UE Testing: WiFi Capacity Test with Layer 4-7
35. AP Testing: Using Wireshark to Sniff WiFi Monitors
36. AP Testing: Scripting a Standalone CT703 or CT704 Attenuator
37. AP Testing: DFS Testing with CT712 RF Noise Generator and RADAR Simulator
38. video=https://www.youtube.com/watch?v=7LSwWG8g0xQ
39. Packet Capture: WiFi Packet Capture and Diagnostics
40. video=https://www.youtube.com/watch?v=8ZyJWP4e8Fg
41. video=https://www.youtube.com/watch?v=J19dj8-qRw
42. UE Testing: Setting up a RADIUS server
43. UE Testing: Setting up WPA3
44. video=https://www.youtube.com/watch?v=_4i38mr_NB
45. AP Testing: Configure EAP-PEAP and MSCHAPv2
46. Chamber View: Basic AP Testing
47. Chamber View: Receiver Sensitivity Testing with LANforge
48. Chamber View: Dataplane test, throughput over different packet sizes
49. Chamber View: Dataplane test, throughput over different AP orientations
50. Chamber View: Rate vs Range test, throughput over different signal strengths
51. Chamber View: WiFi Capacity Test, throughput with many stations
52. Chamber View: WiFi Station Reset Test
53. Chamber View: Compare multiple APs performance with Dataplane
54. Chamber View: Roam test with 802.11k/v/r
55. Chamber View: Automated tests with script
56. Chamber View: Auto-AP test, automated station capacity, throughput, stability tests
57. Chamber View: Automated TR-398 test, receiver sensitivity, throughput, capacity ...
58. Chamber View: Automated Mesh test topology test
59. Chamber View: Create simple LANforge Access Points
60. Chamber View: Create 802.11k/v/r LANforge Access Point cluster
Generating Traffic for WLAN Testing

Goal: Setup and run Wireless LAN traffic using the LANforge CT523 or similar system.

In this test scenario, the LANforge CT523 is used to simulate 4 virtual wireless stations that associate with a third party access point. Three traffic tests will be configured and run to demonstrate possible wireless access point tests. **NOTE:** This cookbook assumes that you have already created a VAP, and have an interface that is handing out DHCP addresses.

1. Create the virtual wireless stations.

   **Note:** All of its virtual stations will use the same wireless AP in this example, but each station may be configured for a different AP as long as all stations on the same radio use APs on the same channel.
A. Go to the Port Manager

B. Select port wiphy0 and click Create
C. Select the **WiFi STA** button, then enter **MAC**, **Quantity**, **STA ID**, and **SSID**. Select the **DHCP-IPv4** checkbox:

A. In this example, all 4 virtual stations will connect to the same access point.

B. If your access point can serve DHCP, you can select the ‘DHCP-IPv4’ checkbox here to enable each virtual station as a DHCP client.

C. If you choose to enter IP addresses manually, the create function will increment the last octet of the IP address for each virtual station created.

D. Click **Apply** when finished.

D. Verify that the virtual wireless stations are created.
For more information see **LANforge User's Guide: Ports (Interfaces)**
2. Create Layer-3 connections between the station interfaces.
   
   A. Go to the Layer-3 tab and click Create

![Layer-3 connections between station interfaces](image1)

B. Create a station-to-station UDP speed test:

![UDP speed test](image2)

A. **Test 1**: sta0-sta1, UDP, 30Mbps
C. Create a station-to-station TCP speed test:

![TCP speed test interface](image)

A. **Test 1**: sta0-sta1, TCP, 1.54Mbps bi-directional traffic

For more information see [LANforge User's Guide: Layer-3 Cross-Connects (FIRE)](https://example.com).

3. Run traffic tests concurrently, and view results.

A. This example shows little packet loss, however being that this is traffic sent wirelessly via stations, their may be interruptions due to busy channel frequencies, if needed, adjust your Tx rate accordingly.

![Traffic test results](image)
B. The **Layer-3 Endpoints** tab has more detail.

![LANforge Manager Version 5.4.1](image)

C. Select the cross-connects or endpoints and Right-Click → Dynamic Report on the **L3 Endp** or **Layer-3** table to view a live report of the connections.

![Dynamic Reports](image)

For more information see **LANforge User's Guide: Layer-3 Endpoints (FIRE)**

For more information see **LANforge User's Guide: Reporting**
Generating Traffic to saturate a particular WiFi Channel

Goal: Setup and run Wireless LAN traffic using the LANforge CT523 in order to fully saturate a WiFi channel.

In this test scenario, the LANforge CT523 is used to simulate 4 virtual wireless stations on one radio that associate with an access point on the other radio. This allows a single LANforge machine to be a complete WiFi network. Please see the Wifi Testing cookbook example first. These steps assume the configuration from that cookbook is already in place.

1. Create a virtual AP on wiphy1.
A. Go to the Port Manager

B. Select port wiphy1 and click Create

C. Select the WiFi VAP button, then enter MAC, Quantity, STA ID, and SSID. Enter IPv4 address info:
D. Configure the radio’s channel (which will apply to the VAP that was just created). Select the wiphy interface in the Port-Mgr tab and click Modify. Select the channel, and optionally the country-code, and then press Ok. If you elect to change the country code, you must do so on all radios in your system in order for proper function.

For more information see LANforge User’s Guide: Ports (Interfaces)

2. Use the Netsmith feature to create a virtual router and configure DHCP for the AP.
   
   A. Go to the Status tab, and click the Netsmith button for Resource 1.
   
   B. Drag the existing interfaces into a more pleasing layout.
   
   C. Right-Click in empty space and create a new Virtual Router. Just click OK, using the default configuration.
   
   D. Drag the VAP interface into the virtual router and click Apply at the bottom-right of the Netsmith window.
   
   E. Double-click the vap0 icon (which should now be green) to bring up the Create/Modify Connection window.
   
   F. Select the DHCP option, and then fill in the Range Min and Range Max values appropriately.
3. Use Batch-Modify to configure all of the existing WiFi stations to talk to the new AP.
A. Go to the Port-Mgr tab, select sta0, sta1, sta2, and sta3, and then click the Batch Modify button. Configure the SSID to match the AP, and then press OK.

<table>
<thead>
<tr>
<th>Up/Down</th>
<th>NA</th>
<th>DHCP Release</th>
<th>NA</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP-IPv4</td>
<td>NA</td>
<td>DHCP Client ID</td>
<td>NA</td>
</tr>
<tr>
<td>DHCP Vendor ID</td>
<td>NA</td>
<td>MTU</td>
<td>NA</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>NA</td>
<td>IPv6 GW</td>
<td>NA</td>
</tr>
<tr>
<td>Reset Port IP</td>
<td>NA</td>
<td>Global IPv6</td>
<td>NA</td>
</tr>
<tr>
<td>IP Mask</td>
<td>NA</td>
<td>Link IPv6</td>
<td>NA</td>
</tr>
<tr>
<td>Gateway IP</td>
<td>NA</td>
<td>DHCP-IPv6</td>
<td>NA</td>
</tr>
<tr>
<td>MAC</td>
<td>NA</td>
<td>TX Q Len</td>
<td>NA</td>
</tr>
<tr>
<td>Rpt Timer</td>
<td>NA</td>
<td>WiFi Bridge</td>
<td>NA</td>
</tr>
<tr>
<td>FTP</td>
<td>NA</td>
<td>HTTP</td>
<td>NA</td>
</tr>
</tbody>
</table>

| SSID             | test-195-0 | WiFi AP      | NA         |
| Key/Phrase       | NA         | Mode         | NA         |
| Freq/Chan        | RTS        | Rate         | NA         |
| RTS              | AMPDU-Density | Tx-Power | NA         |
| AMPDU-Factor     | NA         | AMPDU-Density | NA         |
| Max-AMSDU        | NA         | br ip        | WA         |
| WPA              | NA         | WPA2         | NA         |
| WEP              | NA         | Disable SGI  | NA         |
| Disable HT40     | NA         | Allow Migration | NA         |
| Scan Hidden      | NA         |              | NA         |
| Verbose Debug    | NA         |              | NA         |
| Post IF-UP Script| NA         |              | NA         |

B. The station interfaces should now get DHCP addresses matching the new AP.

4. Create Layer-3 connections between the station interfaces.
A. Go to the Layer-3 tab. If there are existing connections, stop and/or delete them, and then click Create. Give the test a name, select sta0 and sta1 for ports, set rate to 100M, and set payload size. When complete, press Apply to create the new CX.

B. Create a second UDP connection on sta2 and sta3 interfaces. Change name, change ports, and press OK.

For more information see LANforge User's Guide: Layer-3 Cross-Connects (FIRE)

5. Run traffic tests concurrently, and view results.
A. Select both CXs in the **Layer-3** tab, and click the **Start** button.

B. Go to the **Port-Mgr** tab, scroll to the right, and confirm that the Activity for this channel reports a fairly high percentage.
C. Select the 4 station ports and Right-Click → Dynamic Report on the **Port-Mgr** table to view a live report of the ports.

For more information see **LANforge User's Guide: Reporting**
Create Virtual AP in Bridge Mode

Goal: Create a Virtual AP and set it up to bridge with the wired Ethernet port.

Create a Virtual AP and set it up to bridge with the wired Ethernet port. This example uses the LANforge CTS23 but the procedure should work on all CT521, CT522, CT523, CT525 and similar systems.

1. Create a virtual AP on wiphy1.
   
   A. Go to the Port Manager

   ![Port Manager interface]

   B. Select port wiphy1 and click Create.
C. Select the **WiFi VAP** button, then enter **MAC, Quantity, STA ID, and SSID:**

D. Configure the radio's channel (which will apply to the VAP that was just created). Select the wiphy1 interface in the Port-Mgr tab and click **Modify**. Select the channel, and optionally the country-code, and then press **OK**.

For more information see **LANforge User's Guide: Ports (Interfaces)**

2. Use the Netsmith feature to create a bridge device to hold the VAP and the Ethernet Port.
   
   A. Go to the **Status** tab, and click the **Netsmith** button for Resource 1.
   
   B. Drag the existing interfaces into a more pleasing layout and click **Apply**
C. Right-click in empty space and chose the **New Bridge** option.

D. Enter Quantity **1**, and give it a name such as **br0**, and then click **Apply**

E. Click **SYNC** in the Netsmith window and the **br0** interface should appear.
F. Right-click on the **br0** interface and select **Modify Port**

A. Add **vap0** and **eth1** to the bridge.

B. Click **Apply**, and then **Sync**.
G. Go back to the Netsmith window, and you should see the `br0` device connected to `vap0` and `eth1` with purple lines. If you do not, try clicking once on the `br0` icon to force a re-draw. You now have a VAP in bridge mode. Connect the upstream network to `eth1`, and stations associated with `vap0` will be able to communicate with that upstream network.
Goal: Configure LANforge CT523 or similar with as a virtual access point with access to an ethernet network.

LANforge WiFi systems can be configured as wireless access points that are gateways to wired networks where the wired network is a separate broadcast domain.

1. Configure the gateway port
2. From the Status tab, click Netsmith
3. In the **Netsmith** window, right click the ethernet port connected to the destination network and click **Modify Port**.

4. Configure the gateway port with these settings:
A. DNS Servers: 192.168.100.1
B. IP Address: 192.168.100.43
C. IP Mask: 255.255.255.0
D. Gateway IP: 192.168.100.1
E. Click **OK** to commit changes.

5. In the **Netsmith** window, click **Sync**
6. **NOTE:** It is also possible to assign NAT to the outbound gateway port.
   A. From the **Netsmith** screen, you would right click on **plp1**
   B. Choose **Modify**
   C. Select **NAT**
   D. Click **OK**
   E. Click **Apply** in the **Netsmith** window.

7. Create the virtual access point (AP)
   A. Right click the radio **wiphy0** and select **Create Port**:
B. Configure the AP with these settings:

A. Select WIFI VAP
B. Select a MAC Address: 00:eb:7c:d6:0a:49
C. IP Address: 10.26.1.1
D. IP Mask: 255.255.255.0
E. Gateway IP: 192.168.100.43
F. STA ID: 0
G. SSID: vaptest

C. In the Netsmith window, click Sync

8. In the Netsmith window, right click and select New Router
9. Create a router using default settings; click **OK**.

A. In the **Netsmith** window, click **Apply**

10. Drag **vap0** into the virtual router
11. Drag **plp1** into the virtual router

12. Assign DHCP to the **vap0** port
A. Right click on vap0 and select **Modify**

![Netsmith configuration for Resource: jastk.candelatech.com(1.1) Version: 5.2.11](image)

B. Configure DHCP with these settings:

<table>
<thead>
<tr>
<th>Interface-Cost:</th>
<th>RIP-Metric:</th>
<th>OSPF Area:</th>
<th>VRRP IP:</th>
<th>VRRP ID:</th>
<th>VRRP Priority:</th>
<th>VRRP Interface:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>0.0.0.0</td>
<td>0.0.0.0/24</td>
<td>1</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subnets (a.b.c.d/x):</th>
<th>Next-Hop:</th>
<th>IPv6 Subnets (aaa::x/x):</th>
<th>Next-Hop-ipv6:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3 (pip1)</td>
<td>Skip</td>
<td>Skip</td>
<td>Skip</td>
<td>48000</td>
<td>192.168.100.1</td>
<td>10.26.1.20</td>
<td>10.26.1.50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Should this interface serve DHCP?</th>
<th>OK</th>
<th>Cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A. DHCP DNS: **192.168.100.1**
B. DHCP Range Min: **10.26.1.20**
C. DHCP Range Max: **10.26.1.50**
D. Select **DHCP**
E. Click **OK** to commit the settings.

C. In the **Netsmith** window, click **Apply**

13. **NOTE:** To test this setup, you could use a laptop with WiFi or a desktop system with a USB WiFi dongle to associate with the Virtual AP. If you have a second radio in your LANforge CT523 you could create a virtual station on one of those extra radios, as well.
Test WiFi station upload throughput.

Goal: Test WiFi station upload throughput with various numbers of stations.

Test WiFi station upload throughput with various numbers of stations. This example uses a pair of LANforge CT520 systems, but the procedure should work on all CT521, CT522, CT523, CT525 and similar systems. Encrypted throughput (WPA2) will perform better on the CT523 and higher systems because their CPUs are more powerful. This test assumes you have already created a virtual AP on system 1 and configured it to act as a router and give out DHCP.

1. Test TCP upload throughput with one station (Open)
A. Go to the Port Manager, select the wlan0 interface on the second system, and click Modify. Set the SSID to match the VAP on system 1.

B. Go to Layer-3 tab and click Create to build a TCP connection. Select the Protocol, ports, rates, PDU sizes, Send & Receive buffer sizes.
C. Start the test by selecting the tcp-se row and click Start. Right-click and select Dynamic Report to get a real-time graph of the throughput. We see about 250Mbps of TCP throughput.

2. Test TCP upload throughput with one station (WPA2)
A. Modify the VAP to use WPA2 instead of being open. Go to Port-Mgr tab, select vap0, and click Modify.

B. Configure wlan0 to use the same settings so it can connect to the VAP using WPA2 authentication.

C. Go to the Layer 3 tab, start the tcp-se connection, right-click and select Dynamic Report to get a real-time graph of the throughput. We see about 43Mbps of TCP throughput. LANforge currently does the WPA encryption in software on the CPU, so it is much slower than un-encrypted traffic.

3. Test TCP throughput with 50 stations (Open)

A. Go to the Port-Mgr tab, select the existing wlan0 and vap0 interfaces, click Modify, un-select WPA2 on each of them, and click Apply. This changes wlan0 and vap0 back to Open mode.

B. Go to the Port-Mgr tab, select the wiphy0 interface on the second system, and click Create. Select WiFi STA, enter starting MAC, quantity of 49, select DHCP-IPv4, STA ID of 0, SSID, and Key/Phrase. When properly configured, click Apply.
C. You should now see all 50 stations associated with IP addresses.

D. Go to the Layer-3 tab, modify the `tcp-se` connection. Change the name to tcp-se-0001, and change the RX Endpoint side’s port from wlan0 to sta0. Click OK to create the new connection.

E. Now, create 48 more copies. Modify the tcp-se-0001 connection and click Batch-Create. Set quantity to 48, and Port Increment A to 0. Click Apply to create the 48 TCP connections, one on each of the 48 stations.
F. Select all of the tcp-se connections and click **Start**. Each of the connections are configured for higher rates than the network can actually handle. This is OK, but it will give un-even throughput results on different stations. So, you may wish to change the rate to something lower. If so, go to the **L3 Endps** tab, make sure all of the tcp-se endpoints are selected, and click **Batch Modify**. Select **B Only** since we want to just modify one side of the connection. Set Min Tx Rate to 5Mbps, and click **Apply**.

G. Go back to the **Layer-3** tab and view the running connections.
H. Determine total throughput: Select all of the running connections and then Right-Click and select Calculations. In this scenario, we see about 230Mbps of total TCP throughput.

4. Test TCP upload throughput with 50 stations [WPA2]

   A. Modify the VAP and stations to use WPA2 instead of being open. Go to Port-Mgr tab, select vap0, and all of the stations and click Batch Modify. Change WPA2 to be 'ON' and enter password in the Key/Phrase box. Leave all other values set to 'NA' so they are not changed.
5. Test TCP upload throughput with 128 stations

A. Use similar steps to those described above to create 78 more stations. In the Create VLANs window, use STA ID of 49 and Quantity of 78 this time (since stations 0-48 have already been created). When creating more TCP connections, you can click Modify on the tcp-se-0049 connection and click Batch Create.

B. In this scenario, we see about 36Mbps throughput with TCP in WPA2 mode, and 28Mbps to 40Mbps in Open mode.

Test WiFi Multicast Download.

Goal: Test WiFi Multicast Download.

Test WiFi Multicast Download with a small number of stations. This example uses a pair of LANforge CT520 systems, but the procedure should work on all CT521, CT522, CT523 and CT525 systems. Multicast is a bit special in Wireless networks. Packets are normally transmitted at the lowest rate, so even a small bit of multicast traffic will slow down the entire network. In this example, we will transmit multicast frames from the AP to the stations. Many users will instead use the wired Ethernet port as the transmitter, but aside from the different port, the procedure should be the same. This example assumes you have already created and configured the desired amount of WiFi station interfaces.

1. Create Multicast transmitter on AP interface
A. Go to the L3 Endps tab, and click Create. Set the IGMP Addr, IGMP Dest Port, name, PDU Size, Port, etc and click OK when done.

2. Create Multicast receivers on Station interfaces

A. Go to the L3 Endps tab, and click Create. Set the IGMP Addr, Min IP Port, name, Port. The IGMP Addr and IP Port should match the transmitter. Make sure you also select the ‘Rcv Mcast’ checkbox. Click Apply when done. You can then change the name, change the Port, and click Apply again to create a duplicate endpoint on another station interface.

3. Test throughput

A. Select the Multicast transmitter and receiver endpoints on the L3 Endps tab and click Start. Observe transmit and receive rates, packet-loss, and other statistics to very performance is at expected value.
LANforge WiFi Dual Virtual AP Setup with Limited Stations

Goal: Configure Two virtual APs with a maximum of ten stations each.

Requires at least a two-radio WiFiRE system such as a CT522, CT523 or CT525. This cookbook provides a basic setup to put a Virtual AP on each of two radios. Both APs are operating on separate channels but share the same SSID. We layout a basic constellation of APs in WPA2 mode that quickly fill up and force a station to search multiple channels for a free AP. This is the condition for issuing a Code 17 association refusal. This is not a roaming setup (Wireless Roaming/HS2.0 or 802.11r) because it is not configuring enterprise authentication or roaming specifications.

1. Configure two radios to serve the role of Virtual APs.
A. Start at the **Ports** tab. We will configure our second ethernet port as the upstream port for the virtual APs.

A. Highlight port **eth1** and click **Modify**
B. Set the IP address to **10.26.1.3**
C. and the netmask to **255.255.255.0**
D. with a gateway address of the **10.26.1.2**. (This gateway address matches the eth1 port of a separate system that hosts stations.
E. Click **OK**
B. In the Ports tab, select radios wiphy0, wiphy1 and click Modify. You will get two modify windows that you will want to place side by side.

A. Set the channel of wiphy0 to 36
B. and the channel of wiphy1 to 44
C. Click OK in both windows.

C. Time to create the first virtual AP. In the Ports tab, select wiphy0 and click Create.

A. Select WiFi VAP
B. Enter a MAC address: 00:10:26:02:00:01
C. Quantity is 1
D. IP of 10.26.2.1
E. Let's use a typical subnet mask: 255.255.255.0
F. Gateway IP will be from eth1: 10.26.1.3
G. We will setup WPA2 with the SSID limited-AP and Key/Phrase limited-AP1
H. Click Apply to commit.
I. Click Cancel to close the window.
D. Now craft a second virtual AP. In the **Ports** tab, select **wiphy1** and click **Create**.

A. Select WiFi VAP.
B. Enter a **MAC address**: 00:10:26:03:00:01.
C. **Quantity is 1**.
D. **IP of 10.26.3.1**.
E. And a typical **subnet mask of 255.255.255.0**.
F. **Gateway IP** will be from eth1: 10.26.1.3.
G. We will setup **WPA2 with the SSID Limited-AP and Key/Phrase Limited-AP**.
H. Click **Apply** to commit.
I. Click **Cancel** to close the window.

E. We now have two virtual access points on two radios on separate channels. Each is on their own subnet. Now we limit the number of stations that can connect to them.
F. In the Ports tab, highlight endpoints vap0 and vap1 and click Modify

A. At the bottom of the Port Configure Settings window for vap0, change Max-STA to 10
B. Click OK
C. Repeat this for vap1

2. We now have two virtual access points that can both accept a small number of stations. We put them on different subnets because configuring DHCP on each VAP is simpler than adding a bridge device.

3. Let’s proceed to configuring DHCP for the 10.26.2.0/24 and 10.26.3.0/24 networks.

4. In the Status tab, click on Netsmith
A. Arrange your ports in the **Netsmith** windows and click **Apply**

B. Select **vap0** and right click, choose **Modify**
C. Enable the DHCP pool and the Next-hop for the port

A. Select DHCP
B. Set DHCP Lease Time to 120
C. Set DHCP Range Min to 10.26.2.10
D. Set DHCP Range Max to 10.26.2.250
E. Set Next-Hop to 10.26.1.3
F. Add Subnet 0.0.0.0/0
G. Click OK

D. Click Apply in the Netsmith window to commit the changes to LANforge. If you do not, these changes will disappear.

E. In the Netsmith window, select vap1 and right-click, choose Modify
F. Configure the DHCP pool and the Next-hop for vap1

A. Select DHCP

B. Set DHCP Lease Time to 120

C. Set DHCP Range Min to 10.26.3.10

D. Set DHCP Range Max to 10.26.3.250

E. Set Next-Hop to 10.26.1.3

F. Add Subnet 0.0.0.0/0

G. Click OK

G. Click Apply in the Netsmith window to commit the changes to LANforge.

H. We will create a virtual router to allow upstream traffic to reach the virtual access points:

A. Right click in the Netsmith window and select New Router
B. You will see the Create/Modify Virtual Router window. We can use a default configuration.

C. Click OK to save a default router.

D. Drag the endpoints vap0, vap1 and eth1 into the virtual router, then click Apply in the Netsmith window.
LANforge WiFi Station Association Code 17

Goal: Configure Two virtual APs with a maximum of ten stations each.

This cookbook provides a basic station setup to emulate over-populating an AP with stations. Requires a WiFIRE system such as a CT520 or better than can provide more stations than your AP(s) under test will accept. This is not a roaming setup (Wireless Roaming/HS2.0 or 802.11r) because it is not exercising enterprise authentication or roaming specifications.

1. Set up one AP with a maximum of 10 stations permitted and an SSID of jedtest. (Not shown.)
2. Create 11 stations for SSID jedtest.
A. In the Port Mgr tab, select wiphy0 and click the Create button.

B. In the Create VLANs window, create 21 stations:

A. Select WiFi STA.
B. Select DHCP-IpV4.
D. Then enter 11 for Quantity.
E. STA ID should be 0
F. and SSID will be jedtest for this example.
G. We also will select WPA2
H. ...and click the Apply button.
C. We will see 11 stations in the Port Mgr tab:

D. The stations should start and ten will associate.

E. In the LANforge Wireless Events window, you will see a warning for Association denied.
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.
8. 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.

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.
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:

![Configuration Settings](image)

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, testpass when freeradius is installed via if_kinstall.pl --do_radius. Phase-2 must be configured as shown for EAP-TLS with MSCHAPV2.

![Configuration Settings](image)
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:

![Configuration Settings](image_url)

- **Standard Configuration**
  - **Enable**
  - **Set IP Down**
  - **Set MAC**
  - **Set TX Q Len**
  - **Set MTU**
  - **Set Offload**
  - **Set PROMISC**

- **Advanced Configuration**
  - **DHCP IPv6**
  - **DHCP IPv4**
  - **Secondary-IPs**
  - **DHC Client ID**
  - **DNS Servers**
  - **IP Address**
  - **IP Mask**
  - **Gateway IP**
  - **MTU**
  - **MAC Addr**
  - **Rpt Timer**

- **Misc Configuration**
  - **Aux-Mgt**

- **Low Level**
  - **PROMISC**
  - **TSO Enabled**
  - **UFO Enabled**
  - **GSO Enabled**
  - **LRO Enabled**
  - **GRO Enabled**

- **General Interface Settings**
  - **DHCP Release**
  - **Down**

- **WiFi Settings**
  - **SSID**
  - **Mode**
  - **Freq/Channel**
  - **Rate**
  - **DTIM-Period**
  - **Max-STA**
  - **Beacon**
  - **Use WPA**
  - **Use WPA2**
  - **Use WEP**
  - **Disable HT40**
  - **Disable SGI**
  - **Verbose Debug**

![Network Configuration](image_url)
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
crtl_interface=/var/run/hostapd
crtl_interface_group=0
ssid=ben-138
country_code=US
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-STBC12][MAX-AMSDU-7935][DSSS_CCK-40][PSMP][LSIG-TXOP-PROT]
ht_capab=[HT20][HT40+][SHORT-GI-40][SHORT-GI-20]
#vht_capab=[HT28][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
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:

C. Select the Misc Configuration tab in the Port-Modify window and select Custom WPA Cfg and specify the WPA Cfg file name:
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=lf138.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 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
```

F. Create the `/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 00000000000
5554433322111 512250214c3e7723a9dd523fc145fc0 981d464c7c52e6e5036234984ad0bcf 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.

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.

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
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_amdsu=-1
    ampdu_factor=-1
    ampdu_density=-1

cred=

    username="0555444333222111@wlan.org"
    password="5122259214c33e723a5dd523fc145fc0:981d464c7c52eb6e5036234984ad0bcf:16f3b3f70fc1"
    realm="lanforge.org"
    domain="lanforge.org"
    eap=AKA

```
**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 hlr_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:

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:

```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
country_code=US
hw_mode=a
ieee80211n=1
bssid=00:0e:8e:c3:19:79
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

timeout=0:00:00:00:00:33
mytest.com
lanforge

# 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]
```
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
da_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
da_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 this:

```
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:

```bash
# Parameters for Milenage (Example algorithms for AKA).
# The example Ki, OPc, and AMF values here are from 3GPP TS 35.208 v6.8.0
# 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 cb9ccc4b9258e6dca4760379fb82581 61df 000000000000
55544332222111 512225b214c33e723a5dd523fc145fc0 981d464c752eb6e5036234984ad0bcf c3ab 16f3b3f70fc1
```

B. As root user, start the hlr_auc_gw tool:

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

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

C. In the LANforge-GUI, select the MAC VLAN interface (eth1#0 in our example) and click **Reset** to restart the hapstopd 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:

![StaL (ct523-3n-f20) Configure Settings](image)
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 Identifier 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
cert_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
hs20=1
bss_max_count=2000

network={
    interworking_defaults=1
    disable_ht=0
    disable_vht=1
    disable_ht40=0
    disablesgi=0
    ht_mcs=""
    disable_max_amdsu=1
    ampdu_factor=1
    ampdu_density=1
}

cred={
    username="1232010000000000@mytest.com"
    password="90dca4eda45b53cf6f12d7c9c3b6a89:cb9cccc4b9258e6dca4760379fb82581"
    realm="mytest.com"
    domain="mytest.com"
    eap=SIM
}
```

For more information see WiFi Station Cookbook
LANforge WiFi Testing Fast Roaming Stations with 802.11r

**Goal:** Use automated script to migrate stations between APs and report results.

Requires LANforge 5.2.11 or later. Configure Stations to use FT-EAP (802.11r) and associate them with an 802.11r AP network. Use the 'WiFi Mobility' LANforge-GUI Plugin to automate roaming the stations between the APs. The plugin will create graphs and other reports that can be saved to HTML. This example uses a LANforge CT523 system but the procedure should work on all CT520, CT523 and similar systems.

The two APs under test are on the same channel, so a single radio/NIC on LANforge can roam virtual stations between the APs. But, if the APs were on different channels, only a single station per radio would be supported. Multiple CT523 or other high-density systems can be used to migrate stations between APs on different channels.

1. Configure stations to connect to APs configured for 802.11r. This requires special AP software support and usually an AP Controller (APC).
   A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create desired number of Station interfaces.
B. The new stations should appear in the Port-Mgr table. Double-click to modify one of them. Configure IP Address information, SSID and select WPA2:
C. Select the Advanced Configuration tab in the Port-Modify window and configure the Key Management, Private Key and other values needed to connect to the APs. Be sure to un-select the Restart DHCP on Connect checkbox so that DHCP is not refreshed each time a station roams.

D. Once the single station is connecting properly, use Batch-Modify to configure the rest of the stations to match the first.

For more information see LANforge User’s Guide: Ports (Interfaces)

2. Create VOIP connections between the wired Ethernet eth1 interface and the stations. This will add realistic traffic load to the network under test and allow LANforge to report packet-loss statistics during roaming. The VOIP feature costs extra, so you may wish to use a normal Layer-3 UDP connection which should also provide good reports and a realistic traffic load. The steps below are for VOIP, but Layer-3 would be very similar.
A. Go to the VOIP/RTP tab, click Create, and configure a VOIP connection on eth1 and the first station:

<table>
<thead>
<tr>
<th>Cross Connect Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CX Name:</td>
<td>WTV-001</td>
</tr>
<tr>
<td>Multi Call</td>
<td>☑</td>
</tr>
<tr>
<td>Continuous Call</td>
<td>☑</td>
</tr>
<tr>
<td>Ring Time</td>
<td>20 s</td>
</tr>
<tr>
<td>Max Call Duration</td>
<td>100 s</td>
</tr>
<tr>
<td>Min Call Gap</td>
<td>3 s</td>
</tr>
<tr>
<td>Max Inter Call Gap</td>
<td>3 s</td>
</tr>
<tr>
<td>Codec</td>
<td>G.711u</td>
</tr>
<tr>
<td>CX Type</td>
<td>Voice - SIP</td>
</tr>
</tbody>
</table>

**TX Endpoint (endpoint A):**

- **Endp Name:** WTV-001-A
- **Shelf:** 1
- **Resource:** 1 (61521-925657616)
- **Port:** 2 (1/1)
- **IP Addr:** AUTO
- **Display Name:** 9670135
- **Reg Expire:** 500

**TX File:** mediafemale_voice_4khz.wav

**RX Endpoint (endpoint B):**

- **Endp Name:** WTV-001-B
- **Shelf:** 1
- **Resource:** 1 (61521-925657616)
- **Port:** 1 (eth1)
- **IP Addr:** AUTO
- **Phone #:** AUTO
- **Display Name:** 9670135
- **Reg Expire:** 500

**RX File:** mediafemale_voice_4khz.wav

B. Apply the configuration and make sure the call can complete. Then click Modify on the VOIP connection and use Batch-Create to create one connection for each of the WiFi stations.

C. Select the VOIP and/or Layer-3 connections and start traffic flow. For this example, the connections should remain running while the roaming takes place. It would also be valid to do roaming without any traffic if that is the desired test case.

3. Start the WiFi Migration script.

A. Go to the Port Manager tab, select the stations you wish to roam, right-click and choose the WiFi Mobility menu option.
B. The options at the top default to common values and may not need to be changed. The ports will be automatically configured based on the selection on the Port Manager tab, and can be adjusted before starting the script. The Ports in Use should normally include all stations used in the script. The configuration requiring the most work from the user is the roaming script itself. There is a help section on the left, and a script-entry field on the right. Once the script is written, it should be saved in a text file on the user's PC so that it can easily be pasted into future WiFi Mobility scripts. Some key points are that you must scan about 1 second before roaming or the roam logic in the supplicant process will either fail or do its own roaming. Either way, the results may be worse than if you do the roam properly in the script. It can take a bit of time for LANforge to get all of the data it needs to report on the roam attempt, so it is suggested that stations not roam more often that about once every 10-20 seconds. If reporting is less important, then the stations can roam more often.
C. Once the script is properly configured, click Start to start the roaming. A window will pop up that has live-updating graphs of various reports. A text log is at the bottom for more detailed analysis, and the whole thing can be saved as HTML. The graphs can be scaled and configured through right-click menus if desired. It will take 1-2 complete roam attempts before the graphs are able to show any useful information.

The migration is verified after the Auto-verify timer has expired. If the migration has not completed in that time, it will be counted as failed.
D. Migration totals graphs.

The migration is verified after the Auto-Verify timer has expired. If the migration has not completed by that time, it will be counted as failed.

**Migration Totals**

- Total
- Types: Roam Succeeded, Roam Failed

**Migration Totals per AP**

- DC.A5.4F.3E.9E
- Amount: 104
- DC.A5.F4.4F.4E
- Amount: 101

**Migration Totals per Station**

- 1.sta5
- Amount: 30
- 1.sta6
- Amount: 30
- 1.sta7
- Amount: 30
- 1.sta1
- Amount: 28
- 1.sta2
- Amount: 29
- 1.sta3
- Amount: 29
- 1.sta4
- Amount: 29

**RX Packet Loss Per Roam**
E. Packet Loss graphs.

Migration Script Contents:
```
$oc_c1i scan 1 1 sta1 NA 'trigger freq 5180 5490'
sleep 1
from 1 sta1 dc:a5:f4:ff:df:ae
from 1 sta2 dc:a5:f4:ff:df:ae
from 1 sta3 dc:a5:f4:ff:df:ae
from 1 sta4 dc:a5:f4:ff:df:ae
from 1 sta5 dc:a5:f4:ff:df:ae
from 1 sta6 dc:a5:f4:ff:df:ae
from 1 sta7 dc:a5:f4:ff:df:ae
sleep 20
$oc_c1i scan 1 1 sta1 NA 'trigger freq 5180 5490'
sleep 1
from 1 sta7 dc:a5:f4:ff:df:ae
from 1 sta6 dc:a5:f4:ff:df:ae
from 1 sta5 dc:a5:f4:ff:df:ae
from 1 sta4 dc:a5:f4:ff:df:ae
from 1 sta3 dc:a5:f4:ff:df:ae
from 1 sta2 dc:a5:f4:ff:df:ae
from 1 sta1 dc:a5:f4:ff:df:ae
sleep 20
```
F. Text log with timestamps. Can be coorelated with wpa_supplicant logs and other log files to debug specific roam attempts.
LANforge WiFi Access Point Network with 802.11r

Goal: Configure a virtual AP network with 802.11r to allow testing fast transition (FT) clients.

Configure virtual Access Points to use 802.11r with FT-EAP. This example uses a LANforge CTS23 system but the procedure will work on all CT522, CT523 and CT525 multi-radio systems.

The wifi clients under test are also 802.11r enabled so that they can initiate FT Requests and roam. Here we are using another LANforge WiFi as the system under test to emulate 802.11r stations and force them to roam.

In LANforge, each virtual access point will be running its own hostapd process configured to enable 802.11r and bridged to other virtual access points. The bridged VAP network will emulate the Distributed System (DS) for FT over-the-DS roaming.

1. Setup a single virtual access point on each wifi NIC for at least two NICs and configure them for the same channel and SSID.
   A. Go to the Port Manager tab, select the parent device such as wiphy0, click Modify, set a specific channel/frequency. Repeat for wiphy1.
   B. Select wiphy0, click Create, fill out appropriate information and create a virtual access point. Repeat for wiphy1.
C. The new vap should appear in the Port-Mgr table. Double-click to modify. Configure SSID and select WPA2 but do not fill in the Key/Phrase:
D. Select the **Advanced Configuration** tab in the Port-Modify window and check the box Advanced/802.1x and fill in the RADIUS IP/Port/Secret. Here the RADIUS server will be another instance of hostapd configured on a bridge interface and accessible via localhost.

E. Select the **Custom WiFi** tab in the Port-Modify window to fill in the additional hostapd options to enable and configure 802.11r. These lines will be appended to the end of the LANforge generated hostapd configuration file located in /home/lanforge/wifi of the resource in use.
vap1 00:0e:8e:7e:e2:71 - Your MAC will be different.

wpa_key_mgmt=FT-EAP
tf_over_ds=1
nas_identifier=000e8e7ee271  #vap1 MAC without colon delimiters, yours will differ.
 mobility_domain=ala1
 r0_key_lifetime=10000
 r1_key_holder=000e8e7ee271  #vap1 MAC without colon delimiters, yours will differ.
 reassociation_deadline=1000
 pmk_r1_push=1

#r0kh is vap2 MAC address, vap2 nas identifier, AES key
r0kh=00:0e:8e:cb:fc:48 000e8e7ee271 000102030405060708090a0b0c0d0e0f

#r1kh is vap2 MAC address, vap2 r1 key holder MAC, AES key
r1kh=00:0e:8e:00:0e:cb:fc:48 00:0e:8e:cb:fc:48 000102030405060708090a0b0c0d0e0f

full configuration file: hostapd_vap1.conf

vap2 00:0e:8e:cb:fc:48 - Your MAC will be different.

wpa_key_mgmt=FT-EAP
tf_over_ds=1
nas_identifier=000e8ecbfc48  #vap2 MAC without colon delimiters, yours will differ.
 mobility_domain=ala1
 r0_key_lifetime=10000
 r1_key_holder=000e8ecbfc48  #vap2 MAC without colon delimiters, yours will differ.
 reassociation_deadline=1000
 pmk_r1_push=1

#r0kh is vap1 MAC address, vap1 nas identifier, AES key
r0kh=00:0e:8e:7e:e2:71 000e8e7ee271 000102030405060708090a0b0c0d0e0f

#r1kh is vap1 MAC address, vap1 r1 key holder MAC, AES key
r1kh=00:0e:8e:7e:e2:71 00:0e:8e:7e:e2:71 000102030405060708090a0b0c0d0e0f

full configuration file: hostapd_vap2.conf

In this example, we are configuring push mode key distribution where the master key holder, R0KH, derives
the R1 key for all secondary key holders, R1KH, listed in the configuration file and sends it to them over the DS via bridge interfaces. The R0KH and R1KH entries must be configured for all virtual access points in the 802.11r network.

For more information on hostapd 802.11r configuration, see:

**general hostapd configuration**
https://www.w1.fi/cgit/hostap/plain/hostapd/hostapd.conf

**how to enable wifi roaming**

**802.11r hostapd example**

F. Repeat above steps A-E for vap2 on wiphy1.

2. Create a bridge device for the first virtual access point, vap1. This bridge will be placed inside a virtual router so that it can serve DHCP requests and act as a RADIUS authentication server.

A. Go to the port manager tab, select Create, then select Bridge and enter Quantity 1 and a Bridge Name, then Apply to create the bridge.

```
<table>
<thead>
<tr>
<th>VLAN ID:</th>
<th>Port: 0 (eth0/1MGT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent MAC: 00:90:0b:2d:6a:02</td>
<td></td>
</tr>
<tr>
<td>MAC Addr: 00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>Quantity: 1</td>
<td></td>
</tr>
<tr>
<td>Bridge Name: br0</td>
<td></td>
</tr>
<tr>
<td>STA ID:</td>
<td></td>
</tr>
<tr>
<td>WiFi AP:</td>
<td></td>
</tr>
<tr>
<td>WPA:</td>
<td></td>
</tr>
<tr>
<td>WPA2:</td>
<td></td>
</tr>
<tr>
<td>WEP:</td>
<td></td>
</tr>
</tbody>
</table>
```

Click Apply to finish.
B. Modify the new bridge device to add vap1. Type vap1 in the text entry box, then select Add Ports, then select Apply.

C. Select Sync to verify vap1 is a configured and current bridge member.
D. Go to Netsmith, right-click the bridge and select Modify to add DHCP service. Select the DHCP checkbox at the bottom, then fill in the DHCP Lease Time, DHCP DNS, DHCP Range Min, DHCP Range Max and DHCP Domain if needed, then select OK.

E. Go to Netsmith, right-click in a free area and select New Router and select OK. Then drag the bridge br0 into the virtual router and select Netsmith Apply.

For more information see Virtual Router with DHCP Cookbook (skip the wanlink portion)

3. Add a RADIUS server to the bridge device.

   A. Go to Netsmith, right-click the bridge and select Modify Port to add RADIUS service.
B. Select the RADIUS checkbox, then select OK.

C. Setup the following configuration files to start the RADIUS service. You will need to create these files, but the certificate files can be created by running the if_kinstall script with the --do_radius option.

/etc/hostapd.radius_clients

0.0.0.0/0 lanforge

/etc/hostapd.eap_user

"dot11r.user" PEAP
"dot11r.user" MSCHAPV2 "!!dot11r123" [2]

/home/lanforge/wifi/hostapd_br0.conf

interface=br0
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
eapol_key_index_workaround=0
eap_server=1
eap_user_file=/etc/hostapd.eap_user
server_id=ct523-3n-f20 #Your server_id will be different.
radius_server_auth_port=1812
radius_server_clients=/etc/hostapd.radius_clients
cacert=/etc/raddb/certs/ca.pem
server_cert=/etc/raddb/certs/server.pem
private_key=/etc/raddb/certs/server.key
private_key_passwd=lanforge
D. Verify that there are three hostapd processes running with the command:

```
ps auxww |grep hostapd
```

which should show something similar to the following:

![Image showing command output]

4. Create a second bridge device for the second virtual access point, vap2.
   Each vap in the 802.11r network requires its own bridge so that the bridge device receive logic can correctly process packets from each vap during fast-transition client roaming.

   A. Go to Netsmith, right-click in a free area, select New Bridge, enter Quantity 1 and a Bridge Name, then select Apply. Sync Netsmith to view the new bridge.

![Image showing Bridge configuration]
8. Right-click the new bridge and select Modify Port to add vap2 as a bridge member.

5. Each bridge will share a connection to a redirect device (rdd) pair so that FT messages can be sent and received.

   A. In Netsmith, right-click in a free area and select New Connection to create a rdd pair. Select Skip for Port 1-8, WanLink and Port 2-8 then select OK. Select Netsmith Apply after creating the new connection.
B. Right-click and select Modify Port br0, then add rddVR0 to br0, select Add Ports then select Apply. Your rddVRX numbering may differ depending on what other Netsmith objects are created.
C. Right-click and select Modify Port br1, then add rddVR1 to br1, select Add Ports then select Apply. Your rddVRX numbering may differ depending on what other Netsmith objects are created.

D. The final Netsmith display should show the two bridged virtual access points connected by a rdd pair.
6. Connect clients and force them to roam from vap to vap. This can be accomplished with a wpa_cli command for one or two clients or the Mobility Plugin Script for many clients. If the system under test is not able to force a roam, a variable attenuator on each vap radio may help induce a client to roam as the signal strength from vap to vap is varied.

A. Client connected to vap1.
B. Client roams to vap2.
C. Client roams back to vAP1.
E. A wireless capture of over-the-air packets shows the transition.

F. Output graph of the Mobility Plugin script of several roaming stations.
LANforge WiFi Access Point Network with 802.11r

Goal: Configure four virtual APs in an 802.11r network to test fast transition (FT) clients.

Configure four virtual Access Points to use 802.11r with FT-EAP. This example uses a LANforge CT525 system but a similar procedure will work on all multi-radio systems.

The wifi clients under test are also 802.11r enabled so that they can initiate FT Requests and roam. Here we are using another LANforge WiFire as the system under test to emulate 802.11r stations and force them to roam.

In LANforge, each virtual access point will be running its own hostapd process configured to enable 802.11r and bridged to other virtual access points. The bridged VAP network will emulate the Distributed System (DS) for FT over-the-DS roaming.

1. Setup a virtual access points on a wifi NIC and configure it for a channel and SSID.
A. Go to the Port Mgr tab, select the parent device such as wiphy0, select Create, then fill out appropriate information and create a virtual access point.

B. Modify the new vap, select the Advanced Configuration tab in the Port-Modify window and check the box Advanced/802.1x and fill in the RADIUS IP/Port/Secret. Here the RADIUS server will be a freeradius process configured on localhost. The default RADIUS secret is lanforge and the default login is testuser/testpasswd when freeradius is installed via If_kinstall.pl --do_radius.

C. Repeat above steps A and B to create a single vap on wiphy1, wiphy2 and wiphy3 for a total of four virtual access points.
2. Modify each vap, select the **Custom Wifi** tab and enter the additional lines that will be appended to each vap
hostapd configuration file.

A. For each `vap`, fill in the first 8 lines to enable 802.11r as well as the first part of the 3 `r0kh` entries and 3 `r1kh` entries for neighboring `vap`'s.

The first part of the `r0kh` is the neighboring `vap` MAC address and NAS identifier which in this example is the MAC without colon delimiters.

The first part of the `r1kh` is the neighboring `vap` MAC address and `r1kh-id` which in this example are the same.
B. Each vap will be represented by a corresponding 0kh and 1kh entry in all of the neighboring vap’s custom configuration sections. Here vap0 entries are highlighted.
C. Generate a unique 128-bit AES hex key for each r0kh entry in the vap.

D. Copy the r0kh keys to the r1kh lines that correspond to the vap.

E. Repeat steps C and D for the other three vap's.
vap0: full hostapd configuration file
vap1: full hostapd configuration file
vap2: full hostapd configuration file
vap3: full hostapd configuration file

For more information see Two WiFi Access Point Network with 802.11r

3. Create four bridge devices, one for each virtual access point.
   A. Go to the port manager tab, select Create, then select Bridge and enter Quantity 4 and a Bridge Name, then Apply to create the bridges.
B. Modify each bridge device to add a vap. Netsmith will show a purple line when each vap has been added as bridge member.
C. Add a single virtual router, drag br0 into the router, then give it an IP address and make it a DHCP server.

For more information see Virtual Router with DHCP Cookbook (skip the wanlink portion)

4. Each bridge will share a connection to a redirect device (rdd) pair so that FT messages can be sent and received.

A. In Netsmith, right-click in a free area and select New Connection to create an rdd pair. Select Skip for Port 1-B, WanLink and Port 2-B then select OK. Select Netsmith Apply after creating the new connection.
B. Right-click and select Modify Port br0, then add rddVR0 to br0. Your rddVRX numbering may differ depending on what other Netsmith objects are created.
C. Right-click and select Modify Port br1, then add rddVR1 to br1. Your rddVRX numbering may differ depending on what other Netsmith objects are created.
D. Create two more rdd pairs for bridges br2 and br3.

E. Add rddVR2 and rddVR3 to bridge br0.
F. The objects vap2/br2 and vap3/br3 can be moved so that their logical relationships can be visualized. Add rddVR3 to br2, then add rddVR5 to br3.
G. The final Netsmith display should show all four of the bridged virtual access points connected by a wap pair, with br0 as the central bridge.

5. Connect LANforge clients and force them to roam from vap to vap. This can be accomplished with a wpacli command for one or two clients or the Mobility Plugin Script for many clients.

   A. Client connected to vap0 04:10:21:b9:8f:00.
B. Client roams to vap1 04:00:21:69:91:03.
C. Client roams to vap2 04:00:21:33:28:06.

```
[root@ben-5pci ~]# wpa_cli -i wlan4 scan
OK
[root@ben-5pci ~]# wpa_cli -i wlan4 roam 04:00:21:33:28:06 DS
OK
[root@ben-5pci ~]# iwconfig wlan4
wlan4     IEEE 802.11abgn  ESSID:"roamer"
    Mode:Managed  Frequency:5.745 GHz  Access Point: 04:00:21:33:28:06
    Bit Rate=6 Nb/s  Tx-Power=19 dBm
    Retry short limit:7  RIS thr:off  Fragment thr=2346 B
    Encryption key:off
    Power Management:off
    Link Quality=70/70  Signal level=2 dBm
    Rx invalid mr:0  Rx invalid crypt:0  Rx invalid frag:0
    Tx excessive retries:0  Invalid misc:0  Missed beacon:0

[root@ben-5pci ~]
```
D. Client roams to vap3 04:f0:21:b1:d7:0b.

```
[root@ben-5pci ~]# wpa_cli -i wlan4 scan
OK
[root@ben-5pci ~]# wpa_cli -i wlan4 roam 04:f0:21:b1:d7:0b DS
OK
```

LANforge Manager Version(5.3.4)

All Ethernet Interfaces (Ports) for all Resources.

<table>
<thead>
<tr>
<th>bps TX LL</th>
<th>Bytes TX LL</th>
<th>bps RX LL</th>
<th>Bytes RX LL</th>
<th>Reset</th>
<th>TX-Rate</th>
<th>RX-Rate</th>
<th>Status</th>
<th>AP</th>
<th>Activity</th>
<th>Signal</th>
<th>Noise</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1024</td>
<td>0</td>
<td>0</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>3 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>2048</td>
<td>2048</td>
<td>2048</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>3072</td>
<td>3072</td>
<td>3072</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>4096</td>
<td>4096</td>
<td>4096</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>5120</td>
<td>5120</td>
<td>5120</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>6144</td>
<td>6144</td>
<td>6144</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>7168</td>
<td>7168</td>
<td>7168</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>8192</td>
<td>8192</td>
<td>8192</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>9216</td>
<td>9216</td>
<td>9216</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>10240</td>
<td>10240</td>
<td>10240</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>11264</td>
<td>11264</td>
<td>11264</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>12288</td>
<td>12288</td>
<td>12288</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>13312</td>
<td>13312</td>
<td>13312</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>14336</td>
<td>14336</td>
<td>14336</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>15360</td>
<td>15360</td>
<td>15360</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
<tr>
<td>0</td>
<td>16384</td>
<td>16384</td>
<td>16384</td>
<td>Completed</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 bps</td>
<td>0 dBm</td>
<td>0 dBm</td>
<td>0 dBm</td>
</tr>
</tbody>
</table>

Logged in to: localhost:4002 as: Admin
E. Client roams back to vap0 04:f0:21:b9:8f:00.

```
[root@ben-Spci ~]# wpa_cli -i wlan4 scan
OK
[root@ben-Spci ~]# wpa_cli -i wlan4 roam 04:f0:21:b9:8f:00 DS
OK
[root@ben-Spci ~]# iwconfig wlan4
wlan4     IEEE 802.11abgn ESSID:"roamer"
        Mode:Managed Frequency:5.745 GHz Access Point: 04:F0:21:B9:8F:00
        Bit Rate=6 Nb/s  Tx-Power=19 dBm
        Retry short limit:7  RTS thr:off Fragment thr:2346 B
        Encryption key:off
        Power Management:off
        Link Quality=70/70  Signal level=17 dBm
        Rx invalid mcs:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

For more information see Two WiFi Access Point Network with 802.11r
Goal: Use automated script to reconnect stations to an AP and report results.

Requires LANforge 5.2.11 or later. Configure Stations to use HotSpot 2.0 (802.1x, 802.1u, etc) and associate them with a HotSpot 2.0 AP. Use the 'WiFi Mobility' LANforge-GUI Plugin to automate re-connecting to the AP and querying ANQP. The plugin will create graphs and other reports that can be saved to HTML. This example uses a LANforge CT520 system but the procedure should work on all CT521, CT522, CT523, CT525 and similar systems. The AP in this test is another LANforge machine, but it could be any AP that supports HotSpot 2.0. A similar test could roam between multiple APs. If the APs are all on the same channel there are no restrictions, but if the APs are on different channels, then only a single station can be configured per LANforge radio. In that case, multiple 3-radio CT523 or other high-density systems may be a good choice.

1. Configure stations to connect to an AP configured for HotSpot 2.0.
   A. Go to the Port Manager tab, select wiphy0 on proper resource, click Create, fill out appropriate information and create desired number of Station interfaces.
B. The new stations should appear in the Port-Mgr table. Double-click to modify one of them. Configure IP Address information, set SSID to [BLANK] and select WPA2.
C. Select the **Advanced Configuration** tab in the Port-Modify window and configure the Key Management, EAP Method, passwords, select **Use 802.1x**, **Enable 802.11u** and **HotSpot 2.0**. If you want to report on DHCP negotiation times, be sure to select the **Restart DHCP on Connect** checkbox. If you want to get packet-drop statistics during roam, Un-select **Restart DHCP on Connect**.

![Configuration Settings](image)

D. Once the single station is connecting properly, use Batch-Modify to configure the rest of the stations to match the first.

For more information see [LANforge User’s Guide: Ports (Interfaces)](link), [WiFi Station Cookbook], [WiFi HotSPot 2.0 Cookbook]

2. Start the WiFi Migration script.
A. Go to the Port Manager tab, select the stations you wish to roam, right-click and choose the WiFi Mobility menu option.

B. The options at the top default to common values and most do not need to be changed. For this example, you must unselect Skip Room to current AP because the script is requesting exactly that. The ports will be automatically configured based on the selection on the Port Manager tab, and may be adjusted before starting the script. The Ports in Use should normally include all stations used in the script. The configuration requiring the most work from the user is the roaming script itself. There is a helpful section on the left, and a script-entry field on the right. Once the script is written, it should be saved in a text file on the user’s PC so that it can easily be pasted into future WiFi Mobility scripts. Some key points are that you must scan about 1 second before roaming or the roaming logic in the supplicant process will either fail or do its own roaming. Either way, the results may be worse than if you do the roam properly in the script. It can take a bit of time for LANforge to get all of the data it needs to report on the roam attempt, so it is suggested that stations not roam more often that about once every 10-20 seconds. If reporting is less important, then the stations can roam more often.
C. Once the script is properly configured, click Start to start the roaming. A window will pop up that has live-updating graphs of various reports. A text log is at the bottom for more detailed analysis, and the whole thing can be saved as HTML. The graphs can be scaled and configured through right-click menus if desired. It will take 1-2 complete roam attempts before the graphs are able to show any useful information.

Stations are configured for Hot-Spot 2.0 (EAPOL key management, EAP-TTLS). Stations are configured to re-negotiate DHCP on each station re-connect. The script forces ANQP query before each roam attempt to provide ANQP query reports (without this, roaming to the same AP will not cause a new ANQP query). Re-negotiating DHCP on such roam is not normally how user-endspoints would act, and it disturbs any network traffic. So, no traffic is configured on these interfaces and the packet-loss graphs will not show any useful data.
D. ANQP and 4-Way Authentication graphs.
E. DHCP Negotiation and Migration Totals graphs.

The migration is verified after the Auto-Verify timer has expired. If the migration has not completed in that time, it will be counted as failed.
F. Text log with timestamps. Can be correlated with wpa_supplicant logs and other log files to debug specific roam attempts.

Migration Script Contents:

# When roaming to self, anap is not natively done
# so this script forces an ANQP query so that we
# get some ANQP query report lines to display.
do_cli scan 1 3 sta1 NA 'trigger freq 5180 5300'
delay 1
do_cli wifi_cli_cmd 1 3 sta1 'fetch_anap'
  floor 3 sta1 00:04:05
  floor 3 sta2 00:04:05
  floor 3 sta3 00:04:05
  floor 3 sta4 00:04:05
  floor 3 sta5 00:04:05
  floor 3 sta6 00:04:05
  floor 3 sta7 00:04:05
  floor 3 sta8 00:04:05

Log Messages:

136514744.462 CLU: scan 1 3 sta1 NA 'trigger freq 5189 5300'
136514744.464 CLU: wifi_cli_cmd 1 3 sta1 'fetch_anap'
136514744.817 CLU: wifi_cli_cmd 1 3 sta1 roam 00:01:02:03:04:05
136514744.888 CLU: wifi_cli_cmd 1 3 sta2 'fetch_anap'
136514744.920 CLU: wifi_cli_cmd 1 3 sta2 roam 00:01:02:03:04:05
136514744.970 CLU: wifi_cli_cmd 1 3 sta3 'fetch_anap'
136514744.922 CLU: wifi_cli_cmd 1 3 sta3 roam 00:01:02:03:04:05
136514744.973 CLU: wifi_cli_cmd 1 3 sta4 'fetch_anap'
136514745.125 CLU: wifi_cli_cmd 1 3 sta3 roam 00:01:02:03:04:05
136514745.175 CLU: wifi_cli_cmd 1 3 sta5 'fetch_anap'
136514745.227 CLU: wifi_cli_cmd 1 3 sta5 roam 00:01:02:03:04:05
136514745.277 CLU: wifi_cli_cmd 1 3 sta6 'fetch_anap'
136514745.328 CLU: wifi_cli_cmd 1 3 sta6 roam 00:01:02:03:04:05
136514745.378 CLU: wifi_cli_cmd 1 3 sta7 'fetch_anap'
136514745.430 CLU: wifi_cli_cmd 1 3 sta7 roam 00:01:02:03:04:05
136514745.820 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat1), BSSID: 00:01:02:03:04:05
136514745.921 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat1), BSSID: 00:01:02:03:04:05
136514745.962 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat1), BSSID: 00:01:02:03:04:05
136514746.023 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514746.126 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514746.229 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514746.326 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514746.632 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514746.762 detected 0 dropped (n) packets during roam attempt. station 1.3 (stat2), BSSID: 00:01:02:03:04:05
136514747.160 sta1 connected to: 80:01:02:03:04:05 in 27,702 us 4-way-ath 10,178 us ANQP: 5,582 us DHCP: 1,172 ms
136514747.161 sta2 connected to: 80:01:02:03:04:05 in 29,833 us 4-way-ath 10,223 us ANQP: 6,113 us DHCP: 1,618 ms
136514747.165 sta3 connected to: 80:01:02:03:04:05 in 35,327 us 4-way-ath 10,094 us ANQP: 5,952 us DHCP: 1,197 ms
136514747.167 sta4 connected to: 80:01:02:03:04:05 in 25,150 us 4-way-ath 11,226 us ANQP: 5,707 us DHCP: 1,980 ms
136514747.169 sta5 connected to: 80:01:02:03:04:05 in 29,814 us 4-way-ath 5,559 us ANQP: 5,681 us DHCP: 1,204 ms
136514748.731 CLU: scan 1 3 sta1 NA 'trigger freq 5189 5300'
136514748.883 CLU: wifi_cli_cmd 1 3 sta1 roam 00:01:02:03:04:05
136514748.924 CLU: wifi_cli_cmd 1 3 sta2 'fetch_anap'
136514748.964 CLU: wifi_cli_cmd 1 3 sta2 roam 00:01:02:03:04:05
136514747.025 CLU: wifi_cli_cmd 1 3 sta3 'fetch_anap'
136514747.065 CLU: wifi_cli_cmd 1 3 sta3 roam 00:01:02:03:04:05
136514747.136 CLU: wifi_cli_cmd 1 3 sta4 'fetch_anap'
136514747.187 CLU: wifi_cli_cmd 1 3 sta4 roam 00:01:02:03:04:05

For more information see Complete report for this test case
LANforge WiFi testing HotSpot 2.0 Release 2

Goal: Setup HotSpot 2.0 Release 2 Example

Requires LANforge 5.3.2 or later on Fedora 20 or later.

- Run LANforge install script to begin setup of HotSpot 2.0 R2 related servers and certificates.
- Configure the OSN Server-only authenticated layer-2 Encryption Network (OSEN) AP and Passpoint AP.
- Initiate Online Sign-Up (OSU) procedure, select a provider and obtain an IP address from the Passpoint AP.
- Send traffic through the Service Provider Network.

For more information see:
WiFi Alliance Passpoint Release 2 Deployment Guidelines

1. Run LANforge installation script to begin hostapd RADIUS, certificates and HotSpot 2.0 setup:
   ```
   cd /home/lanforge
   ./lf_kinstall.pl --lfver 5.3.2 --do_radius --do_hs20
   ```

2. Make two copies of the `ca.pem` certificate to different directories:
   ```
   cp /home/lanforge/hs20/ca/ca.pem /home/lanforge/ota-ca.pem
   cp /home/lanforge/hs20/ca/ca.pem /home/lanforge/wifi/osu_wlan2/osu-ca.pem
   ```

   `ota-ca.pem` is used by the client for Over-The-Air authentication to the OSEN AP
   `osu-ca.pem` is used by the client for the Online-Sign-Up server authentication before connecting to the Passpoint AP

   This is an all-in-one example on a single LANforge system, but if the authentication servers were setup on different systems, the proper certificates would need to be copied instead.

3. Create `devinfo.xml` and `devdetail.xml` files in `/home/lanforge/wifi/osu_wlan2`
4. Create two MAC-VLANs for two hostapd RADIUS server instances.
A. Go to the Port Manager tab, select eth1, select Create, select MAC-VLAN, quantity 2 then Apply.
8. Double-click each new MAC-VLAN interface in the Port-Mgr tab to modify. Select the RADIUS checkbox which will allow a hostapd based RADIUS server on the interfaces using the config files:

/home/lanforge/wifi/hostapd_eth1#0.conf and /home/lanforge/wifi/hostapd_eth1#1.conf

Because this is an all-in-one example, the hostapd RADIUS servers will be referenced to localhost and each MAC-VLAN interface will not need an IP address assigned. If the hostapd RADIUS servers were on different systems or networks, the appropriate IP address would be assigned here.
C. Create 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=/home/lanforge/hs20/AS/hostapd-osen.eap_user
server_id=ct523-3n-f20
eap_sim_db=unix:/tmp/hlr_auc_gw.sock
radius_server_auth_port=1820
radius_server_clients=/home/lanforge/hs20/AS/hostap.radius_clients
cia_cert=/home/lanforge/hs20/ca/ca.pem
server_cert=/home/lanforge/hs20/ca/server.pem
private_key=/home/lanforge/hs20/ca/server.key
private_key_passwd=lanforge
ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

NOTE: The eap_user_file, eap_sim_db and radius_server_auth_port are unique for each RADIUS server.

D. Create config file:

```
/home/lanforge/wifi/hostapd_eth1#1.conf

interface=eth1#1
driver=wired
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
dump_file=/home/lanforge/wifi/hostapd_eth1#1.dump
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
ieee8021x=1
eapol_key_index_workaround=0
eap_server=1
eap_user_file=sqlite:/home/lanforge/hs20/AS/DB/eap_user.db
server_id=ct523-3n-f20
eap_sim_db=unix:/tmp/hlr_auc_gw.sock	db=/home/lanforge/hs20/AS/DB/eap_sim.db
radius_server_auth_port=1821
radius_server_clients=/home/lanforge/hs20/AS/hostap.radius_clients
cia_cert=/home/lanforge/hs20/ca/ca.pem
server_cert=/home/lanforge/hs20/ca/server.pem
private_key=/home/lanforge/hs20/ca/server.key
private_key_passwd=lanforge
ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

NOTE: The eap_user_file, eap_sim_db and radius_server_auth_port are unique for each RADIUS server.

E. 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 &
```

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

F. Reset the MAC-VLAN interfaces on the Port Mgr tab so that the new hostapd RADIUS servers are started. Check that they are running with the command:

```
ps auxwww | grep hostapd_eth
```

If they are not running, check the log files for problems:

```
cat /home/lanforge/wifi/hostapd_log_eth1#0.txt
cat /home/lanforge/wifi/hostapd_log_eth1#1.txt
```

5. Create two VAPs for the HotSpot 2.0 Release 2 Network.
A. Go to the Port Mgr tab and create one VAP on wiphy0 and one VAP on wiphy1.

B. Modify the first VAP on wiphy0 to be the OSEN AP. Configure IP Address and SSID.

C. Select the Advanced Configuration tab in the Port-Modify window to configure 802.1x and RADIUS server information.
D. Select the **Custom WiFi** tab to add the following lines for HotSpot 2.0 Release 2.

```
ocsp_stapling_response=/home/lanforge/hs20/ca/ocsp-server-cache.der
```

E. Modify the second VAP on wiphy1 to be the **Passpoint** AP. Configure IP Address and SSID.
F. Select the **Advanced Configuration** tab in the Port-Modify window to configure 802.1x, 802.1u, HotSpot 2.0, RADIUS server and other information.
G. Select the **Custom WiFi** tab to add the following lines for HotSpot 2.0 Release 2.

```plaintext
hs20_icon=64:64:eng:image/png:logo-64x64.png
osu_ssid="ABCD-1234"
osu_friendly_name=eng:LANforge HS20 Operator
osu_nai=os@lanforge.com
osu_method_list=1 0
osu_icon=logo-64x64.png
osu_service_desc=eng:LANforge Example services
```

H. Modify `wiphy0` and `wiphy1` to be on the same channel and select OK.
I. In Netsmith, setup each VAP with DHCP Service on different IP networks.

J. Check that the VAP hostapd processes are running with the command:

```
ps auxww |grep hostapd_vap
```

If they are not running, check the log files for problems:

```
tail -f /home/lanforge/wifi/hostapd_log_vap1.txt
tail -f /home/lanforge/wifi/hostapd_log_vap2.txt
```

For more information see WiFi Testing: Configuring a Virtual AP with Limited Stations

6. Start the Online Certificate Status Protocol (OCSP) script which will restart the OCSP Responder and update the
cache once per minute. It is only required on the VAP or server side of a HotSpot 2.0 R2 network.

cd /home/lanforge
./ocsp.bash > /dev/null 2>&1 &

7. In Netsmith, we can label the two Virtual Routers containing each VAP. We also setup a single TCP connection named ‘test1’ between the client (wlan2) and a virtual interface connected to the Passpoint AP. In this way, we can verify that the client is only allowed to pass traffic once it has met the authentication requirements for the HotSpot and Service Provider Networks.

For more information see
Virtual Router with NAT Cookbook, Virtual Router with DHCP Cookbook

8. Setup wlan2 as the HotSpot 2.0 R2 client.
A. Modify wlan2 on the Port Mgr tab and set the SSID to the OSEN AP's SSID 'ABCD-1234' in this example and set the authentication to OSEN.

B. In wlan2 Advanced WiFi Settings, select Advanced/802.1x, set Key Management, EAP Identity and CA Cert File.
C. In wlan2 Misc Configuration, set OCSP to Required.

D. Admin up wlan2 and it will associate with the OSEN AP and obtain an IP address on the OSEN AP IP network.
9. Initiate Online Sign-Up

A. In a terminal window type the following:

```
cd /home/lanforge/wifi/osu_wlan2
lanforge/local/hs20/client/hs20-osu-client -x /home/lanforge/local/hs20/spp/spp.xsd -dd -S wlan2 signup
```

B. Select 'LANforge HS20 Operator' from the Service Provider List.

Select service operator

**Select service operator**

- [eng] LANforge HS20 Operator
- [eng] LANforge Example services

BSSID: 00:0e:8e:23:17:48
SSID: ABCD-1334
NAI: osen@lanforge.com
methods: OMA-DM SOAP-XML-SPP
C. Select 'Sign up for free access' from the Online Sign-Up page.

Sign up for a subscription - ct523-3n-f20.lanforge.local

Sign up for free access

Select a username and password. Leave password empty to get automatically generated and machine managed password.
Username: 
Password: 

Complete subscription registration

Enroll a client certificate

D. Select the Accept button to complete the Online Sign-Up.

Hotspot 2.0 - public and free hotspot

Terms and conditions..
10. Client wlan2 will obtain an IP address on the Passpoint AP IP network and TCP connection 'test1' can now pass traffic.

11. If wlan2 is reset or reassociates with the OSEN AP, you will have to remove the Service Provider (SP) directory before attempting the Online Sign-Up again.

    cd /home/lanforge/wifi/osu_wlan2
    rm -rf SP
LANforge WiFi Rate v. Range Test

Goal: Compare WiFi performance for 'upload' traffic (client to AP) using a WiFi access point, a LANforge Attenuator and a LANforge Virtual Station. Traffic is generated by a RFC-2544 script on a Layer-3 UDP connection.

This demo consists of one WiFi access point and one CT523 LANforge WiFiRE machine connected to the LANforge Attenuator with coax SMA cables. [This is not over the air testing]. This requires LANforge release 5.2.7 or higher.

1. Create Virtual Station

A. Select radio wiphy1 and click Modify
B. Set the frequency of the radio to **Auto**

A. Click **OK**

C. On the Port Modify tab, click **Create**
D. Create virtual station with these parameters:

A. Select WiFi STA
B. Choose DHCP-IPv4
C. Quantity 1
D. Station ID 0
E. SSID 'udptest'
F. Click Apply

2. Create upstream port wired to AP
   A. Wire the eth1 port into the upstream connection of the AP under test.
   B. On the Ports tab, click on the eth1 port
   C. Configure eth1 port with an upstream IP, like 10.26.2.3

D. Set the Gateway to the AP wired interface IP.
E. Click OK
3. Create and Test Cross Connect

A. Go to the **Layer 3** tab

B. Create a cross connect with these qualities:

   A. Make sure Endpoint A is *eth1*
   
   B. Make sure Endpoint B is *sta0*
   
   C. Min PDU Size for both should be **1472**
   
   D. **NOTE**: These rate and PDU size settings will be manipulated by the script we setup later.

C. Next, expand the screen to **Level 4** using the [+] button.
D. Configure the send buffer on **Endpoint B** to **1 MB**

A. Click **OK**

E. On the **Layer 3** tab, click **Start** to verify the AP and Station can connect

F. Click the **Display** button to monitor throughput

G. Only a short confirmation is necessary, click **Stop** on the **Layer 3** tab

4. Configure Scripting for Cross Connect
   
   A. On the **Layer-3** tab, click **Modify**
B. In the Level 2 box, click Endpoint A **Script** button

C. The Cross Connect Script window displays with no parameters
D. Select Script Type: **RFC-2544**. Set the following parameters:

A. Select **Symmetric**. This will increment both the A and B rates and payload sizes. (Instead of just side A).

B. Select **Show Attenuation**. This displays attenuation levels in the report.

C. **Run Duration: 10 sec**. This is how long each rate setting will be held.

D. **Pause Duration: 2 sec**. We give it some time to transition.

E. **Max Drop Percent: 10%**

F. **Max Jitter: 200ms**

G. **Max RT Latency: 200ms**

H. **Rates A: 56kbps**. This sets the client upload target rate.

I. **Rates B: 400Mbs**. This sets the client download target rate.

J. **Pld A: 1472**. This sets the client (sta0) MTU. This is a 1500 byte wire packet.

K. **Pld B: 9000**. This sets the upstream (eth1) MTU.

L. **Attenuator Resource: 1.1.2**. You can find your attenuator resources in the **Attenuator** tab.

M. **Attenuation: 0..+5..955**. This is shorthand for: Begin at zero dB attenuation, increase in 0.5dB steps, until 955 dB of attenuation. Individual dB steps could also be specified.

N. Click **OK**

E. On the **Create/Modify Cross Connect** window, click **OK**

5. Run the Cross Connect and Generate a Report
A. On the Layer-3 tab, click Start

B. The Scripting Report window will appear

A. When the script completes, you can view the graphed results.
B. Click on Graphical Display and a window with the graphical report will display
C. Scroll to the top of the window to view the graphs. Highlights are shown below.
D. Attenuation v. RX signal, endpoint A
E. Attenuation v. RX signal, endpoint B

F. TX rate (UDP payload) v. RX signal, endpoint B

G. RX rate including frame headers (UDP payload with frame headers) v. RX signal, endpoint B
H. RX rate v. TX link speed. You see a sawtooth pattern because all attenuations are included.

I. Click on **Save File** and your browser will appear the the HTML copy of the report.
LANforge WiFi Attenuation vs PDU Size Test

Goal: Compare WiFi performance for 'download' traffic (AP to Client) as Payload Size and RF Attenuation levels change using a WiFi access point, a LANforge Attenuator and a LANforge Virtual Station. Traffic is generated by a RFC-2544 script on a Layer-3 UDP connection.

This demo consists of one WiFi access point and one CT523 LANforge WiFIRE machine connected to the LANforge Attenuator with coax SMA cables. [This is not over the air testing].

1. Create Layer-3 Cross Connect
   A. Go to the Layer 3 tab

   ![LANforge Layer-3 Cross Connect]

   A. Click Create
B. Create a cross connect with these settings:

A. Make sure Endpoint A is `eth2` or the wired port to the AP.
B. Make sure Endpoint B is `wlan0` or the station associated with the AP.
C. Min PDU Size for both should be `AUTO`.
D. **NOTE:** These rate and PDU size settings will be manipulated by the script we setup later.
E. Verify that the connection is operational before adding a script.

2. Configure Scripting for Cross Connect
   A. On the **Layer-3** tab, click **Modify**
   B. In the Level 2 box, click Endpoint A **Script** button
C. The Cross Connect Script window displays with Script Type: **NONE**

D. Select Script Type: **RFC-2544** and default values appear:

A. Select **Show Attenuation**. This displays attenuation levels in the report.

B. Run Duration: **30 sec**. This is how long each iteration will run.

C. Pause Duration: **5 sec**. We give it some time to transition.
E. Setup Pass/Fail Criteria and Iteration Steps for the script. For each Attenuation Level, the script will step through each PDU size at the desired rate. If there were multiple rates then for each Attenuation Level, the script would step through each PDU size for each rate.

A. Max Drop Percent 20%
B. Max Jitter 200ms
C. Max RT Latency 1000ms
D. Rates A: 900Mbps, This sets the client download target rate.
E. Pld A: 64, 512, 1024, 1472
F. Attenuator Resource: 1.1.35. You can find your attenuator resources in the Attenuator tab.
G. Attenuation: 0..+50..955. This is shorthand for: Begin at zero dB attenuation, increase in 5.0dB steps, until 955 dB of attenuation. Individual dB steps could also be specified.
H. Click OK

F. On the Create/Modify Cross Connect window, click OK

3. Save Data to be able to view past results.

A. Go to Reporting Menu and select Reporting Manager
B. Select the GUI Data Collection tab
C. Choose a directory and select Save.

4. Run the Cross Connect and Generate a Report

B. View the Dynamic Report
   A. While the script is running, you can view the real-time results of the running script.
   B. Right-Click on wlan0 and select Dynamic Report
   C. Setup the Dynamic Report to view the data you are interested in.
   D. wlan0: RX Signal level shown on Axis-B and RX bps shown on Axis-A

E. To view Dynamic Report data after the test completes:
   F. Set the Reporting Manager, Generate Report to the directory containing saved data.
   G. Adjust the time scale and Load the data in the Dynamic Report window.

C. View the graphical results of the script when it completes.
   A. In the Script Report window, click on **Graphical Display** and a window with the graphical report will display
   B. Scroll to the top of the window to view the graphs. Examples are shown below.
C. Attenuation v. RX signal, endpoint A

![Graph showing Attenuations v/s RX-Signal for endpoint: atten-vs-pdu-A: Requested Rate: 900000000]

D. 3D graph of Peer RX Bps

![3D graph showing Peer RX Bps for endpoint: atten-vs-pdu-A: Requested Rate: 900000000]

E. Click on Save File and your browser will appear the the HTML copy of the report.

See also: Full Report   Raw Report Text
Goal: Use the WiFi Capacity plugin to emulate traffic from hundreds of virtual stations across an access point and report the results.

Requires LANforge 5.2.11 or later. Configure 128 stations and assign them an SSID. Use the ‘WiFi Capacity’ LANforge-GUI plugin to emulate:

- Station download traffic through the AP
- Station-to-station traffic

The `eth1` port of our LANforge in this example is connected to the upstream network of the AP.

This example uses a LANforge CT523 system but the procedure should work on all CT520, CT523, CT525 and similar systems.

1. In the Port Mgr tab, select the radio `wiphy0` and click Create.
2. The Create VLANs window appears. Set the values below.

A. Check WiFi STA.
B. In the MAC Addr dropdown, choose RANDOM.
C. Select DHCP-IPv4.
D. Specify 128 for Quantity.
E. Set STA ID at 0.
F. Our AP for this example is using SSID testAP with Keyphrase test-AP1. (no dashes allowed)
G. Click the Apply button.
H. And then close the window by pressing the Cancel button.
3. Discussion of Capacity Test

A. Computing Intervals and Duration: The WiFi Capacity Test is intended to run in multiple intervals. How many intervals is a product of the number stations in the test divided by the interval increment: \( \text{Intervals} = \frac{\text{num stations}}{\text{station increment}} \). The duration of the test is the product of the number of intervals times the sum of the interval duration plus setup timeout between intervals. Given the setup time between intervals is \( J \) seconds, a test of 128 stations with a station increment of 8 and an interval duration of 30 seconds, the entire test duration is: \((128 / 8) * (30 + J) = 480 + 16J \) seconds. The actual setup time depends on two factors; a) if Seek Lower Rates is enabled, which will attempt to test each rate to try and even out connection rates, and b) DHCP performance. Adding piles of DHCP assignments for every increment can take several seconds, and actual performance depends on your test environment.
8. **Configuring Routes**: the upstream port of your LANforge system should be able to ping the virtual stations. You can use a command from the LANforge command prompt to test this out: `ping -I eth1 10.26.2.100` where eth1 is your upstream port on the same switch as the AP, and 10.26.2.100 is the IP of the virtual station. In the **Port Properties** window, you will probably want to set the gateway address for the port to the IP of the AP. In this case it is **10.26.1.2**. Without this routing configured, the only test performed will be the station-to-station test.

4. **Downloading via 128 Virtual Stations**

   A. In the **Plugins** dropdown menu, select **WiFi Capacity Test**, then begin to configure ports for the test.
A. Highlight free ports that you want to add to the test, this includes the upstream port eth1 and the virtual stations sta0 - sta127.

B. Set Station Increment to 8. This will run 16 intervals with 8 stations added each time going up to 128 total.

C. Set the increment Duration to thirty seconds (in milliseconds) so 30000.

D. Select UDP-IPv4 for the Protocol.

E. For the Payload size select 24,000 B.

F. Configure the Download Rate at 330 Mbps. The theoretical maximum for AP throughput on one radio is about 340 Mbps with perfect conditions. Even 330 Mbps might not be achieved. This download rate is the rate requested of the AP by all the virtual stations. With eight virtual stations, the total download rate per station is 41.25 Mbps.

G. In Advanced Settings, set a Socket Buffer of 1MB.

H. Deselect Try Lower Rates. This will reduce interval setup time.

B. Click the Start button to begin the test.
C. You will see a Graphical Test Results window appear. It will update every test interval.

5. Emulating station-to-station traffic with 128 virtual stations:
   A. Go to the Wifi Capacity Test window.

For more information see LANforge GUI User Guide: Plugins:WiFi Capacity Test.
B. This test is very similar. We remove the upstream port eth1 from the Ports in Use list (in the Select Ports tab). We then configure the traffic to use smaller TCP packets.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>TCP-IPv4</td>
</tr>
<tr>
<td>Payload Size</td>
<td>4000 B</td>
</tr>
<tr>
<td>Total Download Rate</td>
<td>60 Mbps</td>
</tr>
<tr>
<td>Total Upload Rate</td>
<td>60 Mbps</td>
</tr>
</tbody>
</table>

A. In the settings tab, set Protocol and Payload to TCP-IPv4 and 4000 B.

B. Change Total Download and Total Upload rate to 60 Mbps and 60 Mbps. These settings should allow up to 120 Mbps between two stations, which will clearly saturate an AP.

C. Click Start to begin the test.

D. You will see a Graphical Test Results window appear. It will upon each test interval.
Goal: Use the WiFi Port Reset plugin to emulate restarting of stations associated to your WiFi network.

Requires LANforge 5.2.12 or later. Restarting a WiFi station exercises the whole network stack because it forces negotiation across the wired network: your AP, your DHCP server, your AP controller, and possibly your RADIUS server. Performing this test at an unusually high frequency is a challenging robustness test for your wireless topology and can expose possible race conditions when large numbers of stations reset simultaneously while passing traffic. This cookbook assumes the System Under Test is your AP and that a CT520 (or better) is emulating stations to be reset on the network.

1. Create WiFi stations
   A. In the Ports tab, select wiphy0 and click Create
B. In the Create VLANs window, craft ten wifi stations:

A. Select WiFi STA
B. For MAC address, choose XX:XX:XX:XX:XX:XX
C. Select DHCP-IPv4
D. Enter Quantity 10
E. Specify 0 for STA ID
F. The example SSID for this cookbook is jedtest
G. ...and then click Apply

C. You will see ten stations created:
2. Create Connections to Stations
   A. In the Layer-3 tab, click Create

   B. Create station download traffic
A. This example connection is named sta-trf

B. Connection Type is LANforge / TCP

C. This example resource is kedtest, where our stations live

D. The Endpoint A Port will be the station sta0,

E. and the Endpoint B Port will be upstream of the ap, eth1.

F. We'll set the Min Tx Rate for both sides to 265 Kbps

G. and set the PDU Size to TCP Pld (1,460 B).

H. ...then click OK

C. Test this station by selecting it and clicking Start

D. Click Stop when you are done testing the connection

E. Click Modify for sta-trf and we will batch create nine more:
F. Click **Batch Create** in the Create-Modify Cross Connect window

G. Create nine more cross connects like this one:

A. Set Quantity to 9
B. Set Number of Digits to 2
C. We are not changing the B-side port, so we do not need to increment it. Set the Port Increment B to 0

H. Select all connections and click Start

I. Connections should not show dropped packets in the _Rx Drop % A _or _Rx Drop % B_ columns

3. Configure Port Reset Script
   A. In the **Port Manager** tab, select stations sta0 - sta9
B. In the LANforge Manager windows, select the Plugins→Port Reset Test option.

C. In the Port Reset Test window, you will see the ten ports already selected. We will configure quick resets for this test:

A. Set Concurrent Ports to Reset to 5
B. Set Minimum Time between Resets to 5 seconds
C. and Maximum Time between Resets to 20 seconds
D. ...and click Start

4. Observe Results
   A. The Port Reset Test Results window will show the list of ports getting reset.

B. The Layer-3 tab will show the amount of lost and dropped packets.
C. We can graph the throughput of the connections with the Dynamic Report menu option.

D. In the Dynamic Reports window, we are graphing the **Rx-Bps** for each connection in axis A, and in axis B we are graphing the Rx-Bps for the upstream port, eth1.
E. You will also want to watch for warnings and failures. In the Alerts tab, you will see persistent alerts. The alerts in this picture can be safely ignored:

F. Check the LANforge Wireless Events window. You will see station connects and disconnects and failure notices. The messages shown in this picture are normal:
G. In the LANforge Messages window, you will see connection warnings. Connections will warn when their IP changes, and this is normal, as shown in this picture:

H. And in the Event Log tab, you can review more detailed link-up, link-down and connection events that occur with these station restarts:

I. Use these monitoring sources to check for undesirable trends:
   - Undesirable slowing trend in traffic
   - Stations that do not return
   - DHCP failures or pool exhaustion
Goal: Create a scenario where WiFi stations send out corrupted packets that can cause handshake and authentication failures. Learn techniques to capture and inspect packets to view corruption and scan log files to find indications of LANforge corruption injections.

We will learn to use the some WiFi packet corruption features to emulate malfunctioning station equipment. This consists of enabling the corruption features and looking for errors when stations attempt to associate. Part of this will include capturing packets and inspecting them. This scenario requires LANforge version 5.3.6, and a two-radio LANforge system with one radio set in monitor mode.
Open Authentication Test Scenario

We will begin with a basic open authentication test scenario with a single virtual station on a LANforge system connecting to an AP. (See Also: Generating Traffic for WLAN Testing) This test scenario also works for Captive Portal testing.

Create a Station with Corruptions

We will use the simplest form of corruption, ignored frames. Select the Port → Corruptions tab, and set Ignore RX Frames very high, like 75%. To limit this to association frames, select ASSOC.
**Associate a Station with Corruptions**

Introducing corruptions is simple. Watching the effects takes some effort. With aggressive association corruptions, the basic effect will appear as if your station takes an unreasonably long time to associate. Let's set up Wireshark at different interfaces to understand better the kinds of traffic at play.

1. Select a radio for monitoring and set its channel to match the AP channel. If your AP is on channel 44, modify your LANforge wiphy monitor radio to also listen on channel 44. Our test AP is named hedtest-2000-open.
2. Create a monitor port [Port tab → Select Radio → Create → Monitor]

You will see the `mon13000` port below. The channel number will not display.
3. Create a station (wiphy1 — wlan1 will work) and associate it with heatest-2000-open. Highlight the station in the Ports tab and bring it up.

Watch Traffic

With 75% ignore the chances of the station actually associating are very port. On our monitor interface, we see that there are multiple discover and request packets.
On our station interface (wlan1), we see a different number of DHCP requests.

At our AP, we see repeated attempts.
WPA2 Authentication Test Scenario

We will configure a station with WPA2 PSK encryption. We will also use Wireshark to decrypt the packets in order to see that they are corrupt.

Configure the Station

Configure station with WPA2 (See also: Test WiFi station upload throughput)
On the Corruptions tab, you can set stations:
Setup Packet Decryption

We will not be able to inspect packets unless we configure Wireshark to decrypt the packets from this capture. Follow these steps:

1. Wireshark Preferences (Edit → Preferences)
2. Protocol Preferences (Preferences → Protocols)
3. IEEE 802.11 Preferences (Protocols → IEEE 802.11)

- Select **Reassemble Fragmented 802.11 datagrams**
- Select **Call subdissector for retransmitted 802.11 frames**
- Select **Assume Packets have FCS**
- Select **Validate the FCS Checksum if possible**
Select **No** for ignore the Protection bit

Select **Enable Decryption**

Add the SSID and password to the list of Decryption Keys. Select `wpa-pwd` and type in the string `SSID:PSK` to match your password from your AP:

hedtest-2100-wpa2: hedtest-2100-wpa2

With our decryption enabled we can now inspect the captured packets:

Packets from **moni3000** are filtered to show the station of interest using the display filter:

wlan.addr == 04:f0:21:2f:90:31
We can focus into the association by using a display filter:

\[
\text{wlan.addr == 04:f0:21:2f:90:31 && wlan.fc.subtype < 4}
\]

And the packets that form the association:
Notice how the AP only really gets the uncorrupted packets. What we hope will happen is that our WiFi drivers will discard corrupted packets before passing them up to userspace.

We did not need to decrypt packets from our AP (only possible if monitoring inside the AP) vap2100:
Goal: Operate the CT703 WiFi Attenuator with a script to see the effect on a Layer-3 connection.

The LANforge GUI provides scripting support for the CT703 Attenuator. This cookbook provides a basic example of how to graph connection throughput and signal strength with a single station connection. Use this example as a basis for building more complex attenuation scripts. Requires LANforge 5.2.11+ and CT703 Attenuator.

1. Create a WiFi station
   A. In the **Ports** tab, select wiphy0 and click **Create**

   ![LANforge WiFi Interface](image)

B. In the **Create VLANS** window, craft one wifi station:

   ![Create VLANS Window](image)
A. Select WIFI STA
B. For MAC address, choose \texttt{xx:xx:xx:xx:xx:xx}
C. Select DHCP-IPv4
D. Enter Quantity 1
E. Specify 0 for STA ID
F. The example SSID for this cookbook is \texttt{jedtest}
G. ...and then click \texttt{Apply}

C. You will see a station created:

2. Create a connection to the Station
   A. In the Layer-3 tab, click \texttt{Create}
B. Create two-way station traffic

A. This example connection is named jbr
B. Connection Type is LANforge / UDP
C. This example resource is kedtest, where our stations live
D. The Endpoint A Port will be the station sta0.
E. and the Endpoint B Port will be upstream of the ap, eth1.
F. We'll set the Min Tx Rate for both sides to 100 Mbps
G. and set the PDU Size to UDP Pld (1,472 B).
H. Use the + button to expand the window to panel 4 and add 2MB of buffers to the connection:
I. ...then click OK

C. You will see connection jbr in the Layer-3 tab now:

D. Begin traffic on this station by selecting it and clicking Start

3. Create an Attenuator Script
   A. In the Attenuators tab, select your attenuator and click Modify
B. You will see the Modify Attenuator window. Click on the **Script** button.

C. The Add/Modify Script window opens. In the picture below you see a huge list of numbers (the attenuation levels). These numbers are not pre-populated. You can copy and paste them out of this document or create a series with other commands listed below.

A. In the Script Type pulldown, select **ScriptAtten**
B. Type in the name for the script, this example is called attnr.

C. Select Symmetric

D. Choose 5 s for Run Duration. This will run the Attenuator at each dB value for this period of time.

E. Enter the following attenuation values for a 16 minute long test. This will send the attenuator from 5 to 955 dB and back:

```
```

G. ...click OK

D. In the Attenuators tab, you will notice that your attenuator now reads Enabled in the Script column. Select the attenuator and click the Start button.

E. The window Script Report will appear. This monitors the script behavior of the attenuator script.
F. To monitor the progress of traffic and signal as it progresses, you will go to the Ports tab. Click on sta0, right click and select Dynamic Display. The Dynamic Reports window will open. Choose the following selections to refine the display:

A. Unselect Tx-Bps
B. Select Rx-Bps
C. Select Rx-Signal
D. Drag the label sta0-signal to the left side of the X axis
E. Click Adjust and set Maximum Time to 30 min, click OK
F. Click Auto Adjust

G. At the end of the attenuator script run, the Layer-3 connection will still be running, but the Script Report window will say End of Report. At this time, click on Graphical Display. You will see a graph of the attenuation level over time.
4. Creating attenuation sequences

5. It is relatively simple to generate a sequence of numbers right from a Terminal window (on Linux). Below are some examples:

A. The 10 ddB step series we used in this example:
   ```bash
   for d in `seq 5 +10 955` `seq 955 -10 5`; do echo -n "$d, " ; done | fold -sw80
   ```

B. A 5 ddB step series, as precise as the CT703 can run:
   ```bash
   for d in `seq 0 +5 955` `seq 955 -5 0`; do echo -n "$d, " ; done | fold -sw80
   ```

C. A 15 ddB step series from full attenuation to 25 ddB:
   ```bash
   for d in `seq 955 -15 25`; do echo -n "$d, " ; done | fold -sw80
   ```

D. A sawtooth ranging from 950 to 0 ddB:
   ```bash
   i=0; while [ $i -lt 100 ]; do echo -n "$(( $i%11 * 95 ))", " ; i=$[ $i+1 ]; done | fold -sw80
   ```
Generate WiFi Traffic from an External Connection

Goal: Create a bridged WiFi station that redirects traffic from an ethernet port.

It is possible to use a system on a wired LAN to generate traffic through a LANforge virtual WiFi station. This example will show a Windows PC driving traffic across a LANforge CT520 STA to the associated AP. This is a useful scenario for driving custom traffic between traffic testing software endpoints distinct from the LANforge system. A virtualized Windows PC will work with this scenario.

The primary technique in this cookbook uses a technique where the MAC address of the WiFi STA is spoofing the address of the Windows PC. It is also possible to use this technique with IPv4 addresses and not MAC addresses. However, using MAC addresses will allow IPv6 traffic to work.

1. Find the MAC Address of the Windows PC.
   A. We will use MAC address 08:00:27:c4:4e:4f. This will be used when you configure the WiFi STA on the LANforge machine.
   B. Please set the IP address of the interface if it is not yet set.

For more information see Windows IP Addresses

2. Configure your LANforge Wireless Station. We will be configuring the MAC addresses of a station to be the MAC address of the Windows PC we just found.
   A. In the Ports tab, double-click on the ethernet port on the same switch as the Windows PC (eth1 in this example).
B. Configure the port MAC address and WiFi-Bridge settings to be:

A. Do not set the mac address or the ip address of the port
B. Set Rpt Timer to **faster (1 s)**
C. Select 1 for WiFi Bridge
D. Click the **OK** button

C. Configure a WiFi station. This example will be connecting to a WiFi AP with the SSID jedtest.
A. Enable Set MAC
B. Use **08:00:27:c4:4e:4f** for the MAC Addr
C. Set Rpt Timer to **faster (1 s)**
D. Select **1** for WiFi Bridge
E. Enter **jedtest** for the SSID
F. Select **802.11abgn** for the Mode
G. Click the **OK** button

D. (Note: these MAC addresses will remain persistent even through a LANforge Manager restart. To restore the physical mac addresses, you need to reboot the LANforge machine or use **ethtool** to find the physical hardware address.)

3. Sending and Validating Traffic
A. Use ping on the Windows machine to reach 10.26.0.2, the AP machine. To ping from a specific interface, use the -S switch like so: `ping -S 10.26.0.10`

B. On LANforge, use tcpdump to view packets traversing the Station interface. `sudo tcpdump -ni sta0 icmp`
WiFi Captive Portal Bot (portal-bot)

Goal: Execute a battery of captive portal logins from virtual wifi stations using the newer script.

Public access open WiFi service is often gated with a web sign-on form (a captive portal). LANforge virtual stations can emulate sign-in to the captive portal using the portal-bot.pl script. This script is by necessity incomplete because many captive portals have different behaviors and login form requirements. With this script, you provide a bot plugin that bridges the gap. This cookbook will coach you through a basic portal-bot integration and then you will create ten stations that authenticate through a captive WiFi portal.

In this example, we will be testing against a simple LAMP server on the upstream side of the AP. Do not use your LANforge server as the LAMP server because the routing will be difficult. In this chapter, a LAMP server is at 10.26.1.254, and there is an /etc/hosts entry for basic-portal to that address.

Basic Interactions of a Captive Portal

The basic order of operations of a captive portal are summarized in these steps:

1. A WiFi station accesses the LAN and is assigned a DHCP address.
2. The AP redirects any DNS and HTTP(s) request from the station. It returns either
   - a login page directly
   - a 301-Redirect to the login page
3. The station user submits this form. This form knows where to submit itself to, but it is possible that the form does not submit to the same address or service that it came from.
4. A successful authentication provides one of these responses:
   - The originally requested page, either as a 301-Redirect or as a proxied result.
   - A portal-div providing a logout or service menu and the original content inside.
   - A redirect page that uses javascript or meta-refresh mechanisms to tell the browser to reload the originally requested page.
Configuring a Demo Captive Portal

Provide Login/Logout pages

If you wish to set up a login and logout page on an Apache/PHP server to test with, you can copy the below files to the `/var/www/html` directory on the LAMP server.

login.php:

```php
<?php
valid = true;
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    if (!array_key_exists('username', $_POST)) {
        header("HTTP/1.1 400 Bad Request");
        header("X-err-no: 9400");
        header("X-err-msg: missing username");
        $valid = false;
    }
}
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<?php if($valid) {
<title>Login</title>
} else {
<title>Bad Request</title>
?>
<body>
<?php if ($_SERVER['REQUEST_METHOD'] == 'POST') {
<?php if(!$valid) {
<h1>Bad Request</h1>
<?php return;
} ?>
<?php
<?= $_POST['username'] ?> access granted.
<?php } else {  
<form method="post" action="">
<br />
<input type="text" name="username" value="" />
<input type="submit" name="login" value="Login" />
</form>
<?php }
?>
</body>
</html>
```

Provide a Redirect in lieu of Portal Capture

Getting a redirect to the login page does not have to be very complex. The portal-bot script will first start off requesting whatever URL you wish, so request `http://basic-portal/start`. Here is an Apache configuration line to redirect that URL to `login.php`:

```
httpd.conf

<Location /start>
```
Testing your redirect

You can use the command `curl -sv http://basic-portal/start` to test out the redirect you just created.

```
> curl -sv http://basic-portal/start
  * STATE: INIT => CONNECT handle 0x25bd9e8; line 1034 (connection #5000)
  * Added connection 0. The cache now contains 1 members
  * STATE: CONNECT => WAITRESOLVE handle 0x25bd9e8; line 1071 (connection #0)
  * Trying 10.26.1.254...
  * bind-local, addr: (nil) dev: (nil)
  * STATE: WAITRESOLVE => WAITCONNECT handle 0x25bd9e8; line 1151 (connection #0)
  * Connected to basic-portal (10.26.1.254) port 80 (#0)
  * Marked for [keep alive]: HTTP default
  * STATE: WAITCONNECT => D0 handle 0x25bd9e8; line 1229 (connection #0)
  * GET /start HTTP/1.1
  * User-Agent: curl/7.41.0-DEV
  * Host: basic-portal
  * Accept: */*
  * STATE: D0 => D0_DONE handle 0x25bd9e8; line 1314 (connection #0)
  * STATE: D0_DONE => WAITPERFORM handle 0x25bd9e8; line 1441 (connection #0)
  * STATE: WAITPERFORM => PERFORM handle 0x25bd9e8; line 1494 (connection #0)
  * HTTP 1.1 or later with persistent connection, pipelining supported
  * HTTP/1.1 302 Found
  * Date: Fri, 04 Sep 2015 22:52:53 GMT
  * Server Apache/2.4.7 (Ubuntu) is not blacklisted
  * Server: Apache/2.4.7 (Ubuntu)
  * Location: http://basic-portal/login.php
  * Content-Length: 290
  * Content-Type: text/html; charset=utf-8
  * <DOCTYPE HTML PUBLIC "-/"/IETF/DTD HTML 2.0//EN"
  * <html><head>
  * <title>302 Found</title>
  * </head><body>
  * <p>The document has moved <a href="http://basic-portal/login.php">here</a>.</p>
  * <hr>
  * <address>Apache/2.4.7 (Ubuntu) Server at basic-portal Port 80</address>
  * </body></html>
```

Using the Portal Bot bash script

Before we get straight to working with `portal-bot.pl`, let's see how it is used. Your LANforge installation has an example script called `portal-bot.bash-example` for you to copy and modify. This script is intended for you to login and logout separately. The LANforge manager will call `portal-bot.pl` differently when building up the station or tearing down the station, these actions are similar:

```
$ ./portal-bot.bash will log your station in
$ ./portal-bot.bash --logout will log your station out
```

Inside the bash script

The `portal-bot.bash` script is for exercising your `portal-bot.pl` script options from the command line while you develop with it. This is very close to the values you will place in the Ports->Misc/Post IF-UP field.

Switches you won't use in the GUI

You will never place the `PBOT_NOFORK` option in the Ports->Misc/Post IF-UP field because that will interrupt the processing of the LANforge Manager process. You will also never place `S*` in that field, either. You can place the `--verbose` and `--debug` flags in there, but it can fill your disk with log output more quickly.
Below is an example portal-bot.bash script with line-continuation characters formatted for clarity:

```
PBOT_NOFORK=1 ./portal-bot.pl \
  -dev sta100 \
  -bot bp.pm \
  -ip4 10.26.2.30 \
  -dns 192.168.100.1 \
  -mgt /dev/null \
  -delays 0,1,3 \
  -user "bob" \
  -pass "secret" 
  -ap_url "http://basic-portal/" 
  -start_url "http://basic-portal/start" 
  -login_form "login.php" 
  -login_action "login.php" 
  -logout_url "logout.php" 
  -verbose --debug $*
```

Below is the same script using short switches:

```
PBOT_NOFORK=1 ./portal-bot.pl \ 
  -i sta100 \ 
  -b bp.pm \ 
  -ip4 10.26.2.30 \ 
  -dns 192.168.100.1 \ 
  -mgt /dev/null \ 
  -delays 0,1,3 \ 
  -u "bob" \ 
  -p "secret" \ 
  -a "http://basic-portal/" \ 
  -s "http://basic-portal/start" \ 
  -n "login.php" \ 
  -o "login.php" \ 
  -t "logout.php" \ 
  -v -d $*
```

**Using the portal-bot.pl command on the command-line:**

A common misconception is thinking that `$*` is a command-line argument. It is only used in bash scripts. Do not put `$*` on the command-line.

```
PBOT_NOFORK=1 ./portal-bot.pl -i sta100 -b bp.pm -ip4 10.26.2.30 \ 
  -dns 192.168.100.1 -mgt /dev/null -u "bob" -p "secret" \ 
  -a "http://basic-portal/" -s "http://basic-portal/start" \ 
  -n "login.php" -o "login.php" -t "logout.php" -v -d
```

**Using the portal-bot.pl perl script**

**Tips:**

- First thing to do: edit a copy of that script and adjust it for your station device and it's IP address.
- Add `-d` to add more debugging messages. That makes `dbg()` statements print.
- Add `-print` after you get the script to work. This will print out the format of the arguments useful for putting the statements into the GUI Ports->Misc/Post IF-UP field.
The first six arguments are provided by LANforge when you use `portal-bot.pl` with a station. You want to populate these in your bash script, but not in the Post_IF_UP field.

**PBOT_NOFORK**

This environment variable tells the `portal-bot.pl` script to not fork. **Use it only when developing.** Omitting this is normal and allows for multi-processing of web requests from LANforge.

```
-l
  station name

--bot
  The bot plugin you provide

--ip4
  The IP of the station. This script is useless if there has been no DHCP lease.

--ip6
  Use `''` for no IPv6 address.

--dns
  The DNS addresses provided from the DHCP lease

--mgt
  The FIFO that signals the LANforge server. You don’t use it when testing.
```

The second set of arguments describe your own AP environment:

```
--user | -u
  portal user name

--pass | -p
  portal user password

--ap_url | -a
  A string to prepend to URLs when talking to the AP. Not necessary, but if you don’t use it, you have to provide fully qualified URLs to --login_form, --login_action, and --logout_form.

--start_url | -s
  The first URL requested from the AP, this should provide either a login page or a redirect to a login page. If you get your destination page (like, if you request baidu.com and actually get it), your station has probably not been logged out from the captive portal.

--login_form | -n
  This is what you request to get a login form. Often it is returned in the redirect, but sometimes you cannot get a cookie assignment if you do not request it specifically.

--login_action | -o
  Submit your login credentials to this URL.

--delays
  Comma separated list of seconds to delay at certain points:
1. $::delays[0]$ Used to delay the very first 'start_url' GET request
2. $::delays[1]$ Used to delay the first POST request in 'submit_login'
3. $::delays[2]$ Used to delay the 'submit_logout' request.
4. $::delays[3+]$ Your bot can utilize further delays if you specify

You may specify skips by adding a zero: \texttt{--delays\ 1,0,2}

You may specify a random time by using 'random': \texttt{--delays\ 1,random,2}

You may specify just one time for all delays: \texttt{--delays\ 2}

You may specify a random range: \texttt{--delays\ 3-20,4-25}

\texttt{--logout_form\ | -l}
Submit to this URL to log out of the captive portal

\texttt{-v -d}
Verbese and debug output, respectively.

\texttt{--print}
Skips process and prints out formatted arguments.

$\*$
Expands to all remaining shell arguments

We will connect to our LANforge system*. You want to copy this file to your own \texttt{./portal-bot.bash} file, edit it and then make it executable.

* You can connect via VNC, PuTTY or other SSH client.

* Use \texttt{chmod +x portal-bot.bash} to make your script executable.

Now let's see how to use this script with station \texttt{sta100}. Run the commands:

\begin{verbatim}
$ cd /home/lanforge
$ chmod +x portal-bot.bash
$ ./portal-bot.bash
\end{verbatim}

You will see a lot of output, it will show the contents of the web pages it finds.
Watching the Logs

Typically you won’t need to look at this output in the terminal, and you will not add `-d -v` flags to your LANforge stations. You very likely will need to check the log output from these scripts in case you need to diagnose connection problems during your test. Each virtual station leaves a log in the `/home/lanforge/wifi` directory, like `wifi/portal-bot.sta100.log`

```
> Watch logs using tail:
> tail -P wifi/portal-bot.sta100.log
```

Executing the LANforge `curl` commands yourself

To find the actual `curl` commands being executed, you want to `grep` the logs. Below is an example of grepping the logs and running the curl command.

```
$ cd /home/lanforge/wiki
$ grep Submitting portal-bot.sta100.log
```

You might noticed that some of the commands in the log might appear repeated, there are areas of redundant logging. There is a case where you can legitimately see repeated commands: when you have an `ifconfig` field configured for the port you are testing with. (Remember that the Post IF_UP field should be blank when developing the script.)

Remember, this `curl` command cannot be run without first doing a `source /home/lanforge/lanforge.profile` in your shell (our curl is a custom build). Here is an example. We take a command similar to the one above, add `-qv` and cancel it using `^C`:

```
$ cd /home/lanforge
$ source /home/lanforge/lanforge.profile
# add -qv to see header details
$ /home/lanforge/local/bin/curl -qv -SLki -c /tmp/sta100_cookie.txt -b /tmp/sta100_cookie.txt -4 --interface sta100
```

Explaining the `curl` Command

There are many arguments to the `curl` command, but in general, you should be able to copy and paste the command into a terminal and it should work (see note about `lanforge.profile` above). Below is an example of a `curl` command, with `\` characters as line-continuation marks, formatted for clarity.

```
$ /home/lanforge/local/bin/curl -qv \
-\n SLki \
- c /tmp/sta100 cookie.txt \
- b /tmp/sta100_cookie.txt \
-4 \
```
Your `portal-bot.pl` script is intended to be a way of focusing on the development of your bot plugin and not repetitively typing a long curl command.

Writing your Bot Plugin

Your bot plugin, the Perl module you will write for your captive portal, is central to the operation of the portal-bot.pl script. It is also important that you do not alter the `portal-bot.pl` script unless absolutely necessary, because your changes could be overwritten by upgrades. Any alteration to the time at which the `fork()` call is made in this script can make the LANforge server grind to a halt.

Only edit your bot perl module, please.

The Bot Subroutines

The example bot, bp.pm, provided with LANforge defines four subroutines, in order:

find_redirect_url

This subroutine receives the response of the HTTP(S) GET of your --start_url parameter. Look through this to see if:

- you are already getting destination content--if so, you were not logged out,
- you get a login form directly and not a redirect,
- or you get a redirect to a login page (possibly on a separate port like :8080)

If you get a redirect to another port, compare the --login_url value to this. If it is different, consider updating your login_url parameter.

There might be many form parameters, like ones for a session id, a PHP_SESSID, a cookie, a base64 encoded string indicating your originally requested url (or just a plain URL-encoded url), and any possible co-branding...
parameters that might indicate any advertising campaigns associated with this captive portal. Missing some of these might make submitting the form give you an error. Store these values as necessary in your bot:: namespace. You do not submit your login page in this method.

i Define a package scope variable using our $thing; after your package statement.

submit_login

Here is where you submit your login page forms. The botlib::request() function is provided to make GET and POST requests verbose logging and debugging. The page is returned as lines in the @response array.

```perl
my $post_data = "username=" . uri_escape($user_name);
my @response = ();
request({
  'curl_args' => $::curl_args,
  'url' => $post_url,
  'method' => 'POST',
  'delay' => '0,3', # see --delays option
  'post_data' => $post_data,
  'print' => 1},
  @response);
```

The submit_login function uses the $::delay[1] parameter if --delays were set. See paragraph on randomDelay.

interpret_login_response

Here you determine if you are getting an access denied error or are being forwarded to your original start_url destination. Set your $result variable to OK or FAIL. Use the log() method to add information for the wifi/portal-bot log.

In order to add events, such as page load time, you want to use the botlib::newEvent() function:

```perl
my $page_time = botlib::time_milli() - $::start at;
newEvent("portal_login: $result", $page_time, $::dev);
```

Your event log will gain messages like these:

```
 Logged in to: jeditest:4002 as: Admin
```

get_explanation

Some web applications can provide customized error messages in their response. You can add a get_explanation() function to your bot to collect this information. The botlib::dbgdie() method will take advantage of this method if available. Below is an excerpt from the method found in bp.pm:

```perl
sub get_explanation {
  for $line (@$ra_result) {
    ($err_code) = $line =~ /^X-err-no: (.*)$/;
    if ($line =~ /^X-err-no: /);
    ($err_msg ) = $line =~ /^X-err-msg: (.*)$/;
    if ($line =~ /^X-err-msg: /);
  }
  return "$err_code, $err_msg";
}
```
Notice how this parses out the HTTP headers found if the parameter `username` were missing when doing a POST to `basic-portal/login.php`:

```
header("X-err-no: 9400");
header("X-err-msg: missing username");
```

You will see these messages show up in the LANforge Events log:

![LANforge Manager](image)

```
submit_logout

Many captive portals do not publicise their logout URLs, so it might be available only on an admin page for the AP. You will know when the logout_uri parameter works if you can do a logout with that station, and then successfully log back in using the same station and seeing the captive portal sign-in page again.

randomDelay

The delay parameter to `botlib::request()` has many overloads to the call:

- A simple number is a simple delay in seconds. No other units are used.
- If you specify `random` in the delay parameter, the `botlib::randomDelay()` is called, producing a range between [1 - 119] seconds.
- If you specify `3-16`, `randomDelay(3, 16)` is called to produce a random range between [3 - 16] seconds.
- If you specify two numbers separated by a comma, it looks at your `@::delays` list, and picks the second argument if it can, the last item of `@::delays` if the list is too short, or the first argument if there are no items in the delay list.

We have now covered all of the scripting development areas for the `portal-bot.pl` plugin you will write.

**Configuring your Stations**

**A Single Station**

We assume you have `portal-bot.bash` working at this point. This is how you can configure a single station:

1. Use the `portal-bot.pl --print` command to print out the arguments.
2. Copy the result (starting with "portal-bot.pl") into the Port->Misc window. Avoid populating this field while you are developing the script! If you place a value into that field, your portal-bot script will not only execute, but the Manager process will also execute the script specified in the POST IFUP field. This can be really confusing.
Multiple Stations

To get multiple virtual stations logging in at once using the GUI, we just need a few of those parameters for the station configuration. We will use the Batch Modify feature to alter a series of stations.

1. In the Port tab, create a series of stations. In this example we will create them with:

- Port: wiphy2
- Select DHCP-IPv4
- Quantity: 10
- STA ID: 300
- SSID: jedtest
Passphrase: jedtest1
Select WPA2
Select Down

2. Highlight them and click **Batch Modify**.

3. Click the **Down** button.

4. In your terminal, invoke the `portal-bot.bash` with the `--print` argument:

```
./portal-bot.bash --print
```

5. Use the [*] button to expand to Box 2. We will enter the following version of our command into the Post IF-UP
Click OK

6. In the Ports tab, double click sta300 and in the Misc Configuration tab, you will see the Post IF-UP Script values.

Testing a Station

Exercising these stations starts with bringing them up and down using the Batch Modify tool.

1. Highlight one station, **sta300**, and click **Batch Modify**.

2. Click the **Down** button to admin-down the station.

3. In a shell on the LANforge, got to `/home/lanforge/wifi` and tail the log for station 300:

```
tail -f portal-bot.sta300.log
```
4. Click the Up button to admin-up the station.

5. Click the Portal Login button force the station to login if you do not see any messages in the log file you are failing.

Troubleshooting Techniques

If your station cannot talk to the captive portal, like you have a time-out, these steps will help identify where there is a misconfiguration:

1. **Ping the portal from LANforge**: `ping basic-portal`

2. **Ping the portal from sta300** `ping -I 10.27.0.16 basic-portal`
3. Use `curl` to download the portal page by hand: `curl -sv http://basic-portal/login.php`

4. Check the `route` on the portal side if you are routing. Some examples:

   ```
   route -n
   route add -net 10.27.0.0/23 gw 10.26.1.1
   ```

5. Check access logs for the portal. There might be a hostname issue.

   ```
   root@atlax:/bitwise/x64_bitwise
   > route -n
   Kernel IP routing table
   Destination Gateway Genmask Flags Metric Ref Use Iface
     0.0.0.0     192.168.100.1   0.0.0.0    UG 0 0 0 br0
    10.26.0.0    0.0.0.0    255.255.255.0    U 0 0 0 br0
       10.26.1.0    0.0.0.0    255.255.255.0    U 0 0 0 br2
       10.26.2.0    0.0.0.0    255.255.255.0    U 0 0 0 br0
       10.26.3.0    0.0.0.0    255.255.255.0    U 0 0 0 br1
    192.168.100.0    0.0.0.0    255.255.255.0    U 0 0 0 br0
   > route add -net 10.26.2.0/24 gw 10.26.1.1
   ```

   ```
   root@atlax:/var/log/apache2   Terminal
   root@jedtest/home/is...   root@jedtest/home/is...
   > ls -ll var/log/apache2
   ```

   ```
   root@atlax:/var/log/apache2   Terminal
   root@jedtest/home/is...   root@jedtest/home/is...
   > ls -ll var/log/apache2
   ```

**Using the Port Bringup Plugin**

Using the Port Bringup Plugin is a much more fun way to get data than looking at log files.

1. In the Plugins menu, select Port Bringup Test.
2. Highlight a series of stations and click Add Port:

3. Click Start

4. You will see the reporting window. It often takes many seconds or a few minutes for stations to acquire DHCP addresses and start reporting information into the plugin.
WiFi Captive Portal Login

Goal: Create many user sessions to a WiFi captive portal gateway.

Airports, arenas and coffee shops often offer open WiFi service that is gated with a web sign-on form. This is called a captive portal. LANforge can run a custom login script on a virtual station to emulate sign-in on the captive portal web page. The following example will create one hundred stations and have them authenticate through a captive WiFi portal.

1. Prepare a portal login script (`lf_ifup_post`)
2. The `lf_ifup_post` script will be called after DHCP assignment for a station occurs. It can also be called before DHCP release. This script is called from the LANforge resource hosting the virtual station.
   A. The script should be in directory `/home/lanforge/`.
   B. LANforge will pass these arguments to the script
      A. `-i` - station device
      B. `--ip4` - station ip address
      C. `--ip6` - station ipv6 address
      D. `--dns` - station DNS address
      E. `--mgt` - pipe name for reporting results to LANforge
   C. Custom parameters to the script can be provided.
   D. The script can have another name.
   E. LANforge expects these return values:
      A. `OK`
      B. `FAIL`
      C. `FAIL:reason`, this provides feedback on failure occurrence.
3. Create WiFi stations
   A. In the Ports tab, select wiphy1 and click Create

![LANforce Manager](image)

B. In the Create VLANS window, craft ten wifi stations:

![Create VLANS on Port: 1.1.03](image)

   A. Select WiFi STA
   B. For MAC address, choose **xx:xx:xx:**:*:*:xx
   C. Select DHCP-IPv4
   D. Enter Quantity **100**
   E. Specify **0** for STA ID
   F. The example SSID for this cookbook is **jedtest**
   G. Select the **Down** option. This postpones the stations making a DHCP request until they are explicity admin up.
   H. ...and then click **Apply**
C. You will see ten station created:

![Image of LANforge Manager screen showing ten stations]

4. Batch Modify Stations in order to update `1f_ifup_post` parameters

A. Highlight stations and click Batch Modify

![Image of LANforge Manager screen with Batch Modify button highlighted]
B. In the Batch Modify screen, click the + button and expand to Group 2.

C. Edit the IF POST field. Enter the file name and any extra arguments that the script will want for this port. Example: `if_ifup_post --user bob --pass secret --url http://slashdot.org/`

D. Click the Apply button to apply the changes. Do not close the window yet.
5. Testing a station. We will toggle it up and down and look at the logs to find problems.
   A. Highlight one of your stations in the Ports tab.
   B. Set the Report Time to 1s and click **Apply**
   C. In the Batch Modify window, click the **Up** button. This is the same as setting **Up/Down** to **UP** and clicking **Apply**
   D. Watch the Wireless Messages and LANforge Messages windows for error messages. The Ports tab will update the station status.

6. Use the Batch Modify window to **Force DHCP Renewal**
   A. Click **Down**
B. click Clear DHCP

C. click Up

7. Use the Batch Modify window to Re-Login to Portal
   A. Click Portal Re-Login
   B. If you wanted to change other parameters:
   C. Click Down Logout
   D. Set Up/Down to Down
   E. Change another station parameters and then click Apply
   F. Click Up

8. Use the Batch Modify window to Change station MAC addresses

A. Click Down

B. Set MAC Addr to xx:xx:xx:*:*:* randomize the mac address
LANforge WiFi Many vAP Testing

Goal: Create 7 vAP on a single a/b/g/n/AC radio to emulate a busy environment and test that station devices associate to the proper AP.

Requires LANforge 5.3.3 or later. Configure 7 vAP, add the vAP to a bridge and set up DHCP. The Device Under Test (DUT) in this case is a mobile handset or other wifi station device. Verify that station can handle many APs and select an appropriate AP from the available scan results. This example uses a LANforge CT523 system but the procedure should work on all CT521, CT522, CT523 and CT525 systems.

1. In the Ports tab, select the radio wiphy2 and click Create. Configure the values appropriately and click create.

2. In the Ports tab you will see the new WiFi vAP:
3. Select the **Status** panel in the LANforge GUI, and click the Netsmith button for the appropriate resource. Right-click and select the ‘New Bridge’ option. In this example, I selected ‘br2’ as the bridge name. After creating the bridge, click Sync to show the new bridge device. Right-click on it and select Modify Port. Add each of the vAP you just created to the bridge and then apply:

4. Create a virtual router in Netsmith and add br2, and optionally a wired port (eth1) to the router. Double-click the br2 port and configure DHCP to match its IP address. When complete, Netsmith should look something like this:
5. Now, we should have 7 vAP able to accept stations and give out DHCP addresses. Depending on the DUT, the user may wish to run iperf on LANforge, or on an upstream device connected to the LANforge eth1 port. For an initial test, make sure the DUT can connect to one of the vAP and get an IP address. The DUT should also see each of the vAP in its listing of available APs. This example will use LANforge WiFi Station on a different radio as the DUT. Here is a listing of the scan results:

<table>
<thead>
<tr>
<th>SSID</th>
<th>Channel</th>
<th>Info</th>
<th>Auth</th>
<th>BSSID</th>
<th>Signal</th>
<th>Frequency</th>
<th>Reason</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-20.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-18.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-18.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-18.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-21.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-21.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
<tr>
<td>ben-ota2-1</td>
<td>149+</td>
<td>3x3 MCS 0-9 AC</td>
<td>Open</td>
<td>04:0f:01:84:07:03</td>
<td>-21.0</td>
<td>5745</td>
<td>240</td>
<td>2.83 m</td>
</tr>
</tbody>
</table>

6. To make it a bit more interesting, we will now set the operating modes for one AP to be 802.11a, a second to be 802.11n, and the rest will remain 802.11AC. These APs are running on channel 149, so b and g mode are not available on this radio. To set the mode, double-click the vap200 row and set the Mode to be 802.11a and click OK to apply. Use similar procedure to set vap201’s mode to 802.11an:
7. Now, request the DUT to re-scan and re-associate to the network. There should now be one 802.11a, one 802.11n, and one 802.11ac VAP in the scan results. A well-behaved DUT should attempt to connect to the AP with the highest rate that the DUT supports. In this case, the LANforge Station properly selected the 802.11ac VAP:

8. For additional testing, you may wish to use additional LANforge radios to create more VAPs. Change the SSID and configure the DUT to connect to a particular SSID, admin down the VAP to make sure the DUT will properly connect to a new AP, and much more. You may also run traffic on the different APs to ensure that if a DUT connects to a 802.11a AP, then it does not try to send any 802.11n (HT) encoded traffic. A LANforge radio configured for monitor mode could verify this, as could third-party sniffers.
LANforge WiFi Degraded vAP Testing

Goal: Create 1 vAP on a single a/b/g/n/AC radio and configure it to drop 50% of management frames to test that station devices can handle lost management frames properly.

Requires LANforge 5.3.2 or later. Configure 1 VAP, add the vAP to a bridge and set up DHCP. The Device Under Test (DUT) in this case is a mobile handset or other wifi station device. Verify that station can handle associating with an AP that drops many management frames. This example uses a LANforge CT523 system but the procedure should work on all CT520, CT521, CT522, CT523 and CT525 systems.

1. In the Ports tab, select the radio wiphy2 and click Create. Configure the values appropriately and click create.
2. In the **Ports** tab you will see the new WiFi vAP:

3. Select the **Status** panel in the LANforge GUI, and click the Netsmiith button for the appropriate resource. Right-click and select the 'New Bridge' option. In this example, I selected 'br2' as the bridge name. After creating the bridge, click Sync to show the new bridge device. Right-click on br2 and select Modify Port. Add the vAP you just created to the bridge with the Add Ports button and then apply:
4. Create a virtual router in Netsmith and add br2, and optionally a wired port (eth1) to the router. Double-click the br2 port and configure DHCP to match its IP address. When complete, Netsmith should look something like this:
5. Now, we should have 1 vAP able to accept stations and give out DHCP addresses. For an initial test, make sure the DUT can connect to the vAP and get an IP address. Once that is verified, right-click and choose Port Modify on the vap200 vAP. We will now configure it to not respond to 50% of the management frames sent to it:
6. In this case, we are using open authentication, but it would also be good to test with encryption (WPA2 PSK, for instance) to make sure that the DUT can handle failures of the 4-way authentication handshake, for instance.

7. To verify the results, use a sniffer to watch the association requests and responses. A LANforge radio configured for monitor mode could verify this, as could third-party sniffers. In the capture below you can see that the station had to make two Authentication requests before the AP would answer (because the AP is set to randomly ignore 50% of the association requests):

```
6
7
```
A. Also in Wireshark, go to the **Statistics** menu and select **IO Graphs** to display up to 5 graphs based on the available frames in the capture file.

B. The two images below have been annotated to show the behavior of 10 stations being reset every 30 seconds while their vAP history has increasing impairment of management frames.
Multiple Stations with a Hunt Script

Goal: Do packet sized testing with a hunt script using multiple stations.

We will manipulate the parameters of 10 Layer 3 connections using a single hunt script. The WiFi stations will change packet size as a group by being part of a Test Group. In this scenario, we will create traffic to different upstream destinations using MAC VLANs, and the AP wired up to eth1 of our LANforge machine. Requires a CT-520 for only stations, or a CT-523 if you also want a WiFi monitor station.

1. Create 10 virtual stations: in the Port Mgr tab, highlight radio wiphy0 and click the Create button. In this scenario, we are using SSID jedtest.
A. Select WiFi STA
B. Check DHCP-IPv4
C. Quantity: 10
D. Station ID: 0
E. SSID: jedtest
F. Click Apply and then close the window.
G. You should see stations sta0 - sta9.

For more information see creating virtual stations

2. (Simple Method) This method only requires setting the IP on eth1. In this scenario, our upstream network is 10.26.1.0/24. In the Port Mgr tab, highlight eth1 and click Modify.

A. IP: 10.26.1.10
B. IP Mask: 255.255.255.0
3. (Optional Advanced Method) Create ten MAC VLANs on the `eth1`. In this scenario, our upstream network is `10.26.1.0/24`. In the **Port Mgr** tab, highlight `eth1` and click **Create**.

A. Select MAC-VLAN
B. Quantity: 10
C. IP: 10.26.1.11
D. IP Mask: 255.255.255.0
E. Gateway: 10.26.1.1
F. Click **Apply** and close the window.
G. You should see 10 MAC VLANs, `eth1#0` - `eth1#9`.

4. Create ten Layer-3 cross connects. We will start at 10Mbps transmit on them as a reasonable start. In general hunt scripts start low and try to work their way higher. When using more stations, set a lower starting transmit rate. In the Layer-3 tab, click **Create**.
A. Name: **sta-mac-0**

B. Endpoint A: eth1 (if using the advanced MAC-VLAN method, set this to **eth1#0**).

C. Endpoint B: sta0

D. Type: LANforge / UDP

E. Min Tx Rate: 10Mbps (both sides)

F. Click **Apply**. Leave the window open.

5. Create nine more stations. Click **Batch-Create**.
A. Quantity: 9
B. Deselect Zero Pad.
C. If only eth1 is used for upstream traffic, set Port Increment A to 0. Otherwise leave it at 1.
D. Click Apply and close window.
E. Close the Create/Modify Cross Connect window.

6. You will see ten Layer-3 connections in the Layer-3 tab.

7. Create a Test Group. In the Test Group tab, click Create.

A. Name: sta-mac
B. Select Config As Totals.
C. Highlight all the sta-mac-x connections and click ← Add Cx.
D. Click Apply.
E. Click Script.
F. Configure the Test Group Script.

A. Group Name: sta-mac
B. Script Type: ScriptHunt
C. Script Name: start-10Mbps
D. Starting Rate: 10M
E. Click OK.

G. Close the Create Test Group window.

8. Start the test. Highlight the test group and click Start.
9. You will see the script report window.

10. When the test is finished, click **Graphical Report** to see graphs.
Max Peer RX-Bits-per-second v/s Packet Size

- Peer RX DPS
- Packet Size

- 7,837,878,293
- 32,240,000
- 60,199,056
- 83,642,237
- 98,543,891
- 117,077,401
- 111,410,467

CSV Data for Graph Above

Close  Save File
Running UDP Traffic with Android

Goal: Set up Android to be a LANforge resource and then run UDP traffic.

Requires LANForge 5.3.3 or later. Make sure to configure a realm other than 255 for the VAP system, this is because the Android device needs to be in the same realm to be managed. This cookbook will be using realm 195. You can find information on configuring realms using ifconfig starting from step 4 here.

This cookbook will go through installing and configuring LANforge on an Android device, then setting up a Layer-3 UDP connection between the Android device and another LANforge system. Multiple VAPs will be set up to demonstrate roaming. A bridged VAP setup is used (with the bridge as DHCP server) so the device can retain the same IP during roaming, this prevents the device from having to renew its IP saving some time between roams.

1. First, we will set up the LANforge system so the Android device can connect.
2. Create the first VAP;
A. Go to the Port Mgr tab.

B. Select wiphy0 and click Create.
C. Select WiFi VAP and enter in the below values.

A. **Quantity 1**
B. **STA ID: 0**
C. **SSID: android-test**

D. Click **Apply**.

A. **Note**: we will keep this window open for creating the second VAP.

3. Create the second VAP.

A. Select **wiphyl** from the port drop-down menu.
B. Update the **STA ID** and **SSID** with the below values.
   A. **STA ID: 1**
   B. **SSID: android-test2**
C. Click **Apply** and close the Create Port window.

4. Set up a bridge for both VAPs.
A. Go to the **Status** tab, and click the **Netsmith** button for the AP system (Resource 1 in this example).

B. Right-click in the Netsmith window and select **New Router**.

A. Click **OK** to accept the default values.

B. Click **Apply** in Netsmith.
C. Right-click in the Netsmith window and select **New Bridge**. Then set the below values.

A. Quantity: 1

B. Bridge Name: `br0`

C. IP Address: 195.1.2.1/24

D. Click **Apply** and close the Create Port window.

E. Click **Sync** in Netsmith and the `br0` interface should appear.

F. Drag the `br0` interface into the virtual router. The interface box should change from black to green.
G. Right click br0 and select modify.

H. Select **DHCP** and use the below values.

   A. DHCP Lease Time: **300**
   B. DHCP DNS: **195.1.2.1**
   C. DHCP Range Min: **195.1.2.10**
   D. DHCP Range Max: **195.1.2.20**

I. Click **OK**.
J. Right click br0 and select **Modify Port**.

A. Enter **vap0** and **vap1** into the text box as shown above.

B. Click **Add Ports**.

C. Click **Apply** then **Sync**. The Current Ports column should now show vap0 and vap1.

```
<table>
<thead>
<tr>
<th>Configured Ports</th>
<th>Current Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>vap0</td>
<td>vap0</td>
</tr>
<tr>
<td>vap1</td>
<td>vap1</td>
</tr>
</tbody>
</table>
```

D. Click **OK** to close the window.

K. Click **Apply** in Netsmith.

5. Create a redirect-device inside the virtual router. The Android will connect to this port for management purposes.
A. Right-click in the Netsmith window and select **New Connection**.

B. Select the **Skip** checkbox for Port 1-B, WanLink, and Port 2-B.

C. Click **OK**

B. Click **Apply** in Netsmith.

C. Drag one of the rdd interfaces into the virtual router (rddVR0 is used in this example). The interface box should change to green.

A. **Note:** The other rdd (rddVR1 in this case) will not be used and can be ignored.
6. Set up the Android device.

   A. Install LANforge Resource from the Google Play Store.
B. Once installed, connect your device to **android-test** using Android’s WiFi setup.

C. Launch the LANforge Resource app and set the values below.

A. Realm 195
B. Manager IP:port: 195.1.1.1
C. Resource ID: 2
7. Create and run a Layer-3 UDP connection.

   A. Go to the **Status** tab, and click the **Netsmith** button for the AP system (Resource 1 in this example).

   B. Create a redirect-device inside the virtual router.
A. Right-click in the Netsmith window and select **New Connection**.

B. Select the **Skip** checkbox for Port 1-B, WanLink, and Port 2-B.

C. Click **OK**.

D. Click **Apply** in Netsmith.

E. Drag rddVR2 into the virtual router. The interface box should change to green.

F. Click **Apply** in Netsmith.
G. Right click rddVR2 and select **Modify Port**.

I. Set the **IP Address** to **195.1.3.1/24**
II. Click **OK**.

H. Right click rddVR3 and select **Modify Port**

I. Set the **IP Address** to **195.1.3.2/24**
II. Set the **Gateway IP** to **195.1.3.1**
III. Click **OK**.

I. Close Netsmith.
C. Go to the Layer-3 tab, click Create.

D. Set the below values. Note that Endpoint B Resource will differ depending on the Android device type.

A. CX Name: **android-udp**

B. Endpoint A Resource: **brent-523**

C. Endpoint B Resource: **Nexus**

D. Endpoint A Port: **br0**

E. Endpoint B Port: **wlan0**

F. Endpoint A Min Tx Rate: **T1 (1.544 Mbps)**

G. Endpoint B Min Tx Rate: **Zero (0 bps)**

H. Report Timer: **fast (1 s)**

I. Click OK.
E. Start running traffic.

A. Select the android-udp connection.

B. Click Start.

F. Connect your Android device to **android-test2**. Traffic should start flowing again after about 20-30 seconds.
Verifying Android QoS

Goal: Set up Video and Best Effort QoS connections and verify results.

In this example, LANforge-FIRE is used to set up two connections, one running video QoS traffic, the other with Best Effort QoS traffic. The latency and drops will be compared and wireshark will be used to verify QoS information.

1. Connect the Android device to a LANforge system. You can use the cookbook here for tips: Running UDP Traffic with Android
2. Create two connections between the Android device and a LANforge port. One for Best Effort QoS traffic, one for Video QoS traffic.
A. Creating a Best Effort UDP connection.

B. Creating a UDP connection with video QoS traffic.

A. Set a name for the connection (android-udp-ul-be-100k) in this case.
B. Select your ports. In this case the connection is between the Android (wlan0) and a bridge (br0).
C. Set Min Tx Rate on Endpoint A to DOCSIS 1 (30 Mbps).
D. Set Min Tx Rate on Endpoint B to New Modem (56 Kbps).
E. Make sure IP ToS on both endpoints is set to Best Effort.
F. Set Pkts to Send to 100000 on Endpoint A. Note: Because Android is being managed in-band, this limit should prevent losing management frames that could contain reporting data.
G. Set Min IP Port to 7777 on Endpoint A. A custom port is used to help identify the connection type in wireshark.
H. Set Multi-Conn to 1 for both endpoints. This is so each endpoint is running on its own process.

A. Set a name for the connection (android-udp-ul-vi-100k) in this case.
B. Select your ports. In this case the connection is between the Android (wlan0) and a bridge (br0).
C. Set Min Tx Rate on Endpoint A to DOCSIS 1 (30 Mbps).
D. Set Min Tx Rate on Endpoint B to New Modem (56 Kbps).
E. Set IP ToS on Endpoint A to VI (WiFi).
F. Set Pkts to Send to 100000 on Endpoint A. Note: Because Android is being managed in-band, this limit should prevent losing management frames that could contain reporting data.
G. Set Min IP Port to 7778 on Endpoint A. A custom port is used to help identify the connection type in wireshark.
H. Set Multi-Conn to 1 for both endpoints. This is so each endpoint is running on its own process.
3. Compare latency and drops.

   A. The latency can be found under the **Delay** column.

   B. The drops can be found under **Dropped** column.

   C. If QoS is working properly, you should see less delay (latency) and less drops for connections using VI (WiFi) IP ToS. The delay can be more easily compared if you add endpoint A and B of each connection. As should be expected, the results above show that the particular device is dropping significantly less packets for the connection with video QoS traffic. Because there is a small amount of latency, a major difference isn't shown here.

4. Verify QoS type with wireshark. This is where our custom port setting is helpful.

   A. The packets on port 7777 should show **Best Effort**.
Goal: Create a Test Group that uses ScriptHunt to maximize the total rate of multiple connections based on desired constraints.

ScriptHunt is a script that runs connections or 'iterates' and changes tx-rates until a maximum acceptable tx-rate is reached. This can be done for multiple payload sizes and attenuations. Using a Test Group along with ScriptHunt allows you to test multiple connections at the same time.

This cookbook assumes ports and connections are already created and configured. The following areas will be covered:

- Creating and Configuring Test Groups
- ScriptHunt setup
- Running ScriptHunt and checking results
- Using additional Test Groups for alternate tests

1. It is a good idea to verify connections are running as expected before getting started. The connections below are testing UDP download on 10 wireless stations.
2. Create and Configure Test Group(s).

   A. In the Test Group tab, click **Create**.

   ![Create/Modify Test Group](image)

   A. Give the Test Group a **Name**. The name used here is ‘scripthunt-group-01’

   B. Under Free CXs, shift-select the connections you want in the group and click **Add Cx**.

   C. Select the **Config As Totals** checkbox. This makes it so the tx-rate is based on a combination of all connections instead of individually.

   D. The Test Group must be created before setting up the script. Click **Apply** to create it.

   B. Click **Script** to open the Add/Modify Script window.
A. In the **Script Type** drop-down menu, select ScriptHunt. 
   **Note:** Most options will be left default for now (all but Run Duration and Payload Sizes A). Below are quick summaries of the drop-down options.

B. **Run Duration:** Determines how long each iteration lasts. This should be about 15-20 seconds minimum. This test will use 20s.

C. **Pause Duration:** Sets how long the script waits between each iteration.

D. **Starting Rate:** Sets the first tx-rate the script attempts.

E. **Max Iterations:** Allows you to choose a maximum amount of times you want the script to iterate as it adjusts the rate.

F. **Max Drop Percent:** Determines the acceptable range of drops for an iteration. In this case if there are more than 5% drops, the current iteration will fail and the next will attempt to make adjustments so there are less drops.

G. **Max-Tx-Underrun:** With the current setting of 10%, if the actual tx-rate is running 10% slower than the attempted tx-rate, the iteration will fail.

H. **Max Jitter:** Determines the acceptable maximum jitter for an iteration.

I. **Max RT Latency:** This determines the maximum acceptable round-trip latency for an iteration.

J. **Threshold:** If the percent difference of tx-rate from iteration to iteration reaches the value here or less, the script will finish unless there are additional payloads/attenuations to test.

K. ScriptHunt will find the highest acceptable rate for each payload size listed in **Payload Sizes A and B**. The existing values are suggestions, but any desired value[s] can be entered here. If you wish to test Payload Size B, the **Symmetric** checkbox must be enabled. **Attenuations (dB)** are tested similarly, a Candela attenuator is required and must be connected then selected in the Attenuations drop-down menu. In this specific test, ScriptHunt will just test a payload of 1472 (on endpoint A only) and no attenuations.

L. Click **OK** to add the script.

M. Click **OK** in the Create/Modify Test Group window to close it.

3. Start the Test Group and view the results.
A. Select the Test Group and click Start.

B. Examine the results.

A. After each iteration completes, the results will update with various information on said iteration.
B. When Script Hunt finishes, the results will show a summary of all iterations. This data shows how high the rates reached and which failure constraints the iterations hit. This particular test reached about 429 Mbps tx-rate within the specified constraints. Notice how the configured rate (cfg-rate (bps)) adjusts up and down as the drop percent (drop% peer) goes lower and higher than the 5% constraint set earlier.

4. Create another Test Group with alternate Script Hunt settings.
   A. We will essentially copy the last Test Group, then change Script Hunt settings. Select ‘scriphunt-group-01’ and click Modify.

A. Change the Test Group Name to ‘scriphunt-group-02’.
B. Click OK.
B. Select scripthunt-group-02 and click **Modify**.

C. Click **Script**.

A. Set the **Script Type** to **ScriptHunt**.

B. Again, **Run Duration** should be 15-20s minimum. It is set to **20s** for this test.

C. Since the only constraint limiting the first Test Group was **Max Drop Percent**, we'll raise it to **10%** and compare the results.

D. Remove all but **1472** in **Payload Sizes A**.

E. Click **OK**.

F. Click **OK** in the Create/Modify Test Group window.

D. Be sure 'scripthunt-group-01' is stopped! If you have two different ScriptHunts running on the same connection(s), they will try to fight each other.
E. Select 'scripthunt-group-02' and click Start.

F. Observe the results summary.

A. Compare the two results final tx-bps. The first test group got 429 Mbps at 5% maximum drops. Because the second Test Group's ScriptHunt was set at 10% maximum drops, it was able to achieve a higher tx-bps of 444 Mbps.
Goal: Associate a station to an AP with the WPS Push and PIN methods.

In this test scenario, a LANforge CT523 is used to simulate a station connecting to a commercial AP with WPS Push mode and also with WPS PIN mode. Currently this test requires the use of a terminal on the LANforge system to run some WPS commands.

1. Create a virtual wireless station.
A. Go to the **Port Mgr** tab.

B. Check wiphy0 settings by selecting wiphy0 and click **Modify**.

A. If the **Down** checkbox is selected, Click **Set IF Down** on the left, then uncheck the **Down** checkbox.

B. Make sure **Channel/Freq** is set to **AUTO**.

C. Click **OK**.
C. Back in the Port Mgr tab, select port wiphy0 and click Create.

A. Select WiFi STA.
B. Select DHCP-IPv4.
C. Set Quantity to 1.
D. Set STA ID to 0.
E. Set SSID to [BLANK]. Don't forget to add the brackets.
F. Click Apply.

2. Create a wpa_supplicant.conf file.
   A. Open a terminal on the LANforge system.

   B. Create the file wpa_supplicant.conf in /etc that contains the below text. Alternatively, the command in the next step can be used to create the file.

      ```
      ctrl_interface=/var/run/wpa_supplicant
      ctrl_interface_group=0
      update_config=1
      ```
C. In the open terminal run the below command to create the wpa_supplicant.conf file.
   **NOTE**: Please make sure wpa_supplicant.conf doesn’t already exist in the `/etc` directory.

   First become root:  `su -`
   Then run:
   ```bash
   if [ ! -f '/etc/wpa_supplicant.conf' ]; then printf '%s
' ctrl_interface=/var/run/wpa_supplicant ctrl_interface_group=0 update_config=1 > /etc/wpa_supplicant.conf; fi
   ```

D. Keep in mind the wpa_supplicant.conf file will save AP information for stations. If you want a station to forget the AP information, you’ll need to recreate the wpa_supplicant.conf file.

3. Configure sta0 to use a the wpa_supplicant.conf file created in step 2.
A. Select sta0 in the Port mgr tab and click Modify.
8. In the Misc Configuration tab, select Custom WPA Clg then inside the text field for WPA Clg, add the path of the wpa_supplicant.conf file. In this case, we’ll be using /etc/wpa_supplicant.conf

C. Click OK.

4. Associate the station using WPS Push mode.

   A. In a terminal on the LANforge system, enter in the below command and then push your AP’s WPS button. If you aren’t root, use su -.

   ```bash
   wpa_cli -i sta0 wps_pbc
   ```

   ```bash
   Root@brent-523:~
   ```
B. Your station should now associate and get an IP.

**Note:** The SSID field in the sta0 Modify window will remain as [BLANK]. You also may see a different SSID in the View Details window, this is a bug and can be ignored for now as long as the BSSID is correct.

5. Associate the station using **WPS PIN mode**.

   A. Obtain your AP's BSSID and WPS PIN. This information can usually be found on the AP label or in the AP's software.

   B. In a terminal on the LANforge system, enter in the below command. Replace the x's with the BSSID and numbers with the PIN. If you aren't root, use `su -`

   ```
   wpa_cli -i sta0 wps_reg xx:xx:xx:xx:xx:xx 12345678
   ```
C. Your station should now associate and get an IP.

**Note:** The SSID field in the sta0 Modify window will remain as [BLANK]. You also may see a different SSID in the View Details window, this is a bug and can be ignored for now as long as the BSSID is correct.
Test WiFi MU-MIMO Download.

Goal: Test WiFi MU-MIMO station Download, one 2x2 station, one 1x1.

Test WiFi MU-MIMO station Download using two MU-MIMO capable radios. One radio will emulate a 2x2 station, and a second will emulate a 1x1 station. When testing MU-MIMO, only a single station can be used per radio. For additional non-MU-MIMO station emulation, additional radios can be configured for multiple station virtual devices. This example uses a system similar to the LANforge CT525 system. It is configured with 4 radios; Two of the 4x4 MU-MIMO radios are used for MU-MIMO testing. The other two are not used in this test scenario. This procedure should work on any system that can support at least 2 of the 4x4 wave-2 radios. The AP in this test is a Netgear R7800 configured in bridging mode. This feature requires 2 wave-2 WiFi network cards and LANforge release 5.3.5 or higher.

1. Configure Radios and Station devices for MU-MIMO capabilities.
A. Go to the Port Manager, select the wiphy0 interface, and click Modify. Configure the radio for 2x2 MIMO and click Apply.
B. Select the `wiphy1` interface, and click "Modify." Configure the radio for 1x1 MIMO and click "Apply."

C. For both `wiphy0` and `wiphy1` ensure that the firmware is configured properly for MU-MIMO. The Port Status Information section at the top should mention the 9984 chipset, as other hardware may not support MU-MIMO. Normally the best option is to go into the "Firmware" tab, click the "Customize Firmware" box, click the top "Firmware Defaults for chipset: 9984" button, and then select "Allow MU-MIMO". Please note that selecting MU-MIMO disables a feature that allows multiple virtual stations to work properly on a single radio. So, when you are done with MU-MIMO testing, you should probably change this selection back to "Software Decrypt" settings.
D. Select the wlan0 interface, and click Modify. Configure the station for proper SSID, password, etc., and click Apply. Do the same configuration for wlan1.

E. In this scenario, we are using eth1 as the upstream port. Ensure it is configured properly. In this example, it is actually configured to serve DHCP using a virtual router and the Netsmith feature in LANforge, but for simplicity, it is normally best if you use the AP as DHCP server or just use fixed IP addresses for eth1 and the wlan interfaces instead of using DHCP.

2. Create Layer-3 UDP Download traffic flows.
A. Go to Layer-3 tab and click Create to build a UDP connection. Select the Protocol, ports, rates, and use Multi-Conn 1 so that separate processes are created for optimal throughput performance. Create a second one for the wlan1 interface, with download speed of about 450Mbps since it is only 1x1 MU-MIMO. You may need to adjust the + - buttons at top left to show the section containing Multi-Conn settings.

B. Start the test by selecting the connections click Start. We see about 500Mbps on wlan0 (2x2) and 200Mbps on wlan1 (1x1). For best results, you may need to tune orientation of the first two antenna on the wiphyo radio and the first antenna on wiphy1. In addition, it can take a short amount of time for the rates to reach maximum throughput, so you may wish to clear the counters after around 15 seconds of running to make sure the averages do not include the initial ramp-up time.
C. It can be a bit difficult to know if MU-MIMO is working properly. In general, if you disable MU-MIMO in the AP, then aggregate throughput should decrease significantly. In addition, the current firmware and/or driver is unable to properly report RX encoding rates for MU-MIMO frames, so it always reports low rates. If you see total throughput that is greater than the reported RX Rate, then likely the system is receiving MU-MIMO frames from the AP.
Goal: Use the WiFi Capacity Test plugin to emulate layer 4-7 traffic from ten virtual stations across an access point and report the results.

Requires 5.2.13 or later. This cookbook will go through setting up a VAP (Virtual Access Point) as an HTTP server, and creating/configuring 10 virtual stations to communicate with the VAP. It will also go through the setup of the WiFi Capacity Test LANforge-GUI plugin to have the virtual stations emulate downloading a file using Layer 4-7 endpoints in LANforge.

This example uses a LANforge CT523 system but the procedure should also work on a CT521, CT522, CT525 or similar system.

1. Create a VAP.
   A. Verify the wiphy device used for the VAP is on your preferred channel (this test will use channel 11).
A. In the **Port Mgr** tab of the LANforge Manager, modify the wiphy device that'll be used for the VAP (wiphy0 in this test).

![Port Mgr settings](image.png)

1. Select your preferred channel here.

B. Make sure the wiphy device is up.

![LANforge Manager](image2.png)

1. If the device is down like in the above screenshot, select it and click the **Admin UP** button (also indicated in the above screenshot).
B. In the Port Mgr tab, select a wiphy device (wiphy0 in this test) and click Create.

A. Select the WiFi VAP radio button.
B. Set Quantity to 1.
C. Set STA ID to 0.
D. Set IP Address to 10.0.0.1/24.
E. Set the SSID to layer4test.
F. Click Apply and close the create port window.

C. Configure the VAP.
   A. Open Netsmith from the Status tab.

   B. In Netsmith, right click and select New Router.
   C. Click OK.
D. Drag vap0 into the virtual router.

E. Right click vap0 and select **Modify**.

F. Check **DHCP**.

G. Change **DHCP Range Min** to **10.0.0.10**

H. Change **DHCP Range Max** to **10.0.0.50**

I. Click **OK**.

J. Click **Apply** in Netsmith then close the window.

2. Create 10 virtual stations.
A. Verify the wiphy device used for the stations (wiphy2 in this test) is on the **AUTO** channel.

B. Make sure wiphy2 is up.
C. In the Port Mgr tab, select a wiphy device (wiphy2 in this test) and click Create.

A. Select the WiFi STA radio button.
B. Set Quantity to 10.
C. Set STA ID to 0.
D. Select DHCP-IPv4.
E. Set the SSID to layer4test.
F. Click Apply and close the create port window.

D. Make sure the 10 staX ports get IPs.

3. Create a file for the layer 4-7 endpoint to use.
A. In a terminal on the LANforge system, run the below command to generate a 10MB file in /home/lanforge.

   Note: The smaller a file is, the harder it is to reach higher rates. Therefore it is recommended to use a larger file for these tests.

   ```
   dd if=/dev/urandom of=/home/lanforge/large-file.bin bs=1k count=10240
   ```

B. For the webserver to serve the file we created, it needs to know where to find it. Run the below command in a terminal on the LANforge system to link the file.

   ```
   ln -s /home/lanforge/large-file.bin /usr/local/lanforge/nginx/html
   ```

4. Set up the HTTP server on `vap0`. 
A. Before starting HTTP on vap0, the Apache service may need to be disabled.

A. Stop and disable httpd (Apache) in the LANforge terminal with the below commands.

```
sudo systemctl stop httpd.service
sudo systemctl disable httpd.service
sudo systemctl daemon-reload
```

B. Modify vap0 in the LANforge Port Mgr tab.

1. Enable the HTTP checkbox.

```
5. Create a layer 4-7 endpoint. WIFI Capacity will be using this as a template to copy from.
```
A. In the Layer 4-7 tab, click Create.

B. Set the Name to l4-http.

C. Set the Port to 80.

D. The URL will point to the VAP's IP: http://10.0.0.1/large-file.bin
   **Note:** This is where you can specify an IP of an AP you wish to test. LANforge also supports other layer 4-7 protocols, for more information you can view a tooltip by hovering over the URL text box.

E. Set the Source/Dest File to /dev/null

F. Click OK.

6. Set up and run a WiFi Capacity test.

A. Select the 10 created stations, then open WiFi Capacity Test from the Plugins menu.
B. Go to the Settings tab.

A. Set **Station Increment** to 1.

B. Set the Protocol to **Layer 4-7**. **Note:** This should automatically be set if you first select a Layer 4-7 Endpoint.

C. Select your Layer 4-7 Endpoint (**l4-http** in this test). The capacity test will use this as a template for each of the ten stations.

D. **Total Rate** can stay at 10Mbps. **Note:** This rate can represent either upload or download traffic depending on how you have your layer 4-7 endpoint configured.

C. Run the Capacity test by clicking **Start**.
A. The test will now make a copy of the selected layer 4-7 endpoint for each station. **Note:** You may notice that URLs per 10m is set to a high rate, this is to ensure the maximum amount of URLs are processed as WiFi Capacity adjusts the Max Speed.
Goal: Sniff wireless traffic from a LANforge radio using Wireshark and a WiFi Monitor port.

The best way to sniff wireless packets via Wireshark in LANforge is from a monitor port that is on its own radio (no other AP, STAs, etc.). This example will walk through the monitor port creation, sniffing the monitor port, as well as Wireshark filter recommendations.

This example uses a LANforge CT523 system but the procedure should work on a CT522, CT525, or similar system.

1. Create a monitor port.
   
   A. In the Port Mgr tab, select a wiphy device that you wish to sniff with (this example will use wiphy1, an ath10k radio).
B. If the wiphy device is down, click the up arrow to enable it.

C. Click Modify.

A. Select the channel you wish to sniff. Channel 36 will be used for this test.
B. Click OK.
D. Back in the **Port Mgr** tab, with the wiphy device still selected, click **Create**.

A. Select the **WiFi Monitor** option at the top.
B. Set the **Quantity** to 1.
C. Set the **STA ID** to 0.
D. Click **Apply** and close the Create Port window.

E. In the **Port Mgr** tab again, modify **mon0**.

A. You can disable **HT40** and **HT80** here if needed.
B. Click **OK** to close the window.

2. For this current setup, traffic will be generated with a layer 3 UDP connection between two stations.
   For more information see [Generating Traffic for WLAN Testing](#)
3. Use Wireshark to sniff moni0.
   
   A. If you are running the LANforge GUI from a Windows machine without x server installed, you will need to connect remotely to the LANforge system via rdesktop or vnc.

   A. To connect via rdesktop, type the following command into a console (replace LANforge-IP with the IP of your LANforge system):
   
   
rdesktop LANforge-IP

   I. The login info is username/password lanforge/lanforge
B. To connect via vnc, type the following command into a console (replace LANforge-IP with the IP of your LANforge system. **Don't forget to add the ':1' after the IP**):

```
vncviewer [LANforge-IP]:1
```

The password is `lanforge`.

C. Once you have accessed the LANforge system via rdesktop or vnc, open the LANforge GUI with the desktop icon shown below.
A. To use a filter, simply add the filter constraints to the filter text box as seen below and click **Apply** to the right. The below screenshot has Wireshark filtering on a specific IP.

B. Select **mon0** in the **Port Mgr** tab.

C. Click the **Sniff Packets** button. Wireshark will now open and automatically start scanning for packets. If you get a window that warns about running as user root, click **OK**.
B. If you'd like to only see traffic to/from a single AP use the filter `wlan.addr == [bssid]`

D. There are many filters that can be used in Wireshark. Some handy ones include:

```plaintext
ip: ip.addr==x.x.x.x
Association request wlan.fc.type_subtype eq 0
Association response wlan.fc.type_subtype eq 1
Probe request wlan.fc.type_subtype eq 4
Probe response wlan.fc.type_subtype eq 5
Beacon wlan.fc.type_subtype eq 8
Authentication wlan.fc.type_subtype eq 11
Deauthentication wlan.fc.type_subtype eq 12
```

E. Filters can be combined to specify if packets should match all filters (with `&&`) or any filters (with `||`).

For example, if you wanted to view packets that only contain both IPs 1.1.1.1 and 2.2.2.2 you could use the following: `ip.addr==1.1.1.1 && ip.addr==2.2.2.2`

Or, if you want to see all packets containing 1.1.1.1 and all packets containing 2.2.2.2, you could use the following: `ip.addr==1.1.1.1 || ip.addr==2.2.2.2`

F. You can visit https://wiki.wireshark.org/DisplayFilters for more tips on filters.

A handy ‘cheat sheet’ with most filters can be found here.
Scripting a Standalone CT703 or CT704 Attenuator

Goal: Operate a CT703 or CT704 WiFi Attenuator with a script.

The LANforge GUI provides scripting support for the CT703 and CT704 Attenuators. This cookbook provides a basic example of how to script the signal strength up and down.

Requires LANforge 5.2.11+ and CT703 or CT704 Attenuator.

1. Create an Attenuator Script
   A. In the Attenuators tab, select your attenuator and click Modify

   ![Image of LANforge Manager]

   Logged in to: brent-5234002 as: Admin

   B. You will see the Modify Attenuator window. Click on the Script button.
C. The Add/Modify Script window opens. In the picture below you see a huge list of numbers (the attenuation levels). These numbers are not pre-populated. You can copy and paste them out of this document or create a series with other commands listed below.

A. In the Script Type pulldown, select ScriptAttenu.

B. Type in the name for the script, this example is called attnr.

C. Select Symmetric

D. Choose 5 s for Run Duration. This will run the Attenuator at each dB value for this period of time.

E. Enter the following attenuation values for a 16 minute long test. This will send the attenuator from 5 to 955dB and back:


G. ...click OK
D. In the Attenuators tab, you will notice that your attenuator now reads **Enabled** in the Script column. Select the attenuator and click the **Start** button.

E. The window **Script Report** will appear. This monitors the script behavior of the attenuator script.

F. Also notice the attenuation values change in the LANforge Manager as the script runs.

**Note:** These values update every five seconds, so values may differ within the five second window.
Using CT712 RF Noise Generator and RADAR Simulator to test DFS channels

Goal: Generate RF pulses that simulate RADAR and cause an AP using DFS to exercise its detection and response abilities.

DFS (Dynamic Frequency Selection) allows an AP to use channels in the same spectrum that some RADAR systems use and provide a method of changing channels when RADAR signals are detected. In this example, we will use a LANforge CT712 which is our customized script and integrated GUI control for the HackRF-One Software-Defined Radio (SDR) to generate the RF pulses that simulate RADAR signals and cause a third-party AP under test to detect and change channels. It is recommended that this type of testing be done in a RF isolation chamber to limit interference to production WLAN and RADAR systems in use.

1. Verify a client is connected to a third-party AP using a DFS channel.
   For more information see
   Wikipedia: 5GHz Channels
   WLAN Pros WiFi Channel Reference Sheet

2. On the RF Generator tab, modify the device that corresponds to the CT712 USB device to set the desired channel and pulse characteristics.
   NOTE: The different RADAR types are defined as described in the document FCC DFS Compliance Procedures. RF pulses defined outside of these parameters can be used for other RF noise and interference tests.
3. Select a FCC RADAR type preset button or enter specific values to set the desired pulse characteristics, then set the transmit frequency, then select OK.

4. Highlight the RF Generator entry and select the Start+ button to start transmitting.
5. When the CT712 is activated, the Status will show Started and the HackRF-One device's TX LED should show a red light. The AP under test should detect RADAR within 10 seconds, change to an available channel and not be able to use the previous channel again for 30 minutes.

For more information see
WiFi Alliance: DFS Best Practices

6. An alternate method of controlling the CT712 HackRF-One device is to use the if_hackrf.py script in the LANforgeServer directory:

   A. Open a terminal window on the LANforge system.
   B. cd to /home/lanforge/LANforgeServer-5.3.8
   C. To show the script usage, type: if_hackrf.py --help
   D. Example of radar type 0 on channel S2 at 5.26GHz:
      A. `sudo ./if_hackrf.py --pulse_width 1 --pulse_interval 1428 --pulse_count 18 --sweep_time 500 --freq 5260000`
      B. To stop transmitting, type q to quit or Ctrl-D to exit
WiFi: Mesh Testing: video demonstration

Goal: Learn about how to use the Chamber View feature to create WiFi mesh test scenarios.

Watch a demonstration of how a Chamber View mesh test works. This scenario requires LANforge version 5.3.9, four isolation chambers, four or more programmable attenuators a DUT and three mesh AP nodes.
Goal: Use a diagnostic script to parse a WiFi packet capture file and generate histograms, packet loss stats, and other helpful information for diagnosing WiFi behaviour.

LANforge will be used to create a WiFi capture file, and then we will run the diagnostic script to help understand the on-air behaviour.

1. Create capture file.
   A. If you already have your own capture file or know how to create them, then skip this section.
   B. Packet captures are created using WiFi Monitor interfaces. LANforge can automatically create and manage these for you. The simplest way to create a capture is to use the Port-Mgr tab in the LANforge GUI.
C. Select WiFi radio that you wish to use and double-click it to bring up the modify window. Set the frequency to match the channel you wish to sniff and click OK to submit the changes and close the window.

D. Make sure the radio is still selected, and click the ‘Sniff Packets’ button on the Port Mgr tab. You normally need to be connected to the LANforge system using remote-desktop or VNC for this to work properly. After you click ‘Sniff Packets’, a monitor interface will be created and Wireshark will start. When your capture is complete, stop the capture in Wireshark and save the capture file.

2. Use the do_wifi_diag.bash script to diagnose the capture file.
A. The LANforge scripts package is normally installed in /home/lanforge/scripts. You can also clone the repository from github using this link: https://github.com/greearb/lanforge-scripts. Assuming it is in the standard location, change to the wifi_diag directory: cd /home/lanforge/scripts/wifi_diag. The ./do_wifi_diag.bash script will be used to launch the wifi_diag script.

```
[greearb@ben-dt4 ~/bitbites/x64_bitbites/server/if_scripts/wifi_diag]
[greearb@ben-dt4 wifi_diag]
[greearb@ben-dt4 wifi_diag]# ./do_wifi_diag.bash
Usage: ./do_wifi_diag.bash [-f {input-pcap-file}] [-o {output-directory}] [-d {DUT-bssid}]
[greearb@ben-dt4 wifi_diag]
```

B. Run the do_wifi_diag.bash script with appropriate arguments to match your device-under-test (DUT) and pcap file. The diagnostic script can process around 300 packets per second on a fast machine, so it can take a while to process a big file.

```
[greearb@ben-dt4 ~/bitbites/x64_bitbites/server/if_scripts/wifi_diag]
[greearb@ben-dt4 wifi_diag]
Removing existing output directory: test
Starting the wifi pcap diag.pl script, this can take a while...
NOTE: Processed 18000 packets and 5144163 input lines in 0:0:29 so far (344 pps).
NOTE: Processed 20000 packets and 18581132 input lines in 0:1:2 so far (322 pps).
NOTE: Processed 30000 packets and 15659409 input lines in 0:1:35 so far (315 pps).
NOTE: Processed 40000 packets and 28899107 input lines in 0:2:8 so far (312 pps).
NOTE: Processed 50000 packets and 28102736 input lines in 0:2:42 so far (388 pps).
NOTE: Processed 60000 packets and 31309600 input lines in 0:3:17 so far (384 pps).
NOTE: Processed 70000 packets and 36338360 input lines in 0:3:53 so far (388 pps).
NOTE: Processed 80000 packets and 41706529 input lines in 0:4:26 so far (388 pps).
NOTE: Processed 90000 packets and 46951889 input lines in 0:5:0 so far (388 pps).
NOTE: Processed 95233 packets and 50262066 input lines in 0:5:22 so far (299 pps).
Warning: empty y range [1:1], adjusting to [0.99:1.01]
Warning: empty y range [0:0], adjusting to [-1:1]
Warning: empty y range [0:0], adjusting to [-1:1]
Warning: empty y range [0:0], adjusting to [-1:1]
Report saved to: test/index.html
All done, open this file with a browser to view report: test/index.html
[greearb@ben-dt4 wifi_diag]
```

C. When the test is complete, you can open the [test]/index.html file to view the results, print to PDF, etc.
WiFi Diag Report

RX (All) Retransmit percentage: 5197778377 == 6.63077178253825
RX (Big) Retransmit count: 5167
TX (All) Retransmit percentage: 37108 == 0.0422099651097359
TX (Big) Retransmit count: 0
RX (All) no-ack-found: 56234
RX (Big) no-ack-found: 55705
TX (All) no-ack-found: 6
TX (Big) no-ack-found: 0
RX average gap between AMPDU frames (ms): 0.00344110614165813
RX average AMPDU chain time (ms): 0.0485246330408624
TX BA to RX AMPDU average gap (ms): 1.53520291727184
RX BA to TX AMPDU average gap (ms): 61.600929538206
Duplicate TX BA without AMPDU between them: 54
Duplicate RX BA without AMPDU between them: 32
WMM info from DUT Beacon

Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECMin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECMin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECMin/max 3/4 (CWmin/max 7/15), TXOP 94
Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECMin/max 2/3 (CWmin/max 3/7), TXOP 47

TX Encoding rate histogram.

<table>
<thead>
<tr>
<th>Rate Mbps</th>
<th>Packets</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0</td>
<td>3539</td>
<td>49.788970</td>
</tr>
<tr>
<td>12.0</td>
<td>9</td>
<td>0.126618</td>
</tr>
<tr>
<td>14.4</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>24.0</td>
<td>3509</td>
<td>49.366911</td>
</tr>
<tr>
<td>28.8</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>30.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>45.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>54.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>56.5</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>56.6</td>
<td>6</td>
<td>0.084412</td>
</tr>
<tr>
<td>60.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>65.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
<tr>
<td>87.9</td>
<td>12</td>
<td>0.168824</td>
</tr>
<tr>
<td>97.5</td>
<td>2</td>
<td>0.028137</td>
</tr>
<tr>
<td>117.0</td>
<td>2</td>
<td>0.028137</td>
</tr>
<tr>
<td>117.2</td>
<td>5</td>
<td>0.070343</td>
</tr>
<tr>
<td>130.0</td>
<td>2</td>
<td>0.028137</td>
</tr>
<tr>
<td>175.5</td>
<td>3</td>
<td>0.042206</td>
</tr>
<tr>
<td>195.0</td>
<td>1</td>
<td>0.014069</td>
</tr>
</tbody>
</table>

D. You can find the full report from this example here: examples/wifi-diag-report/index.html You can also view the report in PDF format: examples/wifi-diag-report.pdf
Goal: Learn about how to emulate a crowded WiFi environment that might occur in an airplane cabin.

Watch a demonstration of how to model a roaming WiFi system using multiple virtual APs that might be present in a transportation system. This scenario requires LANforge version 5.3.9, four isolation chambers, programmable attenuators, and multiple LANforges for virtual APs and stations and as a content server.
Goal: Learn about how to combine the WAN emulation and programmable attenuation to emulate different network environments for game consoles.

Watch a demonstration of how to modify the gaming experience using WAN links to drop packets and combining that with attenuating the wifi signal in an isolation chamber. This scenario requires LANforge version 5.3.9, two isolation chambers, one or more programmable attenuators a DUT and three mesh AP nodes.
Setting up a RADIUS Server

Goal: To set up a LANforge wireless access point with a local RADIUS server.

1. The LANforge auto-install --do_radius option will setup FreeRADIUS on the LANforge system with two example EAP methods, EAP-TLS and EAP-TTLS

2. The config files for FreeRADIUS are located in /etc/raddb
   A. /etc/raddb/certs contains the files necessary for EAP-TLS
   B. The LANforge auto-install copies the necessary files into /home/lanforge for use by LANforge wireless clients.
C. For **EAP-TLS**, use client.p12 as the client’s Private Key and ca.pem as the client’s CA Cert File. The Private Key password is lanforge.

D. `/etc/raddb/users` contains the user and password for **EAP-TTLS**.
E. The example **EAP-TTLS** user is testuser with password testpasswd. Additional entries can be added to the users file, then restart FreeRADIUS with systemctl restart radiusd.service.

3. **An alternative to FreeRADIUS is to use the hostapd RADIUS server.**
   A. Stop the FreeRADIUS service with systemctl stop radiusd.service
B. Modify the interface to use for the hostapd process and select the RADIUS checkbox.

C. Create a `hostapd_<port-name>.conf` file in the `/home/lanforge/wifi` directory with the following info.
D. Setup the desired EAP methods and passwords in the `/etc/hostapd.eap_users` file.

```
root@ct521-1ac-f20:/etc
[root@ct521-1ac-f20 etc]# cat hostapd.eap_user
"dot11r.user" PEAP
"dot11r.user" MSCHAPV2 "!!dot11r123" [2]
"dot11r.user@lanforge.com" PEAP
"dot11r.user@lanforge.com" MSCHAPV2 "!!dot11r123" [2]
"user-md5" MD5  "!!user-md5" [2]
"user-fast" MSCHAPV2 "!!fast123" [2]
"lanforge.peap" PEAP
"lanforge.peap" MSCHAPV2 "!!lanforge123" [2]
"lanforge.peap@lanforge.com" PEAP
"lanforge.peap@lanforge.com" MSCHAPV2 "!!lanforge123" [2]
"lanforge.tls" TLS
"lanforge.tls" TLS,TLS
"lanforge.tls" MD5,TLS-CHAP,TLS-MSCHAP,TLS-MSCHAPV2 "!!tls123" [2]
"lanforge.gtc" TLS,PEAP
"lanforge.gtc" GTC "!!gtc123" [2]
"0"*  AKA
"1"*  SIM
*  TLS
*@lanforge.com" TLS
"0"*  SIM,TLS,PEAP,AKA
"1"*  SIM,TLS,PEAP,AKA
*@mytest.com" TLS
"0"*  SIM,TLS,PEAP,AKA
"1"*  SIM,TLS,PEAP,AKA
```

E. If using **EAP-SIM** or **EAP-AKA**, verify entries in the `/etc/hlr_auc_gw.milenage_db` file, then start the HLR tool.

```
[root@ct521-1ac-f20 etc]# cd

File Edit View Search Terminal Help
[root@ct521-1ac-f20 home]# cd /home/lanforge

[Root@ct521-1ac-f20 lanforge]# . lanforge.profile
[root@ct521-1ac-f20 lanforge]# hlr_auc_gw -n /etc/hlr_auc_gw.milenage_db > /tmp/hlr_auc_fw.log &
[1] 27335
[root@ct521-1ac-f20 lanforge]# ps auxwxy | grep hlr
root  27335  0.0  0.0  19676  2204 pts/0   S  09:15  0:00 hlr_auc_gw -n /etc/hlr_auc_gw.milenage_db
root  27338  0.0  0.0  112668  2304 pts/0   S+ 09:15  0:00 grep --color=auto hlr
[root@ct521-1ac-f20 lanforge]#
```
4. Whether you use FreeRADIUS or hostapd RADIUS, setup your AP with the RADIUS server's IP address and port.

A. If using a LANforge AP on the same system as the RADIUS server, then the AP will address the RADIUS server at localhost or 127.0.0.1 with port 1812.

B. If using an external AP or WLAN Controller, then configure the device to address the RADIUS server on the network connected to a LANforge interface configured for RADIUS.
Setting up WPA3

Goal: To set up LANforge wireless access points and clients with WPA3.

This example will cover WPA3-Personal, WPA3-Enterprise and OWE. For an introduction or review of WPA3, see Hemant Chaskar's WLPC video.

1. WPA3-Personal for a VAP and a STA client.
   A. Setup the VAP with SSID, WPA3 security and a PSK.
B. Setup the VAP with 11w PMF option Required.
C. Setup the STA with SSID, WPA3 security and a PSK.

SSID: ABCD-wpa3
Key/Phrase: hello123
Mode: 802.11abgn-AC
Rate: GS Default
E. A capture of the association.

2. WPA3-Enterprise for a VAP and a STA client.
   A. Setup a RADIUS server for the VAP. This example uses a LANforge hostapd RADIUS server on the same system as the VAP.
B. Setup the VAP with WPA3 security and no PSK on the standard configuration screen.
C. Setup the VAP with 11w PMF option Required and select the checkbox for Advanced/802.1X which will also inform the VAP where its RADIUS server is located. In this example the LANforge hostapd RADIUS server is on the localhost.

D. After enabling Advanced/802.1X, the VAP is automatically configured for both WPA-EAP-SUITE-B and WPA-EAP-SUITE-B-192 as shown in the back-end configuration for the VAP.

```
cat /home/lanforge/wifi/hostapd_vap2.conf
...
 wpa_key_mgmt=WPA-EAP-SUITE-B WPA-EAP-SUITE-B-192
...```
E. Setup the STA with WPA3 security and no PSK on the standard configuration screen.
F. Setup the STA with 11w PMF option Required and select the checkbox for Advanced/802.1X which allows choosing the Key Management scheme and EAP Method. Here the STA is setup to use WPA-EAP-SUITE-B with EAP-TTLS and a user identity and password that were configured with the RADIUS server setup.

G. A capture of the association.

A. Setup the VAP with WPA3 security and a PSK on the standard configuration, then select option 11w PMF option Required on the advanced configuration, then admin up the VAP.

B. Copy the back-end config file for the VAP to a new filename and edit the wpa_key_mgmt from SAE to OWE.
   
   ```
cd /home/lanforge/wifi
   cp hostapd_vap2.conf vap2-owe.conf
   vi vap2-owe.conf
   wpa_key_mgmt=OWE
   ```
C. Modify the VAP and select Custom WPA Cfg on the Misc Configuration screen then type in the location of the new VAP config file.
D. Setup the STA with WPA3 security and no PSK on the standard configuration screen.
E. Setup the STA with 11w PMF option Required and select the checkbox for Advanced/802.1x which allows choosing the Key Management scheme. Here the STA will use OWE and a WPA PSK.

F. A capture of the association.
**WiFi: Inflight Entertainment: video demonstration**

**Goal:** Learn about how to emulate a crowded WiFi environment that might occur in an airplane cabin.

Watch a demonstration of how to model the inflight entertainment experience using 200 or more virtual stations simultaneously streaming video. This scenario requires LANforge version 5.3.9, six CT521a, and one CT523c as a controller, for virtual APs and as a content server.
EAP-PEAP AND MSCHAPv2 Configuration

Goal: To set up a lanforge wireless station with EAP-PEAP AND MSCHAPv2 authentication.

1. RADIUS Server is a Windows Server 2012 VM using its internal RADIUS Server specifically on interface 192.168.2.154.

2. RADIUS Server has both EAP-PEAP and MSCHAPv2 configured for use.
3. AP is a Ubiquiti HD AP with SSID ubnt-hd-ent with WPA Enterprise security.

4. The AP controller points to the RADIUS server at 192.168.2.154.
5. LANforge STA1 basic configuration:
6. LANforge STA1 advanced configuration is using EAP-PEAP.
7. Wireshark capture of STA1 EAPOL authentication.

8. LANforge STA2 basic configuration:
9. **LANforge STA2 advanced configuration is using MSCHAPv2.**
10. Wireshark capture of STA2 EAPOL authentication.
Basic AP Testing with LANforge (using Chamber View)

Goal: Set up virtual stations using a LANforge system, connect them to an AP under test, send traffic, and make measurements.

In this test scenario a LANforge system is used to create 5 virtual WiFi stations and configured to connect to a real WiFi AP under test. The AP's ethernet interface is connected to a LANforge ethernet interface allowing the LANforge system to create both the wireless stations and ethernet server. The test is then configured to send simple upstream and downstream UDP traffic between the server and the 5 WiFi stations through the AP under test.

1. Click on the Chamber View button in the LANforge GUI to launch the Chamber View screen.
2. Configure an AP under test (DUT).

3. To configure the DUT:
   A. Right click anywhere on the canvas in Chamber View and select "New DUT" from the menu.
   B. Enter all the known details about the AP under test including the SSID (multiple SSIDs if the AP has multiple SSIDs), BSSID (multiple BSSIDs if the AP has multiple radios with the same SSID).
   C. If the AP has security enabled, enter the security information.
   D. Set the DUT to Active by checking the 'Active' checkbox.
   E. Select the 'AP DUT' checkbox to indicate that this DUT is an Access Point.

4. Once OK is clicked, check to make sure the DUT appears in Chamber View as shown below.

5. Select the LANforge system to be used in the test.
6. All active LANforge systems will automatically appear in Chamber View. Select the unit being used in the test and drag to the middle of the canvas next to the AP under test. The small circles inside the LANforge box represent the SMA connectors. The columns of circles represent the individual radios in the system. For instance, in the screenshot about LF-1 has 4 columns of circle indicating 4 radios. The first two are 3x3 radios and the second two are 4x4 radios with 4 circles each.

7. **Create the test scenario**

   Click on the “Manage Scenarios” button and the open a “Create/Modify” dialog box.

8. In the Create/Modify dialog box

   A. Click on “Build New” button to create a new scenario.
   
   B. Enter a scenario name e.g. MyFirstApTest (no spaces allowed)
   
   C. Click “Add Row” button to add one or more rows.

9. **Create 5 WiFi Stations, map them to the AP under test and create traffic streams.**

    Row 1 is used to create the 5 WiFi stations. Do the following in Row 1:

   A. The “Resource” indicates the ID of the LANforge system being used in the test. Since we are using LF-1 for this test, select resource “1,1”. 
B. For the “Profile” column, pick “STA:STA-AC” profile which is one of the existing default station profiles that will create 11ac WiFi stations. The user can select from existing profiles to create new profiles by clicking on the “Create Profile” button at the top.

C. In the “Amount” drop down, enter 5 to indicate the 5 stations being created.

D. The “Uses-1” drop down indicates the primary hardware interface on which the user intends to create these clients. Here, select the right radio interface on which the WiFi stations are to be created.

E. The “Uses-2” is for bridge mode and it can be left as “AUTO” for this scenario.

F. Under the Frequency section, the user can select the channel on which to create the stations. If left to Auto, the stations will scan across all channels and find the target AP. So in this case we leave this setting to “AUTO”.

G. The “Maps To” represents which target AP the Stations should connect to. Since we have already configured the DUT in step 1, we can simply select the DUT.

H. For traffic, the GUI allows user to run up to 5 traffic streams on each client. In this case we are choosing one of the default traffic profiles “tcp-dl-6m-vi” which is a 6Mbps downstream tcp traffic stream. Once this is selected, the test will create 5 traffic streams of this type, one for each station. Users can create their own custom traffic streams by clicking on the “Create Traffic Profile” button.

10. Create an upstream server

   Add a new row to create an upstream server. For this new row,

   A. Select resource “1.1” as the upstream server is being created on the same LANforge system.
   
   B. Select the profile as “Upstream” to represent an Upstream endpoint.
   
   C. Set Amount to 1 as we are creating only 1 upstream server.
   
   D. Set “Uses-1” to eth1 as we are creating the server on “Eth1” interface on the LANforge system.
   
   E. Now click on “Apply and Save Scenario” to save the test scenario.

11. Load and Run Test Scenario

   The next step is to load the scenario and run the test.

   ![Chamber View - Scenario Configuration](image)

   A. Once the scenario is applied, click on the “Build Scenario” button and this action will configure the 5 stations and the traffic streams.
   
   B. Then in order to run the test scenario, select the “Scenario Test” option from the Tests drop down and click on the “Run Test” button.
   
   C. The test then starts running and the 5 stations will connect to the AP under test.
D. Once the connections are complete (indicated by the thick green line between the LANforge system and the AP under test”), the traffic streams are started (indicated by the dotted lines on both sides of the thick green line).

E. In the above example the Upstream shows a Tx stat of 31Mbps representing a total of about 30Mbps of downstream traffic (5 stations each doing 6Mbps) and the stations show an aggregate receive of about the same 31Mbps

F. “STA-AC (S)” indicates the 5 802.11ac stations connected to the AP under test and the -37db indicated the current signal strength the LANforge stations are seeing from the AP.

---

**Testing Receiver Sensitivity for a WiFi Device**

**Goal:** Setup and run a Receiver Sensitivity test for an AP using the LANforge CT523c or similar system in order to test how well the AP can receive packets with different MCS at different RF Signal levels.

In this test scenario, the LANforge CT523c is used to generate packets at specific MCS and spatial streams at a range of attenuation. This example assumes you are familiar with Chamber View, and that you have a LANforge system with a wave-2 WiFi Card, a programmable attenuator like the CT704b and two isolation chambers like the CT820a. The AP should be in one chamber, the LANforge system is in the other chamber, and the Attenuator is cabled between them. This feature is in LANforge version 5.3.9 and higher.

1. Configure Chamber View for Dataplane and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber-View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configure so that LANforge knows when it is connected to the correct AP.
C. Create a chamber object to hold the DUT, and add the DUT to that chamber. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may not function as desired.

![Create/Modify Chamber interface](image)

D. Create a chamber object to hold the LANforge system, and add the LANforge to it. Add connections from this chamber to the DUT chamber, specifying the proper Attenuator modules.

![Create/Modify Chamber interface](image)
E. Configure an Upstream profile using eth1 on the LANforge system.

F. Configure an STA profile on the LANforge system.

G. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

2. Use Chamber View to run a Receiver Sensitivity test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.
8. Select the **RX Sensitivity** test and click **Run Test**. You should see the RX Sensitivity Test configuration window pop up. It will remember the last configuration for most fields. Select the DUT and WIFI station device, and select the combinations of traffic types you wish to send.
C. When the configuration is complete, click the **Start** button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

D. When the test is complete, click the **Save HTML** button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example **RX Sensitivity Report**.
Testing AP Dataplane throughput at different packet sizes

Goal: Setup and run a Dataplane test for an AP using the LANforge CT523c or similar system in order to test how well the AP can handle sending and receiving packets with different packet sizes.

In this test scenario, the LANforge CT523c is used to generate packets of different sizes in the upstream and downstream direction through an AP. This example assumes you have some experience with Chamber View, and that you have a LANforge system, a programmable attenuator like the CT704b and two isolation chambers like the CT820a. The AP should be in one chamber, the LANforge system is in the other chamber, and the attenuator is cabled between them. In this example, the Attenuator is left at an optimal configuration, but you can also use this same Dataplane test to generate a report at different RF signal levels using the Attenuator. This feature requires LANforge version 5.3.9 or higher.

1. Configure Chamber View for Dataplane and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.
C. Create a chamber object to hold the DUT, and add the DUT to that chamber. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may not function as desired.

![Chamber Object Diagram]

D. Create a chamber object to hold the LANforge system, and add the LANforge to it. Add connections from this chamber to the DUT chamber, specifying the proper Attenuator modules.

![Chamber Object Diagram]
E. Configure an Upstream profile using eth1 on the LANforge system.

F. Configure an STA profile on the LANforge system.

G. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

2. Use Chamber View for Dataplane test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario. Apply the Scenario, then Build the scenario.
8. Select the **Dataplane** test and click **Run Test**. You should see the Dataplane Test configuration window pop up. It will remember the last configuration for most fields. Select the DUT and WiFi station device, and select the combinations of traffic types and packet sizes you wish to send.
C. When the configuration is complete, click the **Start** button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

![Dataplane Test Interface](image)

**Objective**

The Candela WiFi data plane test is designed to conduct an automatic testing of all combinations of station types, MIMO types, Channel Bandwidths, Traffic types, Traffic direction, Frame sizes etc... It will run a quick throughput test at every combination of these test variables and plot all the results in a set of charts to compare performance. The user is allowed to define an intended load as a percentage of the max theoretical PHY rate for every test combination. The expected behavior is that for every test combination the achieved throughput should be at least 70% of the theoretical max PHY rate under ideal test conditions. This test provides a way to go thorough hundreds of combinations in a fully automated fashion and very easily find patterns and problem areas which can be further debugged using more specific testing.

![Throughput vs PDU Size](image)

**Throughput vs PDU Size**

D. When the test is complete, click the **Save HTML** button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example **Dataplane Report**.
Testing AP Dataplane throughput at different orientation

Goal: Setup and run a Dataplane test for an AP using the LANforge CT522 or similar system in order to test how well the AP can handle sending and receiving packets at different rotations.

In this test scenario, the LANforge CT522 is used to generate packets in the upstream and downstream direction through an AP at different AP orientations. An affordable stand-alone turn-table is used to automatically rotate the AP to the desired orientation. This example assumes you have some experience with Chamber View, and that you have a LANforge system and turn-table. Using chambers will make the test perform more consistently, but is not required for this test. This feature requires LANforge version 5.4.1 or higher.

1. Configure Chamber View for Dataplane and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.
C. If using the 'comxim' stand-alone turn-table, the chamber object should automatically be created. For other real chambers, you may have to create the chamber object and configure it to be able to communicate to the chamber control API. This example uses the stand-alone turntable configured with a fake chamber object:

D. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

2. Use Chamber View for Dataplane test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario. Apply the Scenario, then build the scenario.
B. Select the **Dataplane** test and click **Run Test**. You should see the Dataplane Test configuration window pop up. It will remember the last configuration for most fields. Select the DUT and WiFi station device, and select the combinations of traffic types and turn-table degrees that you wish to test. The degrees show in this image will go from zero to 359 in steps of 10 degrees. The mouse-over tooltip for the turntable configuration entry field has the details on the available syntax:

C. You may wish to save/restore configurations or make some advanced configuration on the 'Advanced Configuration' tab.
D. The Report Configuration tab lets you input the operator information, notes about this test setup, and more.

E. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

F. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example Dataplane Rotation Test Report.

3. Stand-alone Turn Table Information.

A. We built a cable stand for the stand-alone turn-table to help keep cables out of the way while rotating.
**Testing Rate vs Range throughput for a WiFi Device**

**Goal:** Setup and run a Rate vs Range test for an AP using the **LANforge CT523c** or similar system in order to test how well the AP can transmit packets at different signal levels. This is a good test of the AP's rate-control logic, as well as tx power and general ability to deal with various RF conditions. This emulates a throughput test as the user walks away from the AP.

In this test scenario, the LANforge CT523c is used to generate packets on the Ethernet port towards the wired side of the AP. The AP will then transmit the frames to the LANforge WiFi station. This example assumes you have some experience with Chamber View, and that you have a LANforge system, a programmable attenuator like the **CT704b** and two isolation chambers like the **CT820a**. The AP should be in one chamber, the LANforge system is in the other chamber, and the Attenuator is cabled between them. This feature is in LANforge version 5.3.9 and higher.

1. Configure Chamber View for Rate vs Range and Similar Tests.
A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.
C. Create a chamber object to hold the DUT, and add the DUT to that chamber. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may not function as desired.

![Chamber Object](image)

D. Create a chamber object to hold the LANforge system, and add the LANforge to it. Add connections from this chamber to the DUT chamber, specifying the proper Attenuator modules.

![Chamber Object](image)
E. Configure an Upstream profile using eth1 on the LANforge system.

![Create/Modify Profile dialog for Upstream profile]

F. Configure an STA profile on the LANforge system.

![Create/Modify Profile dialog for STA profile]

G. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

![Create/Modify Scenario dialog with scenarios]

2. Use Chamber View to run a Rate vs Range test.
A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.

B. Select the Rate vs Range test and click Run Test. You should see the Rate vs Range Test configuration window pop up. It will remember the last configuration for most fields. Select the DUT and WiFi station device, and select the combinations of traffic types you wish to send. Be sure to select the attenuator and configure the attenuation steps. In this case, we have antenna over-the-air connection inside one of the chambers, with total path-loss at zero attenuation of about 25db. One interesting way to use this tool is to select the ‘Another Iteration’ checkbox. When the current test is complete, you will see a popup message notifying completeness. You can then reconfigure the DUT (by changing firmware versions, or some other configuration), and then re-run the test. The second test will be displayed on the same graphs, so it is easy to compare the difference. This particular test is not using that feature, however:
C. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

D. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example Rate vs Range Report.
Testing Station Capacity and throughput for a WiFi Device

Goal: Setup and run a WiFi Capacity Test test for an AP using the LANforge CT523c or similar system in order to test how well the AP can handle different amounts of active stations. This is a good test of the AP’s scalability and stability.

In this test scenario, the LANforge CT523c is used to create 64 stations and generate packets on the Ethernet port towards the wired side of the AP. The AP will then transmit the frames to the LANforge WiFi stations. LANforge will bring up stations in configured amounts, run a throughput test, and then bring up the next set of stations and repeat until the test is complete. This example assumes you have some experience with Chamber View, and that you have a LANforge system and two isolation chambers like the CT820a. The AP should be in one chamber, the LANforge system is in the other chamber, and the Attenuator (if using one) is cabled between them. Set the Attenuator to desired state before starting the test. Chambers and attenuators are not required for this test, but running inside isolation chambers will usually give you better and more reliable test results. This feature is in LANforge version 5.3.9 and higher.

1. Configure Chamber View for WiFi Capacity Test and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configure so that LANforge knows when it is connected to the correct AP.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>APUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW Info</td>
<td>v5.62.1</td>
</tr>
<tr>
<td>Model Number</td>
<td>AP640</td>
</tr>
<tr>
<td>Serial port</td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>0</td>
</tr>
<tr>
<td>SSID-1</td>
<td>labap</td>
</tr>
<tr>
<td>SSID-2</td>
<td></td>
</tr>
<tr>
<td>SSID-3</td>
<td></td>
</tr>
<tr>
<td>Mgt IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Ant-1</td>
<td>0</td>
</tr>
<tr>
<td>Ant-2</td>
<td>0</td>
</tr>
<tr>
<td>BSSID-1</td>
<td>78:d2:94:bf15:43</td>
</tr>
<tr>
<td>BSSID-2</td>
<td>00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>BSSID-3</td>
<td>00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>STA DUT</td>
<td>WEP</td>
</tr>
<tr>
<td>WPA3</td>
<td>Provides DHCP on LAN</td>
</tr>
</tbody>
</table>

```
C. Create a chamber object to hold the DUT, and add the DUT to that chamber. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may have decreased performance due to outside RF interference.

D. Create a chamber object to hold the LANforge system, and add the LANforge to it. Add connections from this chamber to the DUT chamber, specifying the proper Attenuator modules.
E. Configure an Upstream profile using eth1 on the LANforge system. Notice the dhcp-server checkbox is selected, since in this test case our AP is not configured as a DHCP server.

![Upstream profile configuration](image1)

F. Configure an STA profile on the LANforge system.

![STA profile configuration](image2)

G. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT). Choose the appropriate quantity of stations for your test case.

![Scenario configuration](image3)

2. Use Chamber View to run a WiFi Capacity Test.
A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.

B. Select the **WiFi Capacity** test and click **Run Test**. You should see the WiFi Capacity Test configuration window pop up. The Ports are normally selected properly based on the Scenario, but you may need to adjust them depending on your goals and scenario. Select the desired throughput and any other configuration changes from the defaults:
C. When the configuration is complete, click the **Start** button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs. In this particular test, the results are a bit unexpected. Normally rate starts off high and slowly decreases after 5 or 10 stations are active. In this case, we see a falloff after 10, but then it recovers at 60.

D. When the test is complete, click the **Save HTML** button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click ‘Save PDF’ and the browser will be directed to open the PDF file directly. Please see this example WiFi Capacity Test Report.
Testing Station Associate and Disassociate for a WiFi Device

Goal: Setup and run a Port Reset test for an AP using the LANforge CT523c or similar system in order to test how well the AP can handle stations connecting and disconnecting many times. This is a good test of the AP’s management plane stability.

In this test scenario, the LANforge CT522 is used to create 120 stations and then have them connect and disconnect to the AP. The test will count the number of connections and related events. This example assumes you have some experience with Chamber View, and that you have a LANforge system. A programmable attenuator and two isolation chambers would add the ability to test station reconnects at different RF signal levels, but this test normally runs fine without chambers or attenuators. This feature is in LANforge version 5.3.9 and higher.

1. Configure Chamber View for Port Reset and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects. If you do not have chambers or attenuators, just create the DUT object and skip the chamber setup.
B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>w3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image file</td>
<td>NONE</td>
</tr>
<tr>
<td>SW Info</td>
<td></td>
</tr>
<tr>
<td>Model Number</td>
<td></td>
</tr>
<tr>
<td>Serial port</td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td></td>
</tr>
<tr>
<td>API version</td>
<td>0</td>
</tr>
<tr>
<td>SSID-1</td>
<td>w3:0</td>
</tr>
<tr>
<td>SSID-2</td>
<td>w3:1</td>
</tr>
<tr>
<td>SSID-3</td>
<td></td>
</tr>
<tr>
<td>Mgt IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Ant-1</td>
<td>0</td>
</tr>
<tr>
<td>Ant-2</td>
<td>0</td>
</tr>
<tr>
<td>BSSID-1</td>
<td>04:f0:21:7b:37:2a</td>
</tr>
<tr>
<td>BSSID-2</td>
<td>04:f0:21:f2:ee:bd</td>
</tr>
<tr>
<td>BSSID-3</td>
<td>00:00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>STA DUT</td>
<td></td>
</tr>
<tr>
<td>WEP</td>
<td></td>
</tr>
<tr>
<td>WPA</td>
<td></td>
</tr>
<tr>
<td>WPA2</td>
<td></td>
</tr>
<tr>
<td>Provides DHCP on LAN</td>
<td></td>
</tr>
<tr>
<td>Provides DHCP on WAN</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>
```

C. Configure an Upstream profile using eth1 on the LANforge system.

```
| Name:      | upstream-dhcp             |
| Type:      | Upstream (4)              |
| Mode:      | Auto (0)                  |
| Instances | 1 (1)                     |
| SSID:      |                           |
| Pattern:   |                           |
| WPA        |                           |
| WPA2       |                           |
| WPA3       |                           |
| Notes:     |                           |
```
D. Configure an STA profile on the LANforge system.

E. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

2. Use Chamber View to run a Port Reset test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.
8. Select the Port Reset test and click Run Test. You should see the Port Reset Test configuration window pop up. By default, all of the stations will be selected to use in the reset test. You may adjust the selection at this time. If you want each station to act like a new device when it resets, select the 'Change MAC' checkbox. Make any other configuration changes.
C. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

D. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example Rate vs Range Report.
Goal: Compare dataplane throughput for several different APs set up in a similar manner. This allows comparing different hardware performance, and a similar test case can compare different firmware/software versions or other configuration changes.

In this test scenario, the LANforge CT522 is used to create a station and generate packets at different packet sizes to and from a series of APs. We will run one set of iterations of the dataplane test, pause it, make changes to use a different SSID, and then restart the test. The result is a report showing the differences in performance of the different APs under test. This specific test case is run over-the-air in an office. It would perform better and be more repeatable if RF chambers like the CT820a were used.

1. Configure Chamber View for DUT testing.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber-View to create various objects.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP. Create additional DUTs as needed.
C. This example uses a second DUT as well.

D. Configure an Upstream profile using eth1 on the LANforge system.
E. Configure an STA profile on the LANforge system.

F. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT). Please note that we will manually configure the station to connect to the second DUT as part of the test steps below.

2. Use Chamber View to run a Dataplane comparison test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.

B. Select the **Dataplane** test and click **Run Test**. You should see the RX Sensitivity Test configuration window pop up. It will remember the last configuration for most fields. Select the DUT and WiFi station device, and select the combinations of traffic types you wish to send. Select the **Another Iteration** checkbox to allow comparison graphs.
C. We have 4 total BSSIDs that we wish to test. The Scenario creation logic will have chosen one of the BSSIDs for the station, but we will need to override that for each of our comparison runs. Go to the Port-Mgr tab in the LANforge-GUI, double-click the station, and make sure that its SSID is correct. In case you are using different passwords you could change that at this time as well. When complete, click Apply. You can leave the window open as you will need it in future steps:
D. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs.

E. When the first comparison run is complete, a popup window will be shown, and the Paused checkbox will be selected. Select new BSSID by reconfiguring the station with a new BSSID, and when the reconfiguration is complete, un-select the Paused checkbox on the Dataplane test to do the next comparison run. Continue to run new comparisons in this manner until the full test is complete. When complete, unselect the Another Iteration, and then unselect 'Paused' to have the test complete:
F. This is the pause message, it is just informational and you can close it after it pops up.

G. When the test is complete, click the **Save HTML** button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this [example Dataplane Comparison Report](#).
Goal: Setup and run a Station Roam test against a cluster of APs supporting 802.11k, 802.11r, and Protected Management Frames (PMF/MFP). This test uses a 2-radio LANforge CT522 system, but other similar systems will work as well. This tests AP functionality and stability over many roam attempts. This is a good test of the AP’s management plane stability, and may also be a good controller test in case the AP system uses a controller.

In this test scenario, the LANforge CT522 is used to create 2 stations and then have them roam between the APs. The test will count the number of successful roam attempts with various different failure cases. This example assumes you have some experience with Chamber View, and that you have a LANforge system and properly configured AP cluster. A programmable attenuator and two isolation chambers would add the ability to test station roam at different RF signal levels, but this test normally runs fine without chambers or attenuators. This feature is in LANforge version 5.3.9 and higher.

1. Configure Chamber View for Station Roaming and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects. If you do not have chambers or attenuators, just create the DUT object and skip the chamber setup. This image shows the completed setup.

B. Create a Device Under Test (DUT) Profile for each of your APs. The BSSID is important to configure so that LANforge knows when it is connected to the correct AP. The authentication information and BSSID should be the same for all APs in the cluster, so probably you just need to change the name and BSSID for each of your DUTs and click save. To aid the visual representation of the roaming, consider putting the DUTs in a circle around the LANforge system as shown in the image above.
C. Configure an Upstream profile using eth1 on the LANforge system.

D. Configure an STA profile supporting 802.11r on the LANforge system. Roaming tests normally should deselect the Restart DHCP on Connect behaviour, as shown.

E. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radios and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT). You can map to any of the DUT APs in the cluster and the system will still be able to roam to the others.

2. Use Chamber View to run a Station Roam test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario or create a new scenario as needed. Apply the Scenario, then Build the scenario.

8. Select the **Roam Test** test and click **Run Test**. You should see the Wifi Mobility Test configuration window pop up. You can normally just use the defaults in the Roaming Parameters tab, so that tab is ignored in this example. By default, all of the stations will be selected to use in the roam test. You may adjust the selection at this time.
C. You can do some manual testing, including some 802.11k/v features on the Manual Testing tab, but in this example, we will not be using those features.

D. The Script Generator tab is used to create the roaming script. If your APs support Neighbor Report Requests, then you can click the Query Neighbors button and it should populate the BSSID Entry Field as well as the Scan Frequency List. If your stations have not been brought up yet, then the Query Neighbors button will cause them to associate. It make take a small bit of time until the neighbor report becomes available, please click the Query Neighbors button again after 10 or so seconds. Double-check that all of your APs are found and that the frequency list is the expected value. If your AP does not support Neighbor Query, then manually enter the BSSIDs and frequencies.
E. When the BSSIDs have been discovered to manually entered, click the Generate Script button. The generated script describes the roaming behaviour. You may also edit or paste in your own script, and you may save the generated script text for later use.

F. To start the test, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report window will be created and will be updated as the test runs. The AP cluster used in this example has some issues and is rejecting a lot of roam attempts with ‘code-17’, which indicates the AP thinks it has no more capacity. Hopefully your system works better!
Automate WiFi Capacity and other GUI tests.

Goal: Use a command-line script to have the LANforge-GUI run the WiFi Capacity test and generate a pdf automatically.

In this test scenario, a script is used to bring up the WiFi Capacity test with a pre-configured configuration. The capacity test is then started and a report is generated. All of this is automated, and other tests such as Dataplane are also supported. This feature requires LANforge version 5.4.1 or higher.

1. Configure WiFi Capacity Test for automated run.
   A. For this to work, the LANforge GUI must be started with the `-cli-socket 3990` argument. This causes it to open a socket to listen for text commands.
8. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. Create an appropriate scenario and DUT if you have not already done so. Other cookbook examples have more details of how to do this, please see those if you are unfamiliar with Chamber View.

C. Select WiFi Capacity test, and click **Run Test** to configure it as desired.
D. Enter a name in the ‘Save’ field, click save, and make sure it shows up as a loadable configuration. In this case, we are saving the configuration as ‘udp-dl-120’

2. Use the if_gui_cmd.pl script to launch the WiFi Capacity Test.
   A. Open an ssh session or terminal window and log into the LANforge system, or some other system with the LANforge scripts/ repository. On a LANforge system, this will usually be /home/lanforge/scripts In this case, the directory name is called if_scripts
B. Run the `lf_gui_cli_cmd.pl` script with appropriate arguments. Use `--help` for details. Once you run this, the WiFi Capacity test should be automatically opened and the test will be started. The script will end when the capacity test has completed. You may copy the results to some easily found location, such as a web server directory.

![Screenshot of the LF GUI CLI command](image)

C. For details on what GUI-CLI commands are supported, please see the screen-shot below and look at the contents of the `lf_gui_cmd.pl` script.

![Mate Terminal showing LF GUI CLI commands](image)
Testing AP performance and stability with the AP-Auto Automated test suite.

Goal: Setup and run a AP-Auto test for an AP using the LANforge CT522 or similar system in order to test how well the AP can handle station load, performance, and stability. The AP-Auto test is similar to the TR-398 test, but is designed to be functional with a minimum amount of test equipment. A 2-radio LANforge system and DUT is all that is required to run these tests.

In this test scenario, the LANforge CT522 is used to create stations and run throughput, stability, and station capacity tests. This example assumes you have some experience with Chamber View, and that you have a LANforge system and a DUT AP. The AP and LANforge may be in chambers, but that is not required. This feature requires LANforge version 5.4.1 or higher.

1. Configure Chamber View for AP-Auto and Similar Tests.
A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. If you have an appropriate scenario and DUT already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects. When complete, your configuration should look something like this. The ‘jw3’ is the DUT AP, and LF-1 is the LANforge system.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configure so that LANforge knows when it is connected to the correct AP.
2. Use Chamber View for the AP-Auto test.
   A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. Load appropriate scenario. Apply the Scenario, then Build the scenario.
8. Select the **AP-Auto** test and click **Run Test**. You should see the AP-Auto Test configuration window pop up. It will remember the last configuration for most fields, and you can also save and load configurations on the 'Advanced Configuration' tab. Select the DUT 2G and DUT 5G SSIDs. This test requires that Open or PSK is filled out. The enterprise SSID is optional. Use 'NA' for SSIDs that are not enabled. Select the LANforge radios to be used in this test. You need at least one 2.4GHz radio and one 5GHz radio for full functionality. At the bottom, select the test cases to be run.:
C. The Advanced Configuration tab lets you save and restore test configurations and also tune the behaviour of the automated tests:

![Advanced Configuration Tab](image1)

D. The Capacity Configuration tab lets you configure the Capacity test. By default, it will run with maximum capabilities and MTU frame size in the downstream direction. But, you can use this tab to also enable upstream traffic, iterate over different Modes, Spatial Streams and Bandwidths, as well as use the various packet sizes configured on the 'Advanced Configuration' tab:

![Capacity Configuration Tab](image2)
E. The Pass/Fail Configuration tab lets you enter pass/fail criteria based on wifi modes, packet sizes, spatial streams and more. If you do not fill in this section, then the test will attempt to provide some basic automated pass/fail criteria, and you can also just ignore the pass/fail for the Capacity and packet-size tests and let a human judge the results.

F. Here is an example set of pass/fail criteria in text form for easier cut/paste:

```
# modes:  /a, /an-20 4x4, /an-40 4x4, /b, /bg, /bgn-20, /anAC-20,40,80
# stations: 1, 10, 20, 50, ...
# Non-specified and fields set to "*" means match all.
# For a/b modes, Auto-BW == 20, Auto-NSS == 1
# For /ac modes, Auto-BW == 40, Auto-NSS == 4
# For /ax and /ac modes, Auto-BW == 80, Auto-NSS == 4

#/a mode
5 * 64 2Mbps mode=802.11a sta=1
5 * 1370 25Mbps mode=802.11a sta=1
5 * MTU 26Mbps mode=802.11a sta=1

5 * 64 50Mbps mode=802.11an sta=1 bw=20 nss=4
5 * 1370 245Mbps mode=802.11an sta=1 bw=20 nss=4
5 * MTU 456Mbps mode=802.11an sta=1 bw=20 nss=4

#/for any amount of /b stations
2.4 * 64 1Mbps mode=802.11b sta=* 
2.4 * 1370 7Mbps mode=802.11b sta=* 
2.4 * MTU 7Mbps mode=802.11b sta=* 
```

# For any amount of /bg stations
2.4 * 64 2Mbps mode=802.11bg sta=* 
2.4 * 1370 21Mbps mode=802.11bg sta=* 
2.4 * MTU 22Mbps mode=802.11bg sta=* 

# For /bg 20Mhz stations.
2.4 * 64 50Mbps mode=802.11bg sta=1 bw=20 nss=4 
2.4 * 1370 240Mbps mode=802.11bg sta=1 bw=20 nss=4 
2.4 * MTU 241Mbps mode=802.11bg sta=1 bw=20 nss=4 

2.4 * 64 50Mbps mode=802.11bg sta=10 bw=20 nss=4 
2.4 * 1370 240Mbps mode=802.11bg sta=10 bw=20 nss=4 
2.4 * MTU 241Mbps mode=802.11bg sta=10 bw=20 nss=4 

# For /bg 40Mhz /n on 2.4, same values for all number of stations currently.
2.4 * 64 50Mbps mode=802.11bg sta=3 bw=40 nss=4 
2.4 * 1370 280Mbps mode=802.11bg sta=3 bw=40 nss=4 
2.4 * MTU 281Mbps mode=802.11bg sta=3 bw=40 nss=4 

# For /an-AC 20Mhz stations.
5 * 64 50Mbps mode=802.11an-AC sta=1 bw=20 nss=4 
5 * 1370 235Mbps mode=802.11an-AC sta=1 bw=20 nss=4 
5 * MTU 235Mbps mode=802.11an-AC sta=1 bw=20 nss=4 

# For /an-AC 40Mhz stations
5 * 64 50Mbps mode=802.11an-AC sta=1 bw=40 nss=4 
5 * 1370 615Mbps mode=802.11an-AC sta=1 bw=40 nss=4 
5 * MTU 630Mbps mode=802.11an-AC sta=1 bw=40 nss=4 

# For /an-AC 80Mhz stations.
5 DL 64 50Mbps mode=802.11an-AC sta=1 bw=80 nss=4 
5 DL 1370 1300Mbps mode=802.11an-AC sta=1 bw=80 nss=4 
5 DL MTU 1300Mbps mode=802.11an-AC sta=1 bw=80 nss=4 
5 UL 64 50Mbps mode=802.11an-AC sta=1 bw=80 nss=4 
5 UL 1370 1100Mbps mode=802.11an-AC sta=1 bw=80 nss=4 
5 UL MTU 1100Mbps mode=802.11an-AC sta=1 bw=80 nss=4 

5 DL 64 50Mbps mode=802.11an-AC sta=10 bw=80 nss=4 
5 DL 1370 1300Mbps mode=802.11an-AC sta=10 bw=80 nss=4 
5 DL MTU 1300Mbps mode=802.11an-AC sta=10 bw=80 nss=4 
5 UL 64 50Mbps mode=802.11an-AC sta=10 bw=80 nss=4 
5 UL 1370 1200Mbps mode=802.11an-AC sta=10 bw=80 nss=4 
5 UL MTU 1200Mbps mode=802.11an-AC sta=10 bw=80 nss=4 

5 * 64 50Mbps mode=802.11an-AC sta=50 bw=80 nss=4 
5 * 1370 1100Mbps mode=802.11an-AC sta=50 bw=80 nss=4 
5 * MTU 1100Mbps mode=802.11an-AC sta=50 bw=80 nss=4 

# Auto (full capabilities) entries, for tput test, DUT is wave-1 3x3/2x2
2.4 * 64 50Mbps mode=Auto sta=* bw=Auto nss=Auto
G. The Report Configuration tab lets you add some notes and other details to the generated report.

H. When the configuration is complete, click the Start button (which will change to ‘Stop’ once start is clicked) to start the test. An interactive report tab will be created and will be updated as the test runs.

I. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click ‘Save PDF’ and the browser will be directed to open the pdf file directly. Please see this example AP-Auto Report.
Testing AP with automated TR-398 scenario

**Goal:** Setup and run a TR-398 test for an AP using a 6-radio version of the LANforge CT523c or similar system in order to test how well the AP can handle the various test cases specified in the TR-398 test document.

In this test scenario, the LANforge CT523c is used to emulate different station and AP scenarios and generate and receive traffic through an AP. This example assumes you have some experience with Chamber View, and that you have an appropriate LANforge system, programmable attenuators like the CT714 and two isolation chambers like the CT820a and CT840a. The AP should be in the chamber with the 2D turntable, the LANforge system is in the other chamber, and the attenuators are cabled between them. This feature requires LANforge version 5.4.1 or higher and the LANforge TR-398 automation software license.

1. Configure Chamber View for TR-398 and Similar Tests.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects. In this example, the 'Mobilestations' chamber holds the LANforge, and the TR-398 chamber holds the Device Under Test. Your configuration should look like this when these steps are complete.

B. Create a Device Under Test (DUT) Profile that matches your AP. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.
C. Create a chamber object to hold the DUT, and add the DUT to that chamber. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may not function as desired. The turntable configuration is different for different models of chambers, this example [bare IP address] is for the CT840a chamber.

<table>
<thead>
<tr>
<th>Chamber Type</th>
<th>Turntable Type</th>
<th>Managed By</th>
<th>DUT-1</th>
<th>DUT-2</th>
<th>DUT-3</th>
<th>DUT-4</th>
<th>LANforge-1</th>
<th>LANforge-2</th>
<th>LANforge-3</th>
<th>LANforge-4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chamber A</td>
<td>Turntable A</td>
<td>Name</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>LANforge 1</td>
<td>LANforge 2</td>
<td>LANforge 3</td>
<td>LANforge 4</td>
</tr>
<tr>
<td>Chamber B</td>
<td>Turntable B</td>
<td>Name</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>LANforge 1</td>
<td>LANforge 2</td>
<td>LANforge 3</td>
<td>LANforge 4</td>
</tr>
<tr>
<td>Chamber C</td>
<td>Turntable C</td>
<td>Name</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>LANforge 1</td>
<td>LANforge 2</td>
<td>LANforge 3</td>
<td>LANforge 4</td>
</tr>
<tr>
<td>Chamber D</td>
<td>Turntable D</td>
<td>Name</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>LANforge 1</td>
<td>LANforge 2</td>
<td>LANforge 3</td>
<td>LANforge 4</td>
</tr>
</tbody>
</table>

D. Create a chamber object to hold the LANforge system, and add the LANforge to it. Add connections from this chamber to the DUT chamber, specifying the proper Attenuator modules. Please note we use the ‘OTA’ attenuation floor since we have OTA connection between DUT and antennas inside the DUT chamber.
E. Configure a Chamber View Scenario and add the STA profile (mapped to desired wiphyX radio and DUT). Add an upstream profile mapped to DUT LAN side (or possibly WAN side if that is more appropriate for your DUT).

2. Use Chamber View for TR-398 test.
   A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. Load appropriate scenario. Apply the Scenario, then Build the scenario.

   B. To help make the cable routing easier to understand, you may wish to color-code the cables with tape or other similar markings. Inside of the LANforge chamber:
C. Inside of the DUT chamber:

D. Outside, back view:
E. Front view, all closed up and ready to test:
F. Select the TR-398 test and click Run Test. You should see the TR-398 Test configuration window pop up. It will remember the last configuration for most fields. Select the 2.4 and 5GHz DUT, turn-table chamber, and carefully associate the radios with correct attenuator modules. For the first run, we will just run the calibration test to auto-configure the path loss by adjusting the attenuators and testing RSSI:

<table>
<thead>
<tr>
<th>Radio</th>
<th>2.4GHz RSSI 0 Attenuation</th>
<th>5GHz RSSI 0 Attenuation</th>
<th>Attenuator Modules</th>
</tr>
</thead>
</table>
| Group 0
| 2.4GHz | 28                        | 20                      | 1.1.102.1         |
| 5GHz   | 11.2 wiphy0               | 11.3 wiphy1             | 1.1.85.3          |
| Group 1
| 2.4GHz | 28                        | 20                      | 1.1.102.0         |
| 5GHz   | 11.4 wiphy2               | 11.5 wiphy3             | 1.1.85.1          |
| Group 2
| 2.4GHz | 28                        | 20                      | 1.1.102.2         |
| 5GHz   | 11.6 wiphy4               | 11.7 wiphy5             | 1.1.85.0          |

TR-398 tests to run:
- Calibrate Attenuators
- Receiver Sensitivity
- Maximum Connection
- Maximum Throughput
- Airtime Fairness
- Range Versus Rate
- Spatial Consistency
- Multiple STAs Performance
- Multiple Assoc Stability
- Downlink MU-MIMO
- AP Coexistence
- Long Term Stability

Estimated Test Duration: 10 min.
G. Go to the Advanced Configuration tab and make sure the channels are configured properly, and tune any other settings that you wish to modify.

H. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report tab will be created and will be updated as the test runs. For the first run, we will just run the calibration test to auto-configure the path loss by adjusting the attenuators and testing RSSI. If the calibration was acceptable, click Start again to save the calculated zero-RSSI attenuation values for future test runs in which you may decide to skip re-running the attenuation.
I. After the calibration step is complete, select the desired set of test cases and click Start. The test may run for many hours. If you have the webcam configured, you can watch the rotational tests happen using the 'camorama' program (in Linux), or your own preferred USB webcam program. If using the LANforge machine to view camorama, please set the size to small so that it uses less CPU. When you click start, the Report tab is created, you can view that tab to watch the progress.

J. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example TR-398 Test Report.

---

**Testing Mesh APs with automated Mesh scenario**

**Goal:** Setup and run a series of tests in different mesh topologies using the LANforge CT523c or similar system..

In this test scenario, the LANforge CT523c is used to emulate a set of stations that move to different locations relative to a set of mesh APs. Throughput tests are run at each requested topology. A set of 4 chambers are used. One holds the station emulator, the other three hold the mesh APs. Programmable attenuators are used to adjust the signal strength between APs and the station chamber to emulate different topologies. This example assumes you have some experience with Chamber View, and that you have an appropriate LANforge system, programmable attenuators like the CT714 and four isolation chambers like the CT820a. This feature requires LANforge version 5.4.1 or higher.

1. Configure Chamber View for Mesh and Similar Tests.
A. Open Chamber View by clicking on the ‘Chamber View’ button in the LANforge-GUI. If you have an appropriate scenario already created, then skip to the next section, otherwise you will need to build a scenario that matches your system. You can right-click in Chamber View to create various objects. In this example, the ‘Mobilestations’ chamber holds the LANforge, and the other chambers hold mesh APs and additional LANforge traffic generating systems. In this example, the LANforge systems in the AP chambers are not used. Your configuration should look like this when these steps are complete.
B. Create a Device Under Test (DUT) Profile that matches each of your APs. The BSSID is important to configured so that LANforge knows when it is connected to the correct AP.

C. Create chamber objects to hold the mobile stations and DUTs, and add the LANforge and DUTs to the chambers. If you have no chambers, you can create a fake chamber, but your test will not be isolated and may not function as desired. Here is an example of the mobile stations chamber. Please note we will auto-calibrate the Zero-Attenuation values for the station chamber.

D. Here is an example of the RootAP chamber
E. Here is an example of the Node-1 chamber

F. Here is an example of the Node-2 chamber

G. Configure a Chamber View Scenario. This is somewhat optional since the mesh automation logic will create its own temporary scenario to run the automation tests.

2. Use Chamber View to start the Mesh test.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. Load appropriate scenario. Apply the Scenario, then Build the scenario.

B. Select the **Mesh** test and click **Run Test**. You should see the Mesh Test configuration window pop up. It will remember the last configuration for most fields. Select the resources, topologies and other test config to be used for this test. If you have not run the calibration step previously, run that test first:
C. Once the calibration step is complete, reconfigure to run the throughput tests. In this case, we are using the ABC topology where all three nodes are close to each other. The stations will do throughput tests at each of three positions: Close to Root AP, Close to Node 1, and Close to Node 2. We will generate UDP download traffic. No stations will be created on the LANforge systems inside the AP chambers in this test.

D. Configure the appropriate settings on the Advanced tab. In this case, I am disabling 2.4Ghz and doing a 5Ghz only test.
E. When the configuration is complete, click the Start button (which will change to 'Stop' once start is clicked) to start the test. An interactive report tab will be created and will be updated as the test runs. For each topology, throughput graphs and topology snapshot will be generated.

F. When the test is complete, click the Save HTML button to save an HTML report and generate the PDF. The PDF file will be linked from the HTML page. You can also click 'Save PDF' and the browser will be directed to open the pdf file directly. Please see this example Mesh Test Report.

LANforge as Access Point

Goal: Create four LANforge APs in bridged mode using Chamber View

In this test scenario, two LANforge CT522 systems are used to create 4 APs. The APs could be used for testing client devices such as phones. This is a simple example with no authentication.

1. Configure Chamber View to create Access Points.
A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. You can right-click in Chamber View to create various objects. The LANforge system(s) should show up as green boxes in Chamber View.

B. Configure a Chamber View Scenario and add the AP profiles.
C. This example uses 4 different bridged-AP profiles. Each profile is the same except that it has a different SSID.

![Create/Modify Profile window](image)

D. Once you have saved and selected the Scenario, click **Apply Scenario** and then click **Build Scenario**. The APs will be created, bridge devices will be created and will contain the APs and the Ethernet ports selected in the scenario. The Access Point devices will be started as part of the build process, so the system is now ready to be used. You can also make further modifications to the AP configuration by modifying the vap interfaces in the Port-Mgr tab of the LANforge GUI.

![Chamber View window](image)
LANforge as 802.11k/v/r Access Point Cluster

Goal: Create 8 LANforge APs supporting 802.11k, v, and r in bridged mode using Chamber View

In this test scenario, two LANforge CTS22 systems are used to create 8 APs. The APs can be used for 802.11k/v/r roaming and related testing. No external radius server is needed. The 'eth1' interfaces on the two LANforges should be connected to the same LAN. NOTE: As of this writing, there is a bug when 802.11w (MFP) is enabled. We are not currently clear whether it is an AP issue or a Station issue.

1. Configure Chamber View to create 802.11r Access Points.
   A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. You can right-click in Chamber View to create various objects. The LANforge system(s) should show up as green boxes in Chamber View.
B. Configure a Chamber View Scenario and add the AP profiles.

C. This example uses one 802.11r AP profile for all APs.
D. Once you have saved and selected the Scenario, click **Apply Scenario** and then click **Build Scenario**. The APs will be created, bridge devices will be created and will contain the APs and the Ethernet ports selected in the scenario. A radius server will be created and started. The Access Point devices will be started as part of the build process, so the system is now ready to be used. You can also make further modifications to the AP configuration by modifying the vap interfaces in the Port-Mgr tab of the LANforge GUI.
E. To give you some idea of the underlying configuration, please see this VAP configuration window.

F. And the 'custom' magic that makes the 802.11r cluster talk to itself.
G. Normally you would configure your own Station device to connect to this AP cluster. In this case, LANforge stations were used. Here is a screenshot of the config window to give some idea of how to configure your own stations.
H. The Station advanced screen shows the EAP-TTLS config and key management. Note that 802.11w is disabled in this test to work around some bug.

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:**  
- FT-EAP (11r)
- HESSID:

**Pairwise Ciphers:** DEFAULT

**Group Ciphers:** DEFAULT

**WPA PSK:**

**EAP Methods:** EAP-TTLS

**EAP Identity:** testuser

**EAP Anon Identity:**

**EAP Password:** testpasswd

**EAP Pin:**

**Private Key:**

**CA Cert File:**

**Network Auth:** ieee80211w

- Advanced/802.1x
- Enable 802.11u
- HotSpot 2.0
- Enable PKI