

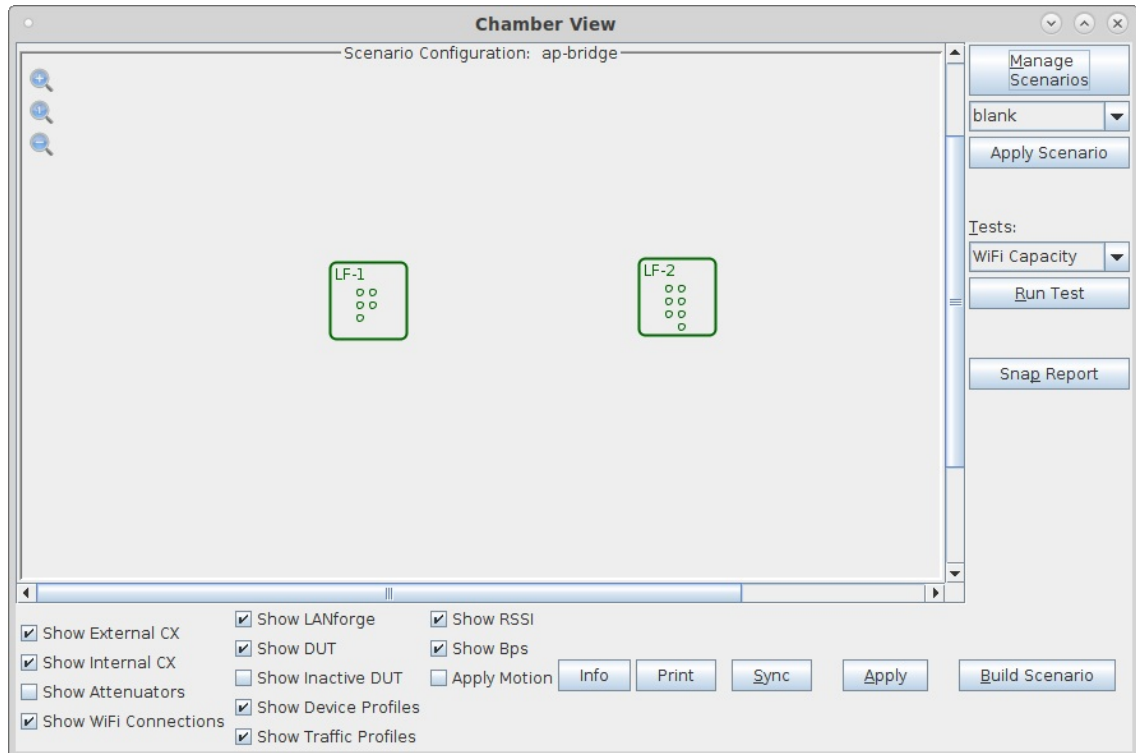
LANforge as 802.11k/v/r Access Point Cluster

Goal: Create 8 LANforge APs supporting 802.11k, v, and r in bridged mode using Chamber View

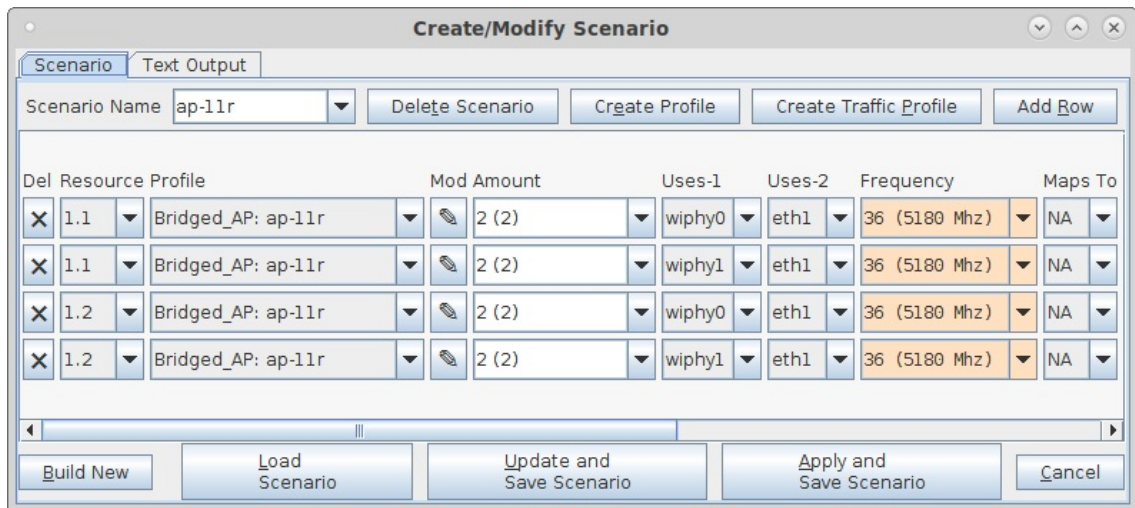
In this test scenario, two LANforge CT522 systems are used to create 8 APs. The APs can be used for 802.11k/v/r roaming and related testing. No external radius server is needed. The 'eth1' interfaces on the two LANforges should be connected to the same LAN. NOTE: As of this writing, there is a bug when 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.

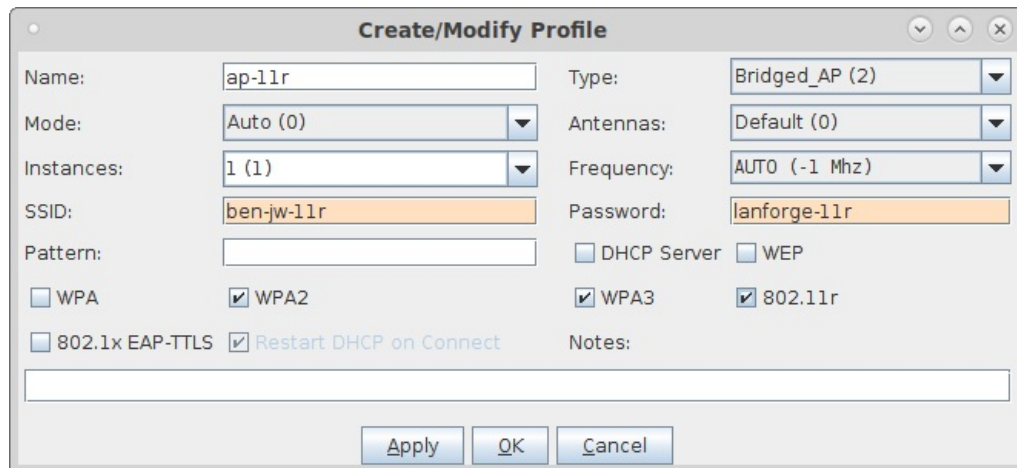
- A. Open Chamber View by clicking on the 'Chamber View' button in the LANforge-GUI. You can right-click in Chamber View to create various objects. The LANforge system(s) should show up as green boxes in Chamber View.



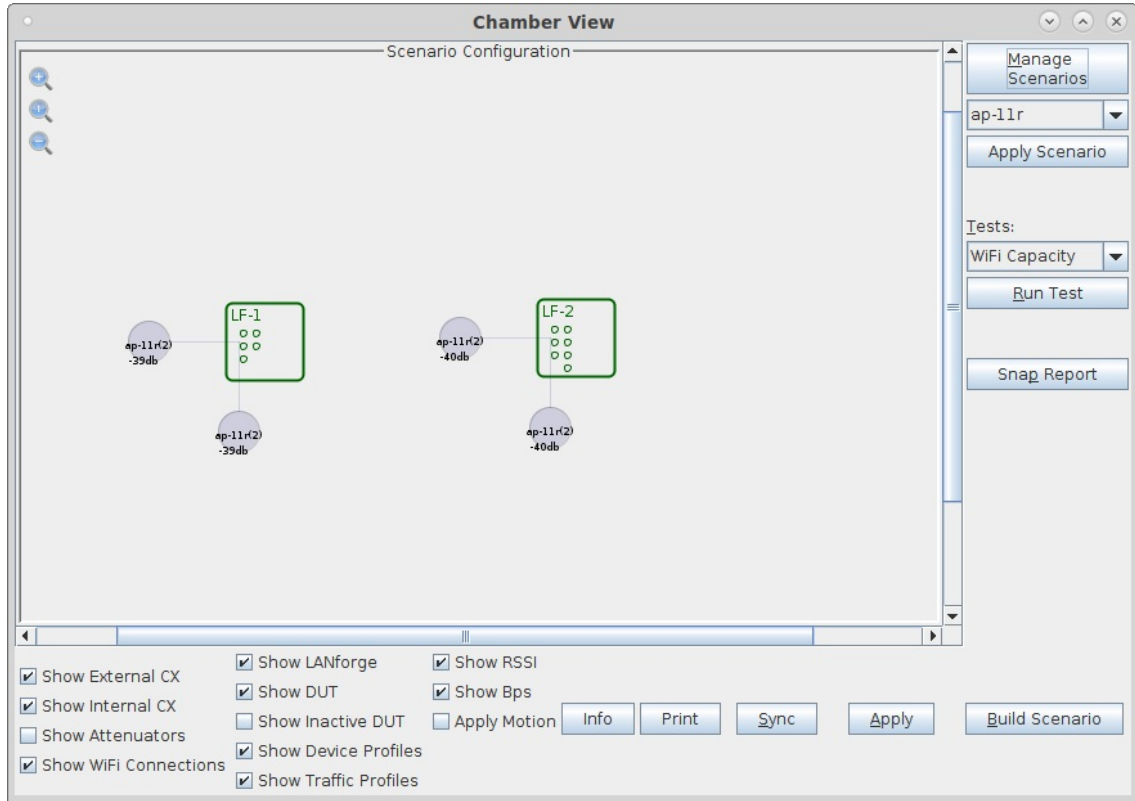
B. Configure a Chamber View Scenario and add the AP profiles.



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.

The screenshot shows the 'vap0001 (jw4-ben) Configure Settings' window. The 'Advanced Configuration' tab is selected, showing 'Advanced WiFi Settings'. The settings include:

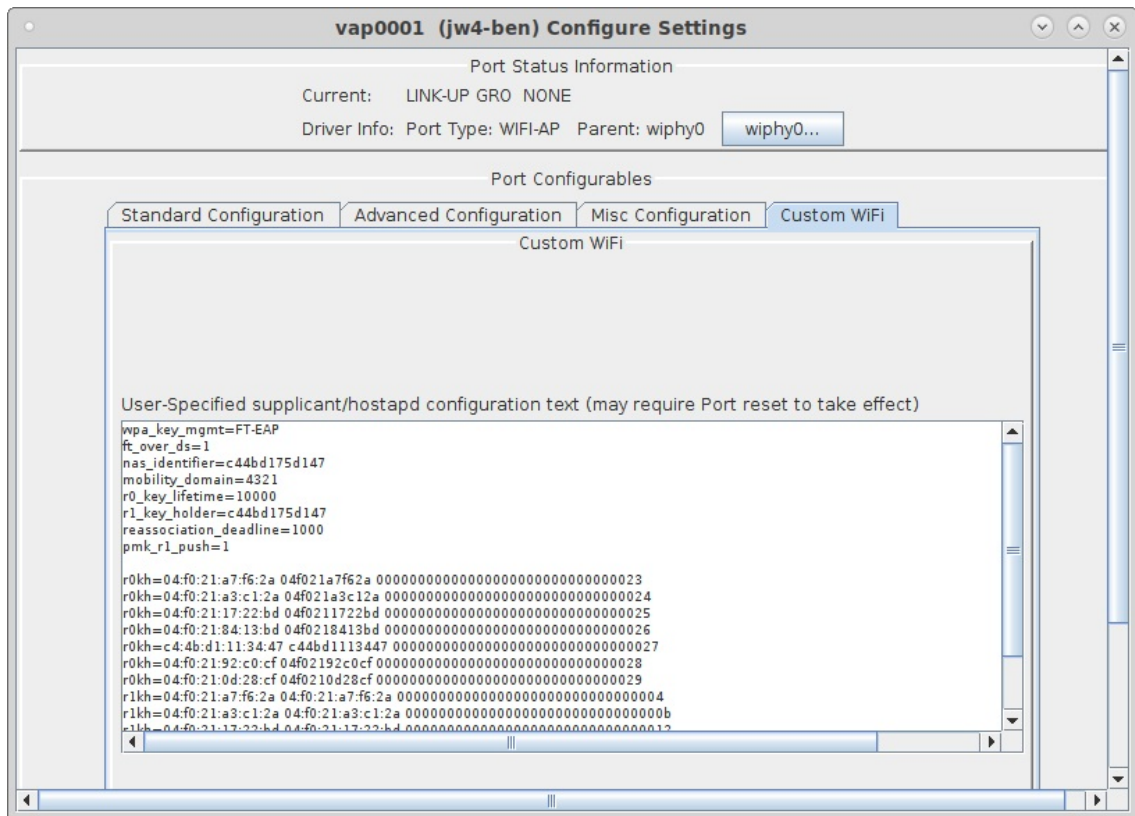
- Pairwise Ciphers: DEFAULT
- Group Ciphers: DEFAULT
- Ignore Probes: zero (0%)
- Ignore Auth-Assoc: zero (0%)
- Ignore Assoc: zero (0%)
- Ignore Re-Assoc: zero (0%)
- Corrupt GTK: zero (0%)
- HS20 Capabilities: [empty]
- HS20 Oper Class: [empty]
- HS20 WAN Metrics: [empty]
- ieee80211w: Optional (1)
- Venue Group: Unspecified (0)
- Network Type: Private (0)
- Network Auth: [empty]
- HESSID: 00:00:00:00:00:00
- Realm: [empty]
- IMSI: [empty]
- Milenage: [empty]
- Domain: [empty]
- Consortium: [empty]
- RADIUS IP: 127.0.0.1
- RADIUS Port: 1812
- RADIUS Secret: lanforge
- Venue Type: Unspecified (0)
- Address Types: Not Available (0)
- 3GPP Cell Net: [empty]

At the bottom, there are several checkboxes for advanced features:

- Use 80211d
- Use 80211h
- BSS-Load
- Neighbor Reports
- BSS Transition
- Advanced/802.1x
- Short-Preamble
- HotSpot 2.0
- Disable DGAF
- Enable 802.11u
- 802.11u Internet
- 802.11u ASRA
- 802.11u ESR
- 802.11u UESA

The window also includes buttons for 'Print', 'Display', 'Logs', 'Probe', 'Display Scan', 'Sync', 'Apply', 'OK', and 'Cancel'.

F. And the 'custom' magic that makes the .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.

sta0000 (If0313-6477) Configure Settings

Port Status Information

Current: LINK-UP GRO Authorized

Driver Info: Port Type: WIFI-STA Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration
Advanced Configuration
Misc Configuration
Corruptions
Custom WiFi

General Interface Settings

—Enable—

Set MAC

Set TX Q Len

Set MTU

Set Offload

Set PROMISC

Down Aux-Mgt

DHCP-IPv6 DHCP Release DHCP Vendor ID: None

DHCP-IPv4 Secondary-IPs DHCP Client ID: None

DNS Servers: 8.8.8.8 Peer IP: NA

IP Address: 0.0.0.0 Global IPv6: AUTO

IP Mask: 0.0.0.0 Link IPv6: AUTO

Gateway IP: 0.0.0.0 IPv6 GW: AUTO

Alias: MTU: 1500

MAC Addr: 04:f0:21:7b:37:f3 TX Q Len: 1000

Rpt Timer: faster (1 s) WiFi Bridge: NONE

WiFi Settings

SSID: ben-jw-11r AP: DEFAULT

Key/Phrase: lanforge-11r Mode: (Auto)

Freq/Channel: 5180/36 Rate: OS Default

WPA WPA2 WPA3 OSEN WEP

Disable HT40 Enable VHT160 Disable SGI

Print
Display
Probe
Display Scan
Sync
Apply
OK
Cancel

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.

sta0000 (If0313-6477) Configure Settings

Port Status Information
Current: LINK-UP GRO Authorized
Driver Info: Port Type: WIFI-STA Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: **FT-EAP (11r)** HESSID: 00:00:00:00:00:00
Pairwise Ciphers: DEFAULT Realm:
Group Ciphers: DEFAULT Client Cert:
WPA PSK: IMSI:
EAP Methods: **EAP-TTLS** Milenage:
EAP Identity: testuser Domain:
EAP Anon Identity: Consortium:
EAP Password: testpasswd Phase-1:
EAP Pin: Phase-2:
Private Key: PK Password:
CA Cert File: PAC File:
Network Auth: IEEE80211w: Disabled (0)

Advanced/802.1x Enable 802.11u HotSpot 2.0 Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel