

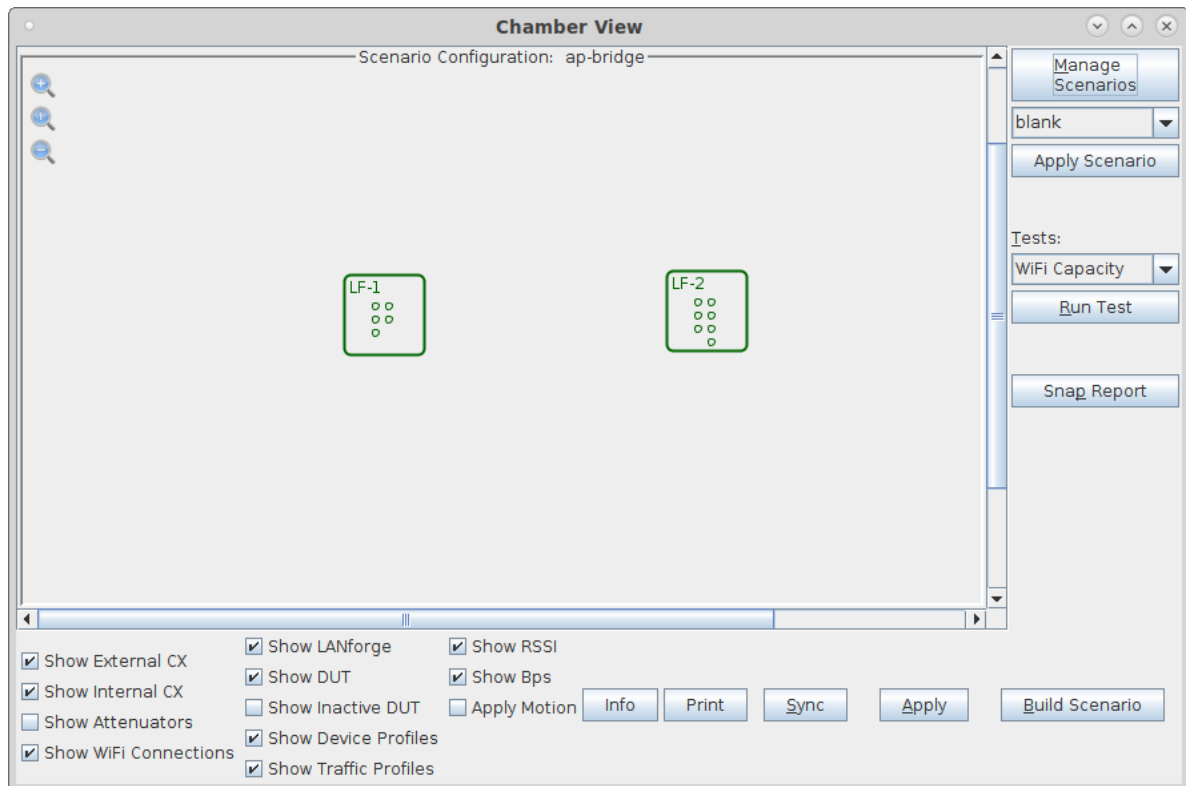
LANforge as 802.11k/v/r Access Point Cluster

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

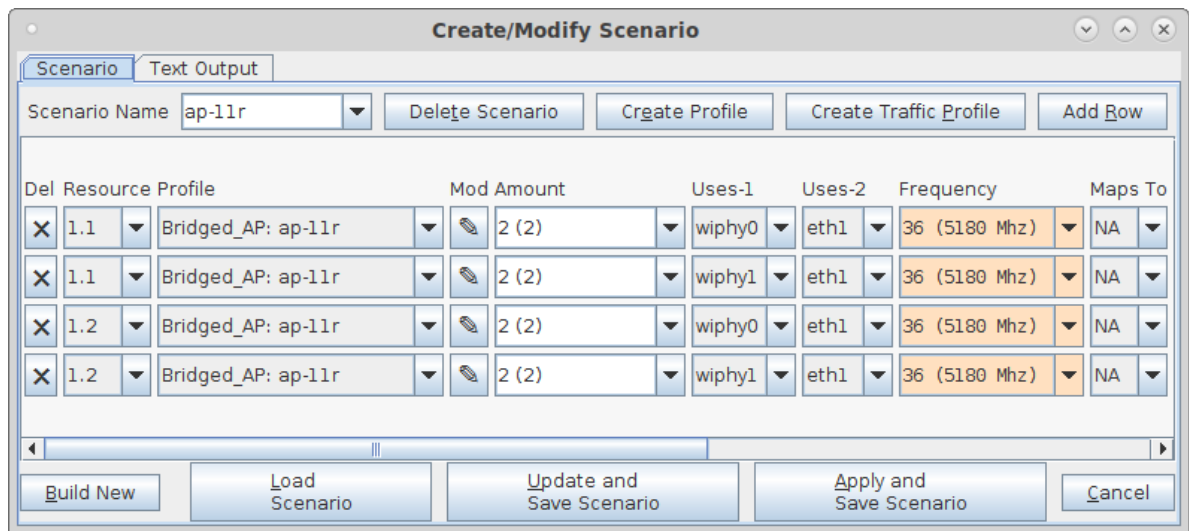
In this test scenario, two LANforge CT522 systems are used to create 8 APs. The APs can be used for 802.11k/v/r roaming and related testing. No external radius server is needed. The 'eth1' interfaces on the two LANforges should be connected to the same LAN. NOTE: As of this writing, there is a bug when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



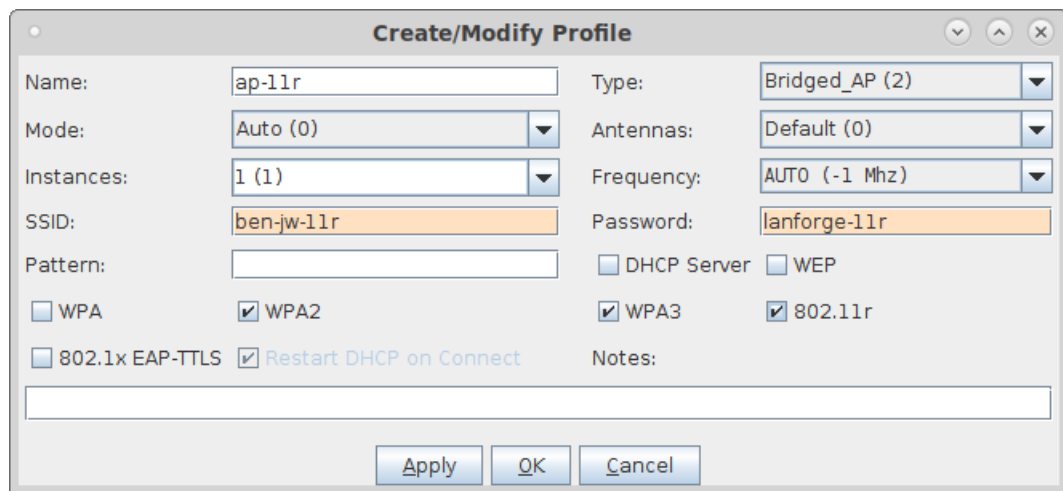
- B. Configure a Chamber View Scenario and add the AP profiles.



The 'Create/Modify Scenario' dialog box shows a table with four rows of configuration. Each row represents a resource profile with a delete icon, a dropdown for the profile name, a dropdown for the mod amount, and two dropdowns for 'Uses-1' and 'Uses-2'. The 'Frequency' column shows '36 (5180 Mhz)' for all rows, and the 'Maps To' column shows 'NA' for all rows. The 'Scenario Name' is 'ap-11r'. Buttons at the bottom include 'Build New', 'Load Scenario', 'Update and Save Scenario', 'Apply and Save Scenario', and 'Cancel'.

Del	Resource Profile	Mod Amount	Uses-1	Uses-2	Frequency	Maps To
X	1.1 Bridged_AP: ap-11r	2 (2)	wiphy0	eth1	36 (5180 Mhz)	NA
X	1.1 Bridged_AP: ap-11r	2 (2)	wiphy1	eth1	36 (5180 Mhz)	NA
X	1.2 Bridged_AP: ap-11r	2 (2)	wiphy0	eth1	36 (5180 Mhz)	NA
X	1.2 Bridged_AP: ap-11r	2 (2)	wiphy1	eth1	36 (5180 Mhz)	NA

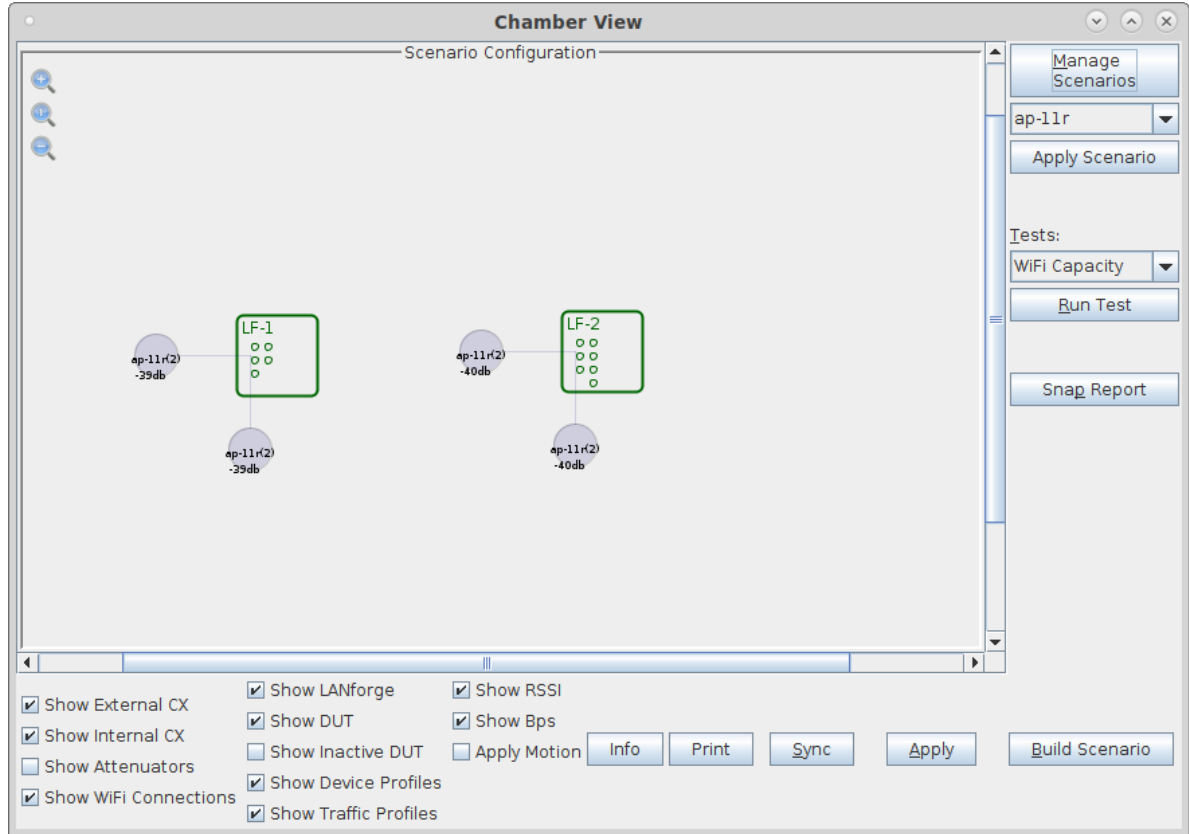
- C. This example uses one 802.11r AP profile for all APs.



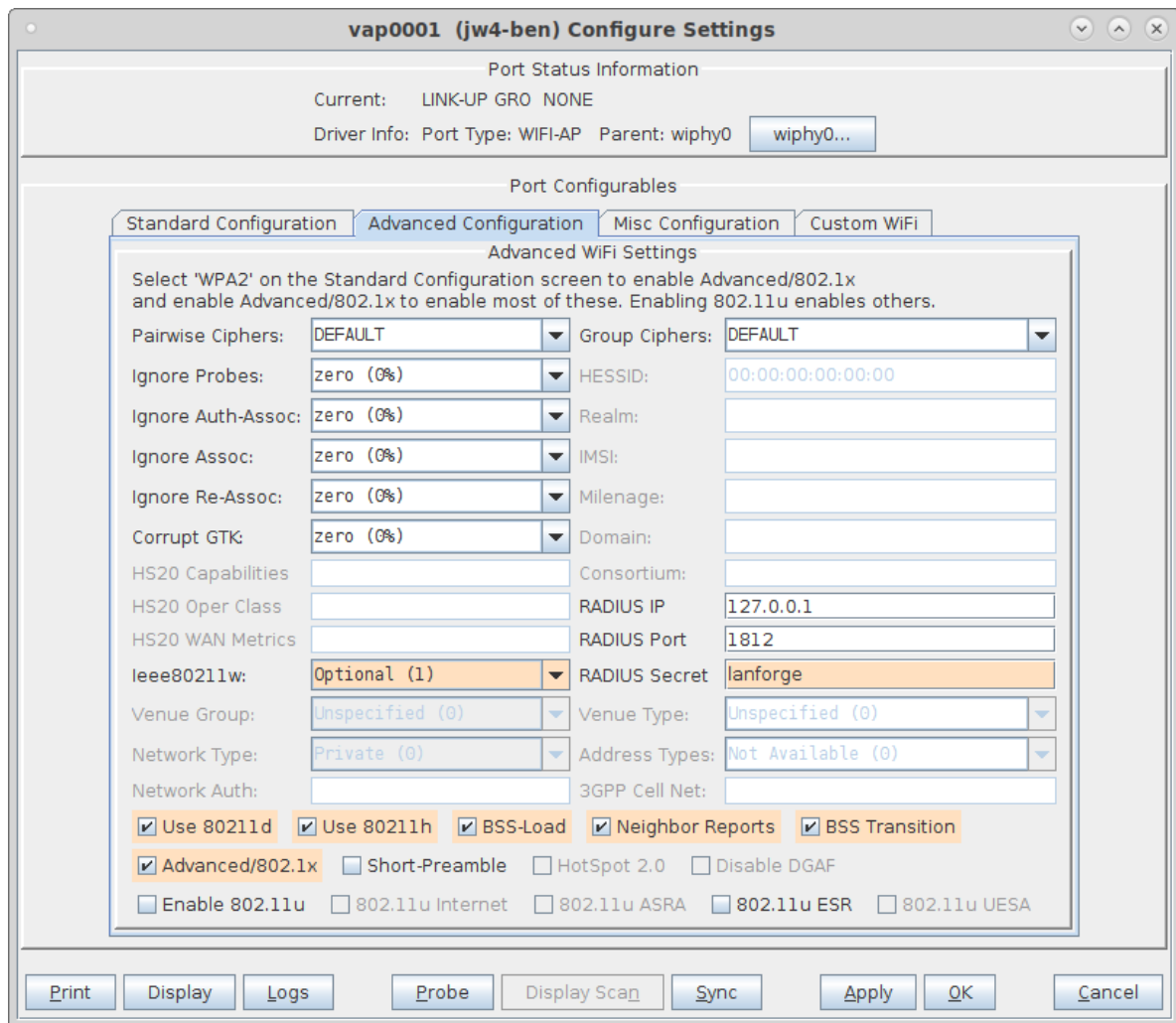
The 'Create/Modify Profile' dialog box shows configuration for a profile named 'ap-11r'. The 'Type' is 'Bridged_AP (2)'. The 'Mode' is 'Auto (0)'. The 'Instances' is '1 (1)'. The 'SSID' is 'ben-jw-11r'. The 'Password' is 'lanforge-11r'. The 'Pattern' is empty. The 'WPA' checkbox is checked, and the 'WPA2' checkbox is checked. The '802.1x EAP-TTLS' checkbox is checked, and the 'Restart DHCP on Connect' checkbox is checked. The 'DHCP Server' checkbox is unchecked, and the 'WEP' checkbox is unchecked. The 'WPA3' checkbox is checked, and the '802.11r' checkbox is checked. The 'Notes' field is empty. Buttons at the bottom include 'Apply', 'OK', and 'Cancel'.

Name: ap-11r Type: Bridged_AP (2)
Mode: Auto (0) Antennas: Default (0)
Instances: 1 (1) Frequency: AUTO (-1 Mhz)
SSID: ben-jw-11r Password: lanforge-11r
Pattern:
☐ WPA ☒ WPA2 ☐ DHCP Server ☐ WEP
☐ 802.1x EAP-TTLS ☒ Restart DHCP on Connect ☒ WPA3 ☒ 802.11r
Notes:
Apply OK Cancel

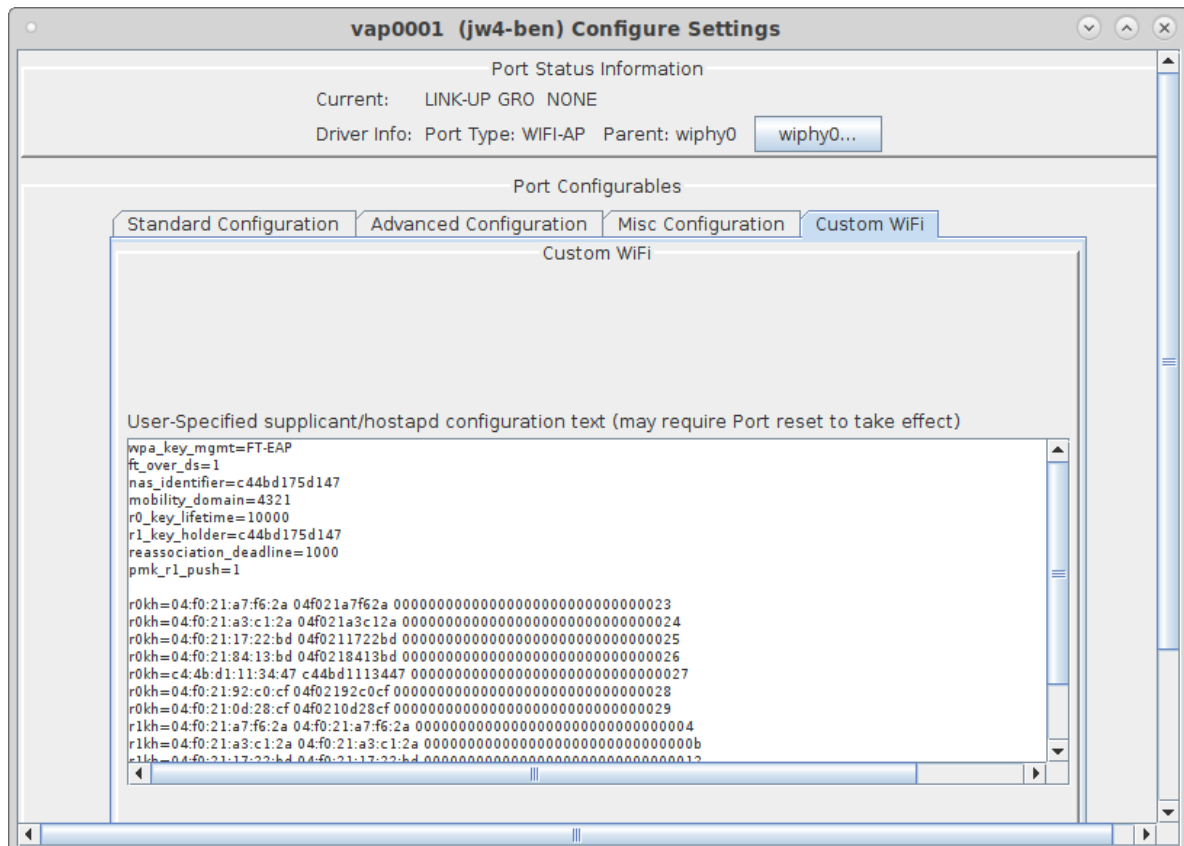
- D. Once you have saved and selected the Scenario, click **Apply Scenario** and then click **Build Scenario**. The APs will be created, bridge devices will be created and will contain the APs and the Ethernet ports selected in the scenario. A radius server will be created and started. The Access Point 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 .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

Enable

- ☐ Set MAC
- ☐ Set TX Q Len
- ☐ Set MTU
- ☐ Set Offload
- ☐ Set PROMISC

Services

- ☐ HTTP
- ☐ FTP
- ☐ RADIUS

Low Level

- ☐ PROMISC
- ☒ TSO Enabled
- ☐ UFO Enabled
- ☒ GSO Enabled
- ☐ LRO Enabled
- ☒ GRO Enabled

General Interface Settings

☐ Down ☐ Aux-Mgt

☐ DHCP-IPv6 ☒ DHCP Release DHCP Vendor ID:

☒ DHCP-IPv4 [Secondary-IPs](#) DHCP Client ID:

DNS Servers: Peer IP:

IP Address: Global IPv6:

IP Mask: Link IPv6:

Gateway IP: IPv6 GW:

Alias: MTU:

MAC Addr: TX Q Len:

Rpt Timer: WiFi Bridge:

WiFi Settings

SSID: AP:

Key/Phrase: Mode:

Freq/Channel: 5180/36 Rate:

☐ 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 (lf0313-6477) 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