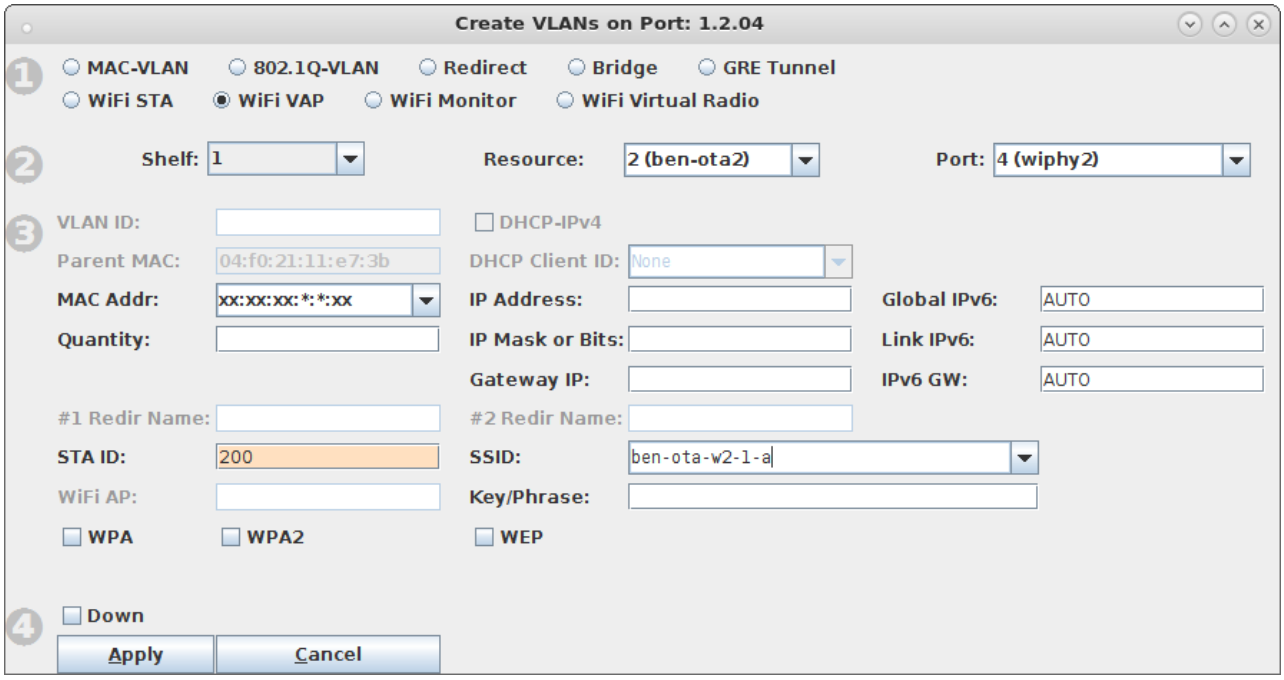
sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

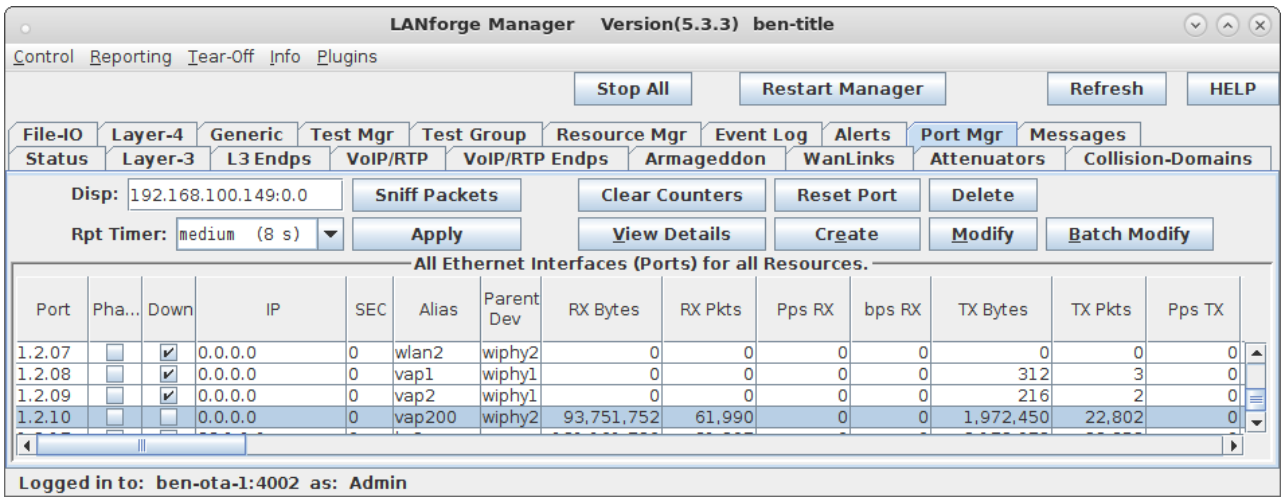
LANforge WiFi Degraded vAP Testing

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.

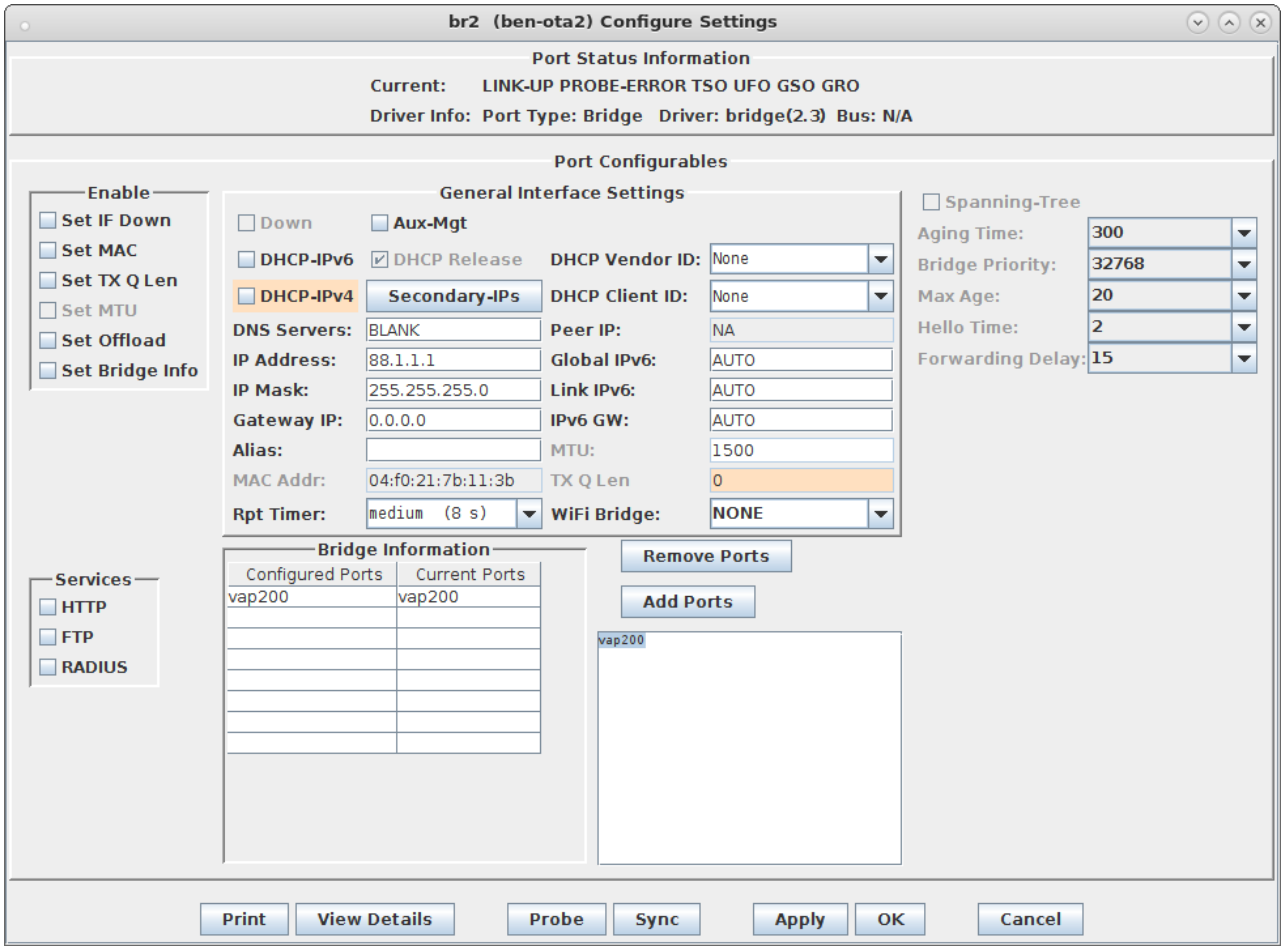


2. In the **Ports** tab you will see the new WiFi vAP:

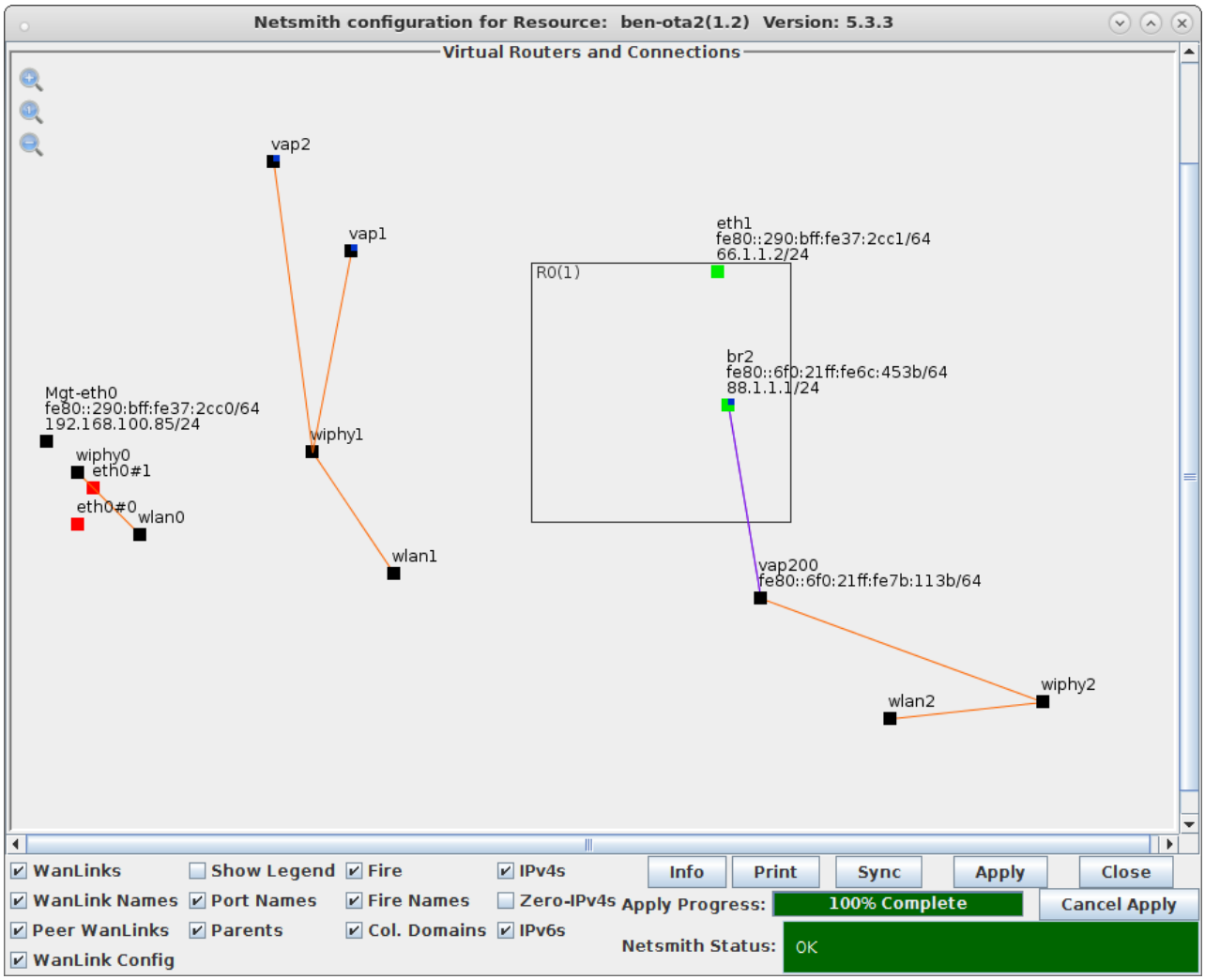


3. Select the **Status** panel in the LANforge GUI, and click the Netsmith button for the appropriate resource. Right-click and select the 'New Bridge' option. In this example, I selected 'br2' as the bridge name. After creating the bridge, click Sync to show the new bridge device. Right-click on br2 and select Modify Port. Add the vAP

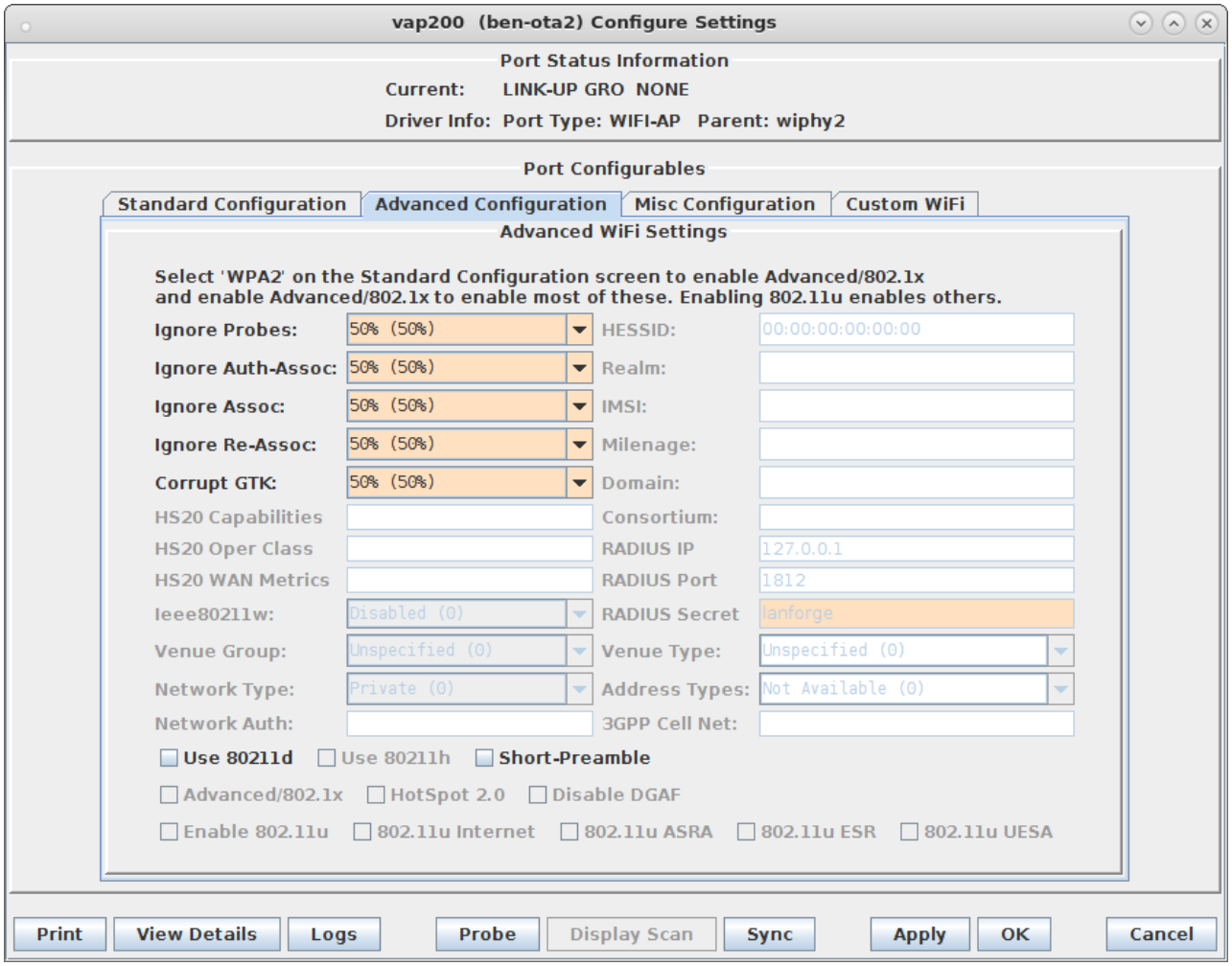
you just created to the bridge with the Add Ports button and then apply:



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:

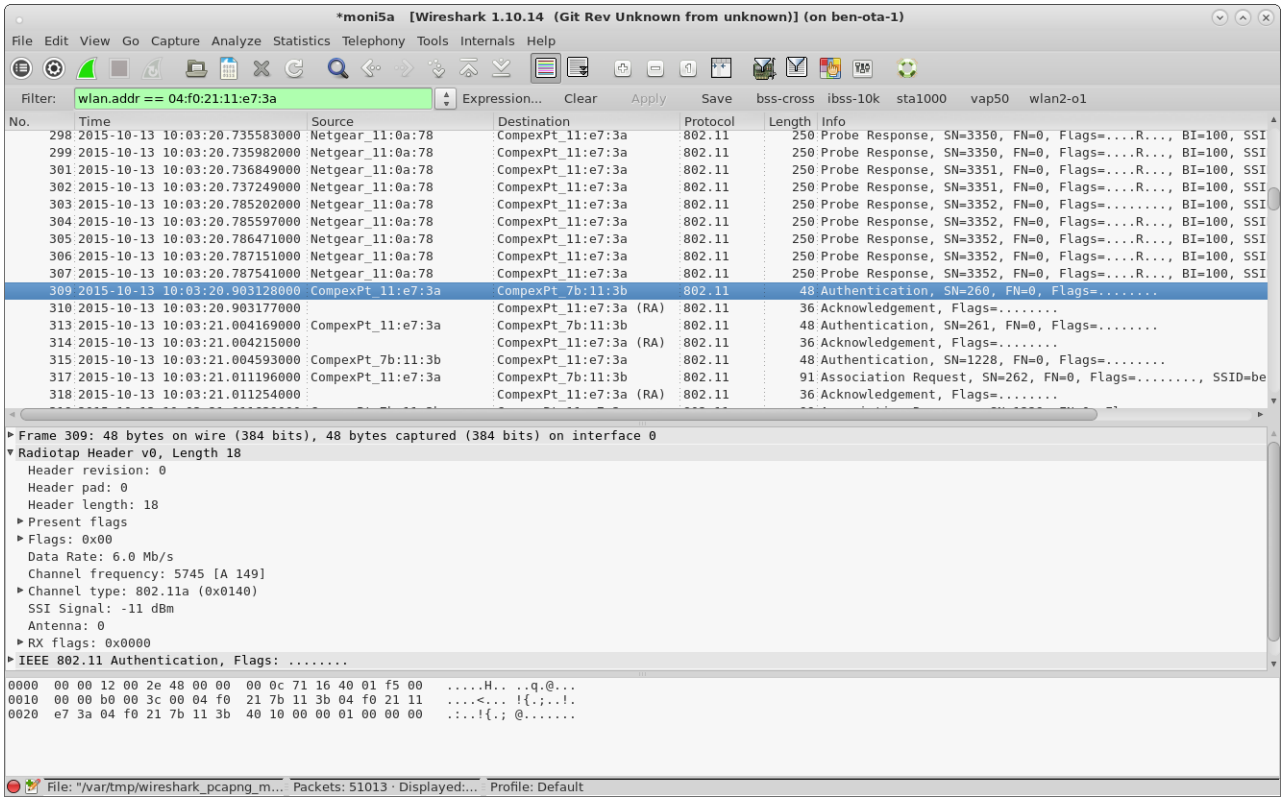


5. Now, we should have 1 vAP able to accept stations and give out DHCP addresses. For an initial test, make sure the DUT can connect to the vAP and get an IP address. Once that is verified, right-click and choose Port Modify on the vap200 vAP. We will now configure it to not respond to 50% of the management 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):



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 has increasing impairment of management frames.