

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.

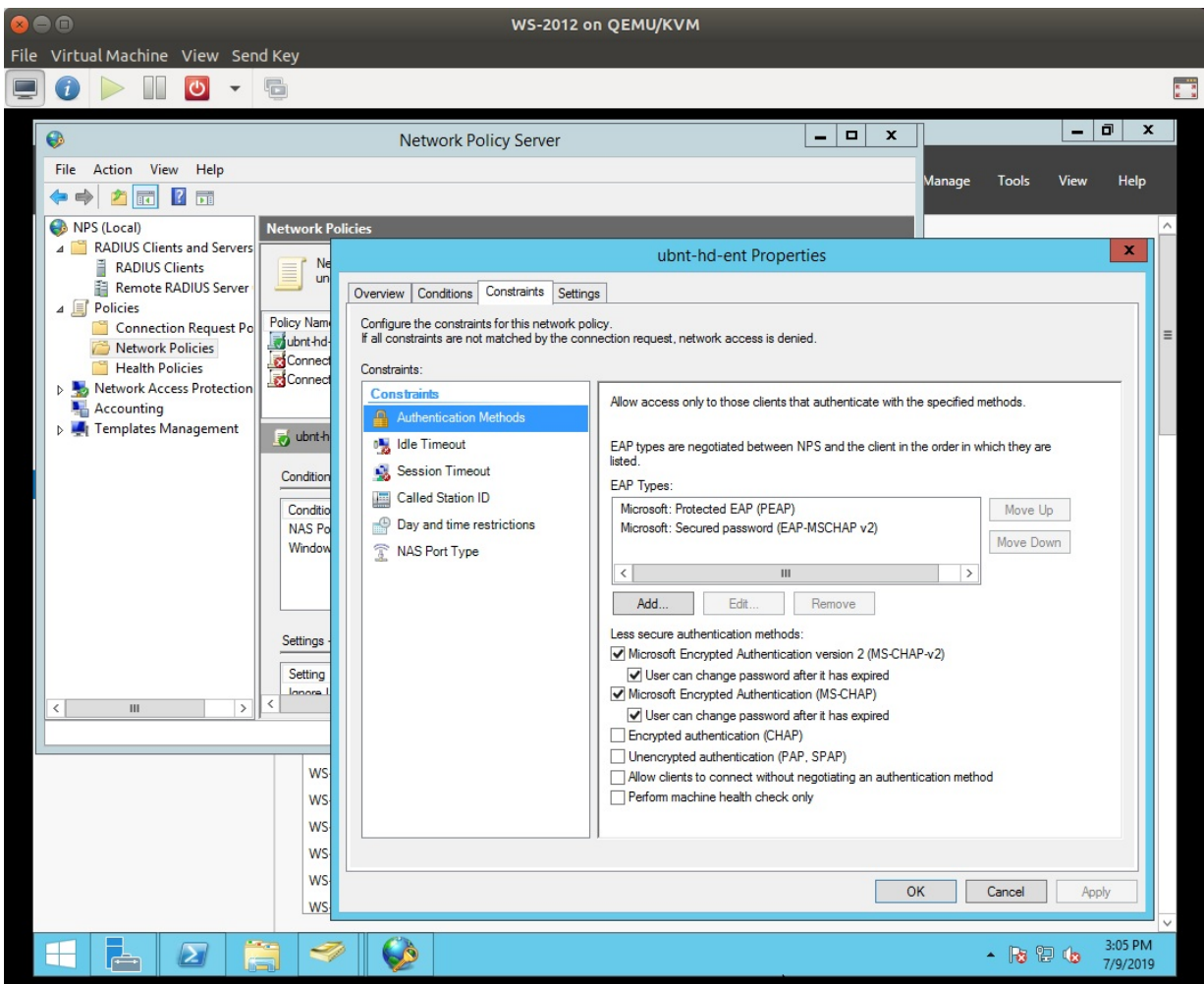
The screenshot shows the Windows Server Manager interface for a server named 'WS-2012'. The 'SERVERS' section displays a table with the following data:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WS-2012	192.168.100.77, 192.168.2.154	Online - Performance counters not started	7/9/2019 3:25:55 PM	00252-10000-00000-AA

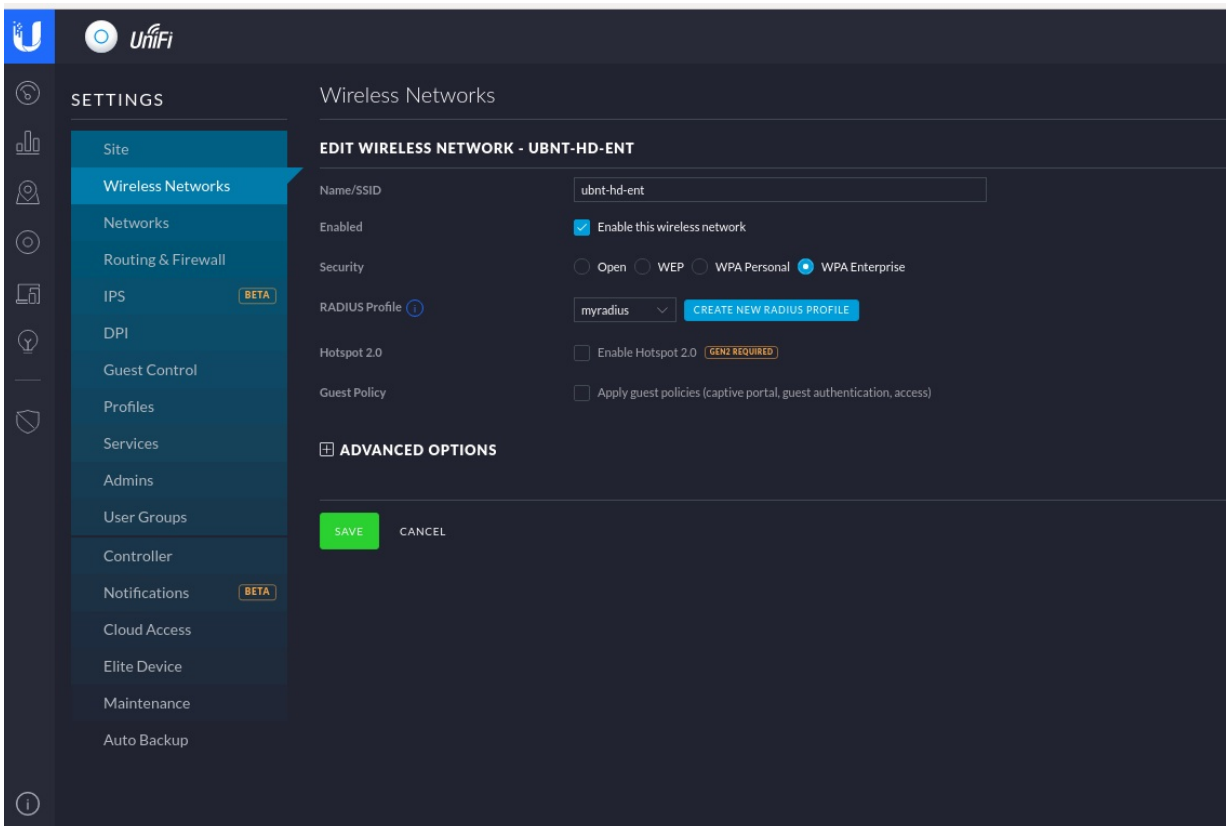
The 'EVENTS' section shows a list of 16 total events, all of which are errors from the NPS System log on 7/9/2019:

Server Name	ID	Severity	Source	Log	Date and Time
WS-2012	13	Error	NPS	System	7/9/2019 9:24:25 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:19 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:13 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:10 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:01 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:23:49 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:23:43 AM

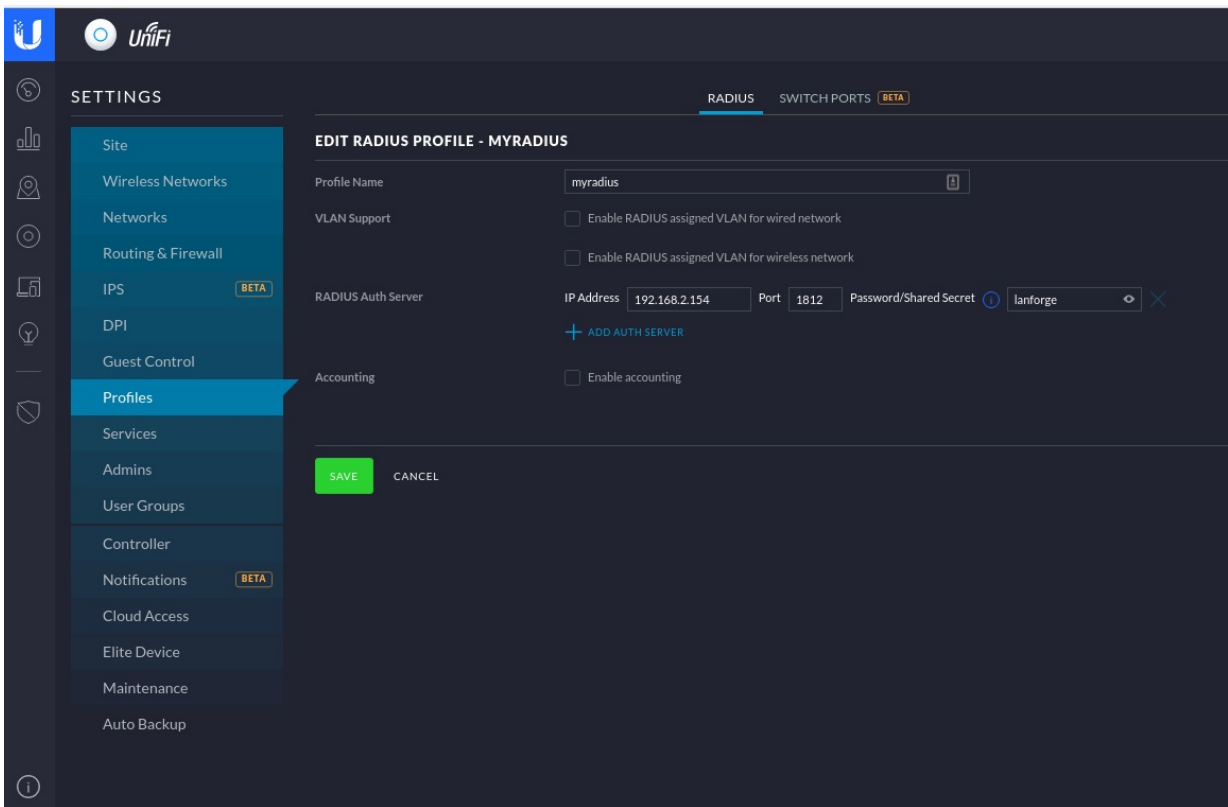
2. RADIUS Server has both EAP-PEAP and MSCHAPv2 configured for use.



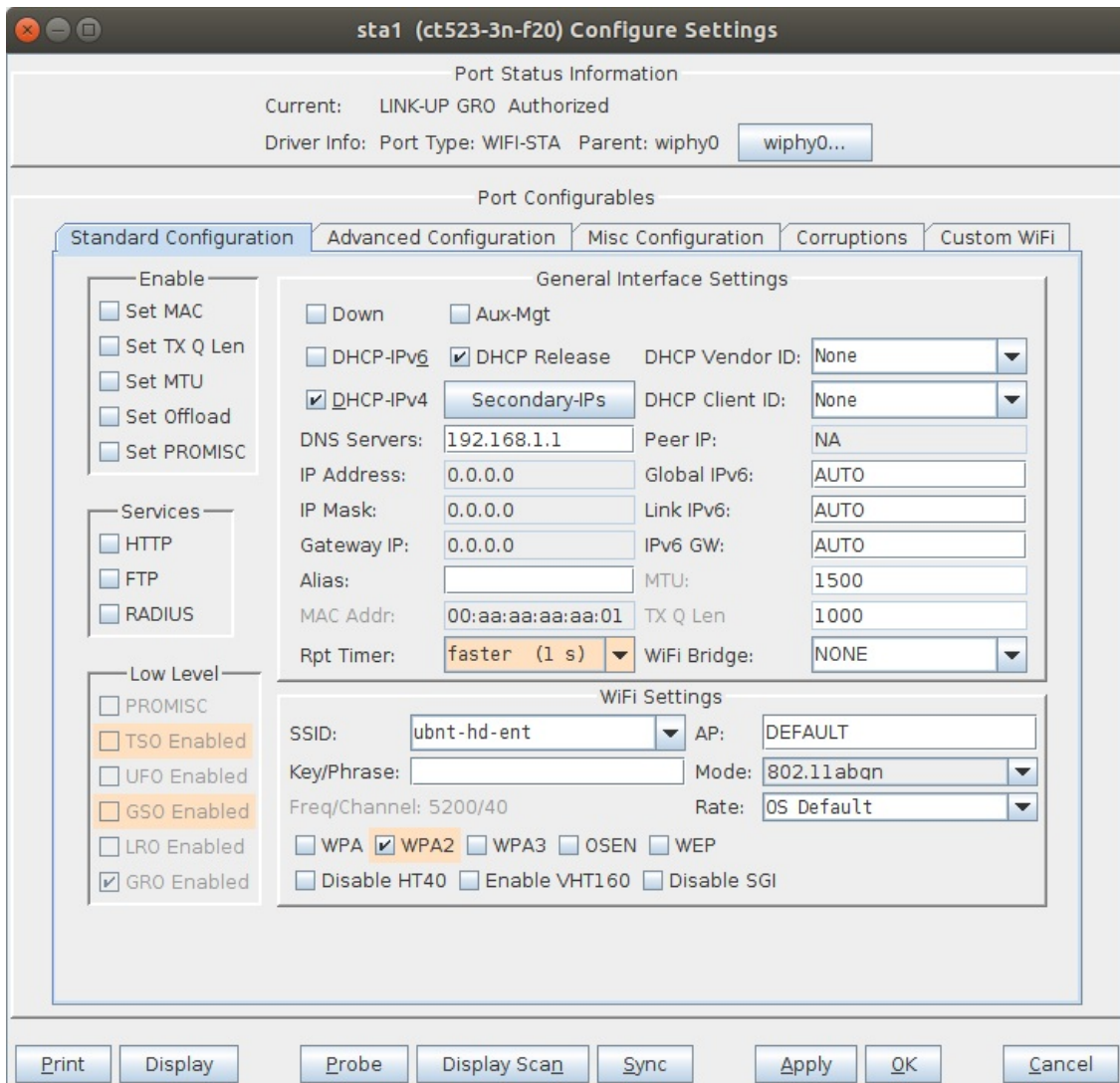
3. AP is a Ubiquiti HD AP with SSID ubnt-hd-ent with WPA Enterprise security.



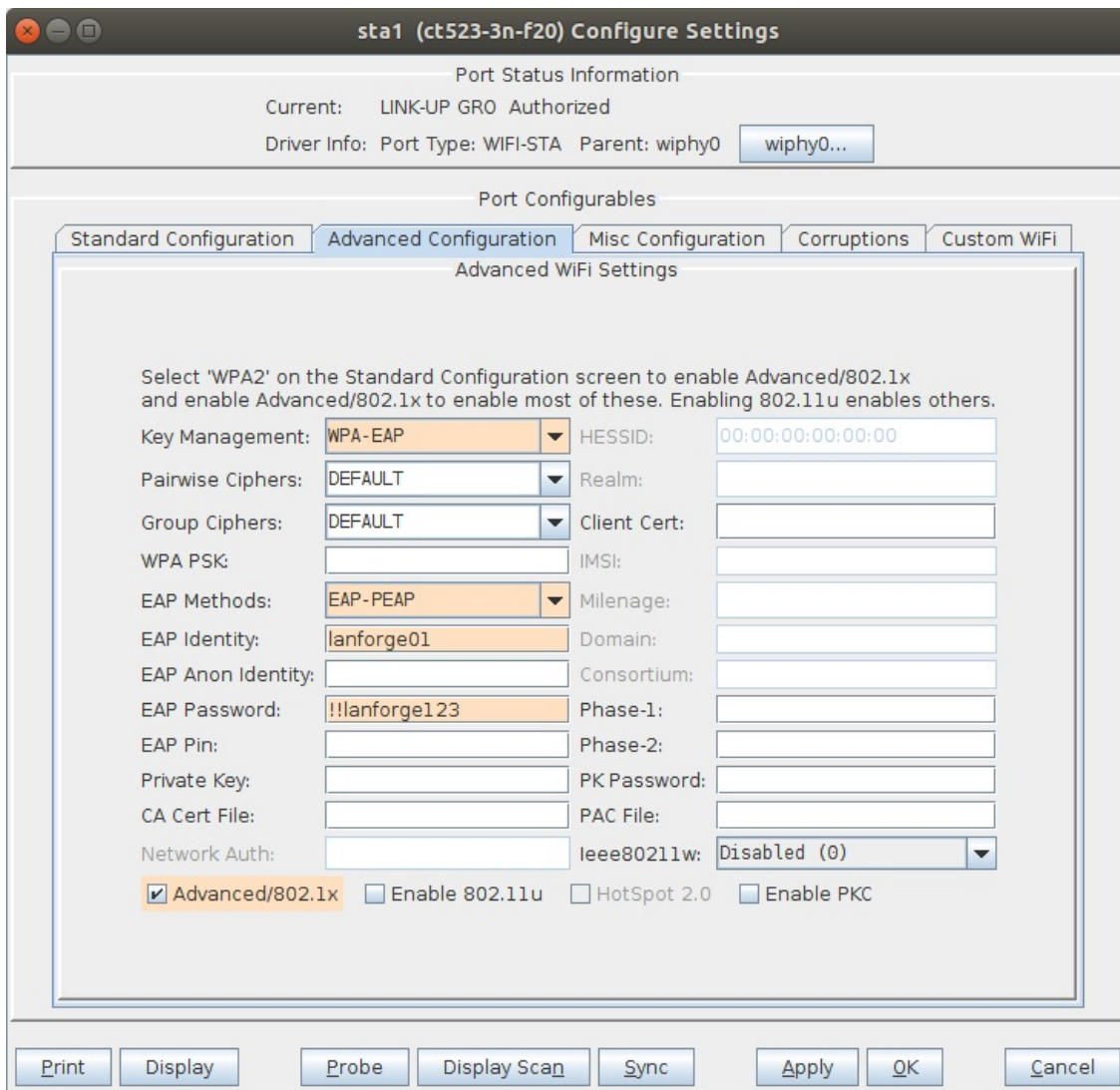
4. The AP controller points to the RADIUS server at 192.168.2.154.



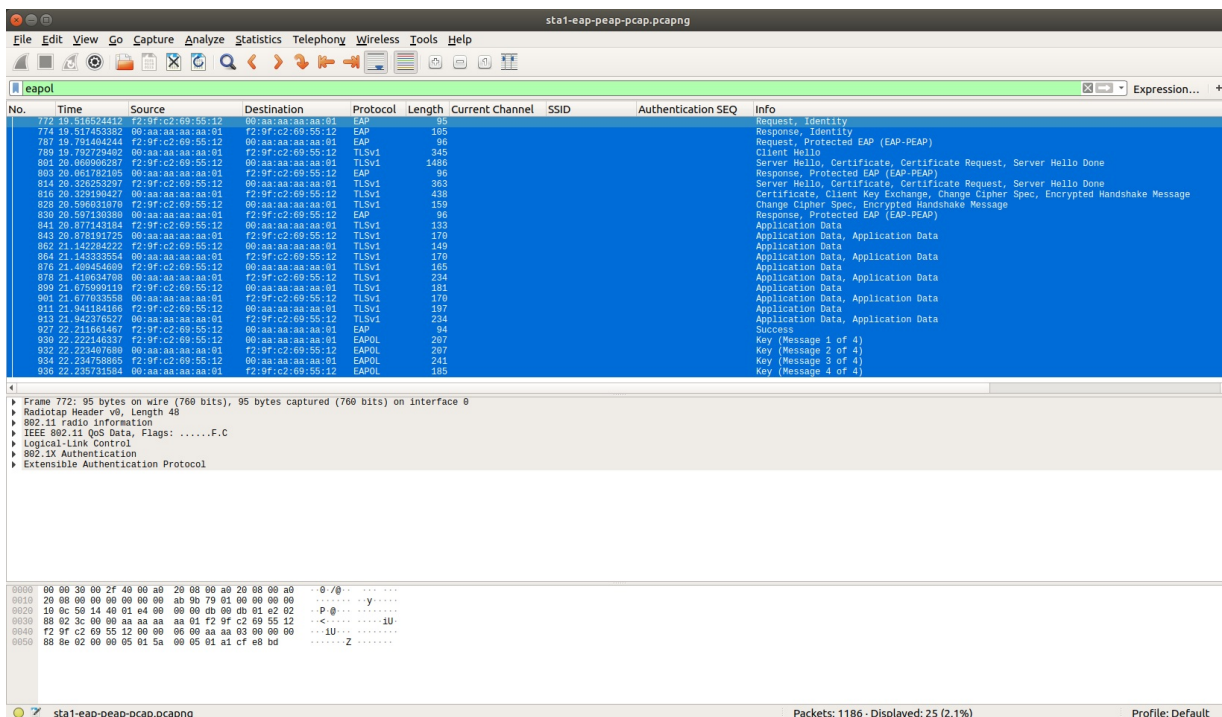
5. LANforge STA1 basic configuration:



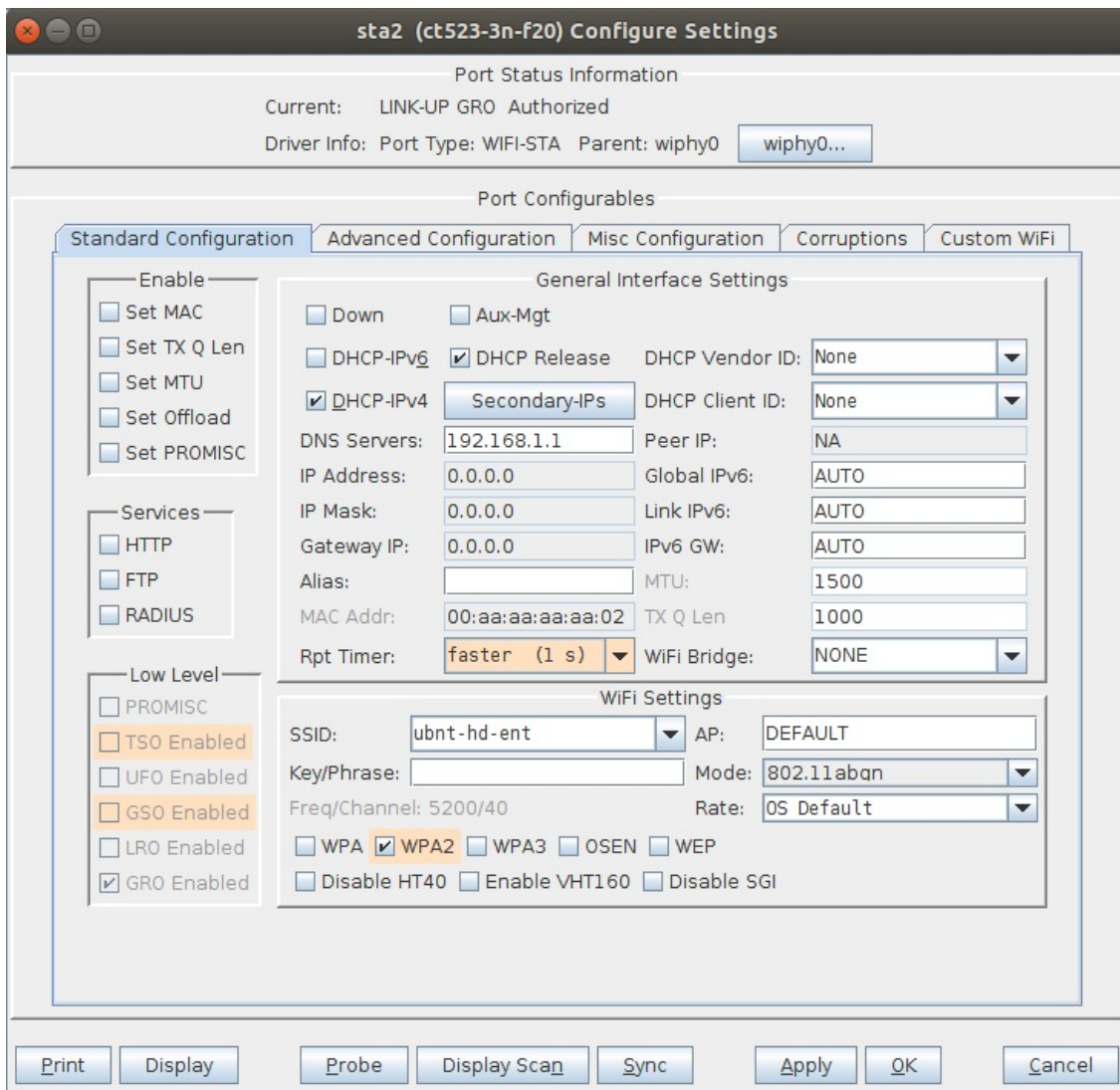
6. LANforge STA1 advanced configuration is using EAP-PEAP.



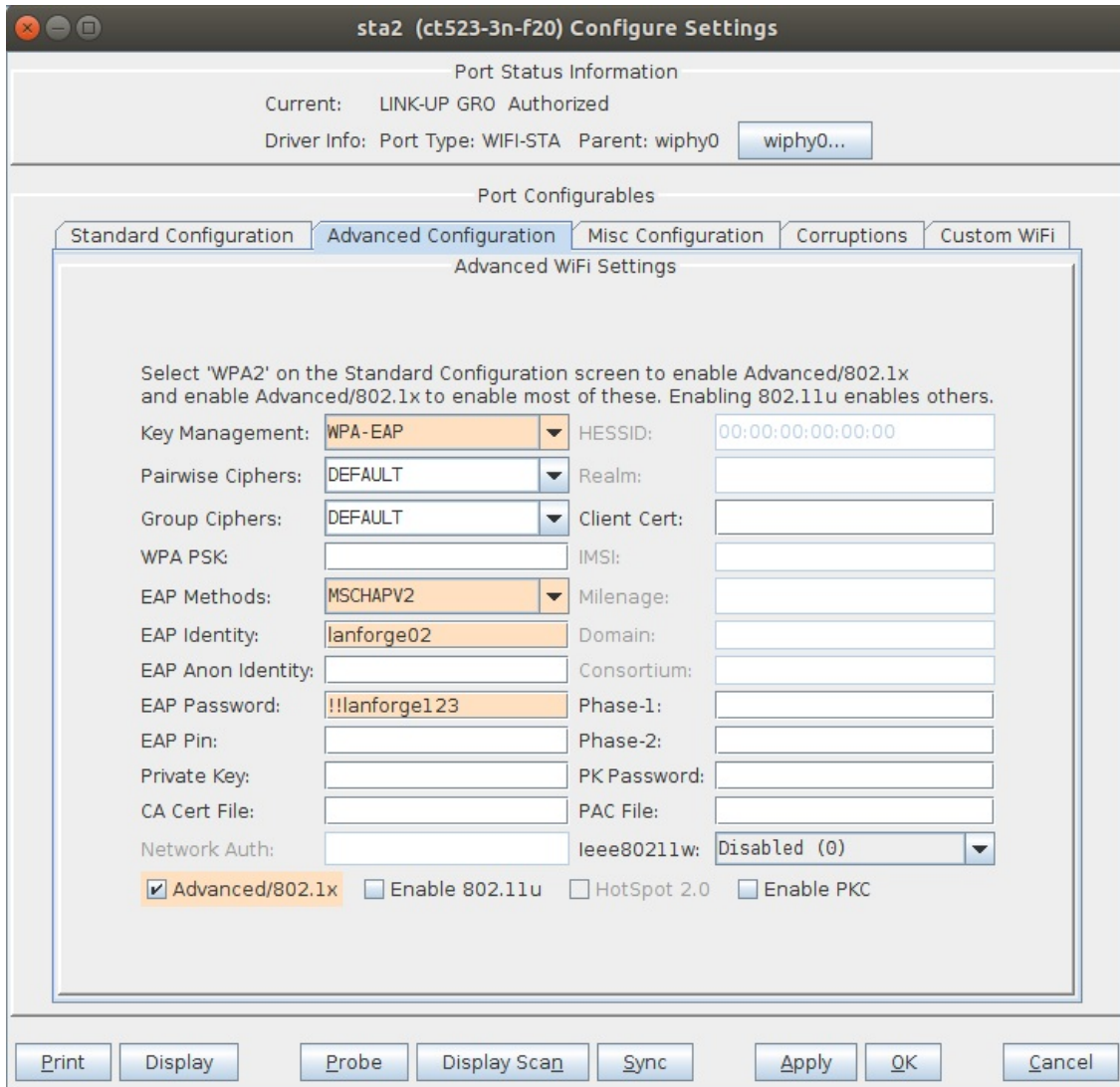
7. Wireshark capture of STA1 EAPOL authentication.



8. LANforge STA2 basic configuration:



9. LANforge STA2 advanced configuration is using MSCHAPv2.



10. Wireshark capture of STA2 EAPOL authentication.

