

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.

The screenshot shows the configuration interface for a virtual access point (vap2). The 'WIFI Settings' section is highlighted with a red box, indicating the configuration for WPA3 security. The SSID is set to 'ABCD-wpa3' and the Key/Phrase is 'hello123'. The security mode is set to 'WPA3', and the 'Verbose Debug' checkbox is also checked.

Section	Parameter	Value
General Interface Settings	Down	<input type="checkbox"/>
	Aux-Mgt	<input type="checkbox"/>
	DHCP-IPv6	<input type="checkbox"/>
	DHCP-IPv4	<input type="checkbox"/>
	DHCP Release	<input checked="" type="checkbox"/>
	DHCP Vendor ID	None
	DHCP Client ID	None
	DNS Servers	BLANK
	IP Address	20.100.1.1
	IP Mask	255.255.255.0
Gateway IP	0.0.0.0	
Peer IP	NA	
Global IPv6	AUTO	
Link IPv6	AUTO	
IPv6 GW	AUTO	
Alias		
MTU	1500	
MAC Addr	00:0e:8e:6c:2d:b5	
TX Q Len	1000	
Rpt Timer	medium (8 s)	
WIFI Bridge	NONE	
IPSec GW	0.0.0.0	
IPSec Password		
IPSec Local ID		
IPSec Remote ID		
WIFI Settings	SSID	ABCD-wpa3
	Key/Phrase	hello123
	Mode	(802.11abgn-AC)
	Rate	0S Default
	Freq/Channel	5745/149
	DTIM-Period	2
	Max-STA	2007
	Beacon	240
	WPA	<input type="checkbox"/>
	WPA2	<input type="checkbox"/>
WPA3	<input checked="" type="checkbox"/>	
OSEN	<input type="checkbox"/>	
WEP	<input type="checkbox"/>	
Verbose Debug	<input checked="" type="checkbox"/>	
Disable HT40	<input type="checkbox"/>	
Disable HT80	<input type="checkbox"/>	
Enable VHT160	<input type="checkbox"/>	
Disable SGI	<input type="checkbox"/>	

B. Setup the VAP with 11w PMF option Required.

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy1 wiphy1...

Port Configurables
Standard Configuration Advanced Configuration Misc Configuration 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.

Pairwise Ciphers:	DEFAULT	Group Ciphers:	DEFAULT
Ignore Probes:	zero (0%)	HESSID:	00:00:00:00:00:00
Ignore Auth-Assoc:	zero (0%)	Realm:	
Ignore Assoc:	zero (0%)	IMSI:	
Ignore Re-Assoc:	zero (0%)	Milenage:	
Corrupt GTK:	zero (0%)	Domain:	
HS20 Capabilities		Consortium:	
HS20 Oper Class		RADIUS IP	127.0.0.1
HS20 WAN Metrics		RADIUS Port	1812
leee80211w:	Required (2)	RADIUS Secret	lanforge
Venue Group:	Unspecified (0)	Venue Type:	Unspecified (0)
Network Type:	Private (0)	Address Types:	Not Available (0)
Network Auth:		3GPP Cell Net:	

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

Print Display Logs Probe Display Scan Sync Apply OK Cancel

C. Setup the STA with SSID, WPA3 security and a PSK.

The screenshot shows the configuration interface for a wireless station (sta202). The window title is "sta202 (ct523-3n-f20) Configure Settings".

Port Status Information:
Current: LINK-UP GRO Authorized
Driver Info: Port Type: WIFI-STA Parent: wiphy2 [wiphy2...]

Port Configurables:
Standard Configuration | Advanced Configuration | Misc Configuration | Corruptions | Custom WiFi

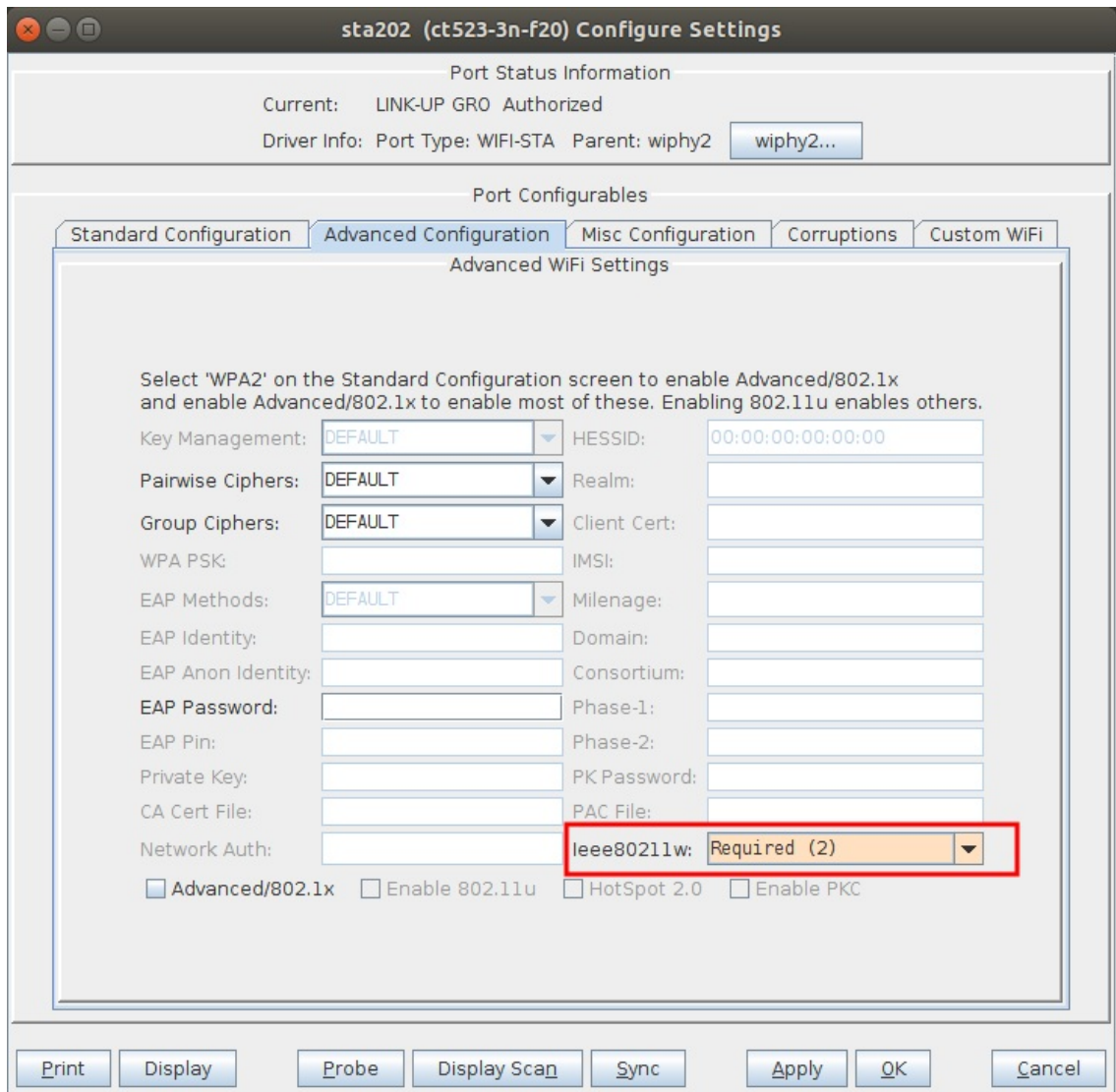
General Interface Settings:
Enable: Set MAC, Set TX Q Len, Set MTU, Set Offload, Set PROMISC
Services: HTTP, FTP, RADIUS, IPSEC-Client, IPsec-Upstream
Low Level: PROMISC, TSO Enabled, UFO Enabled, GSO Enabled, LRO Enabled, GRO Enabled

General Interface Settings (Detailed):
 Down Aux-Mgt
 DHCP-IPv6 DHCP Release DHCP Vendor ID: None
 DHCP-IPv4 Secondary-IPs DHCP Client ID: None
DNS Servers: BLANK 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: 00:03:7f:30:e0:00 TX Q Len: 1000
Rpt Timer: medium (8 s) WiFi Bridge: NONE
IPSec GW: 0.0.0.0 IPSec Password:
IPSec Local ID.: IPSec Remote ID.:

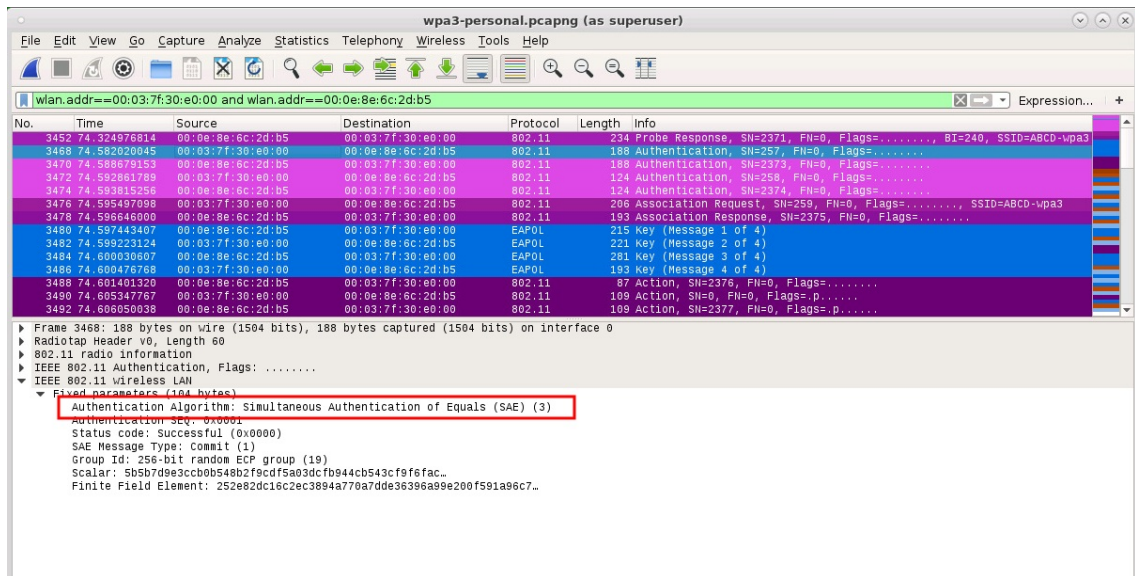
WiFi Settings:
SSID: ABCD-wpa3 AP: DEFAULT
Key/Phrase: hello123 Mode: 802.11abgn-AC
Freq/Channel: 5745/149 Rate: 0S Default
 WPA WPA2 WPA3 OSEN WEP
 Disable HT40 Enable VHT160 Disable SGI

Buttons: Print, Display, Probe, Display Scan, Sync, Apply, OK, Cancel

D. Setup the STA with 11w PMF option Required.



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.

vap2 (ct521-1ac-f20) Configure Settings

Port Status Information
Current: LINK-UP GRO NONE
Driver Info: Port Type: WIFI-AP Parent: wiphy1 wiphy1...

Port Configurables

Standard Configuration | Advanced Configuration | Misc Configuration | Custom WiFi

Enable

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

Services

- HTTP
- FTP
- IPSEC-Client
- IPsec-Upstream

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: None
- DHCP-IPv4 **Secondary-IPs** DHCP Client ID: None
- DNS Servers: BLANK Peer IP: NA
- IP Address: 20.100.1.1 Global IPv6: AUTO
- IP Mask: 255.255.255.0 Link IPv6: AUTO
- Gateway IP: 0.0.0.0 IPv6 GW: AUTO
- Alias: MTU: 1500
- MAC Addr: 00:0e:8e:6c:2d:b5 TX Q Len: 1000
- Rpt Timer: medium (8 s) WiFi Bridge: NONE
- IPSec GW: 0.0.0.0 IPSec Password:
- IPSec Local ID.:
- IPSec Remote ID.:

WiFi Settings

- SSID: ABCDE-wpa3 AP: DEFAULT
- Key/Phrase: Mode: (802.11abgn-AC)
- Freq/Channel: 5/45/149 Rate: OS Default
- DTIM-Period: 2 Max-STA: 2007
- Beacon: 240
- WPA WPA2 WPA3 OSEN WEP Verbose Debug
- Disable HT40 Disable HT80 Enable VHT160 Disable SGI

Print | Display | Logs | Probe | Display Scan | Sync | Apply | OK | Cancel

- 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.

The screenshot shows the configuration interface for a wireless station (sta203). The window title is "sta203 (ct523-3n-f20) Configure Settings".

Port Status Information:
Current: LINK-UP GRO Authorized
Driver Info: Port Type: WIFI-STA Parent: wiphy2 [wiphy2...]

Port Configurables:
Standard Configuration | Advanced Configuration | Misc Configuration | Corruptions | Custom WiFi

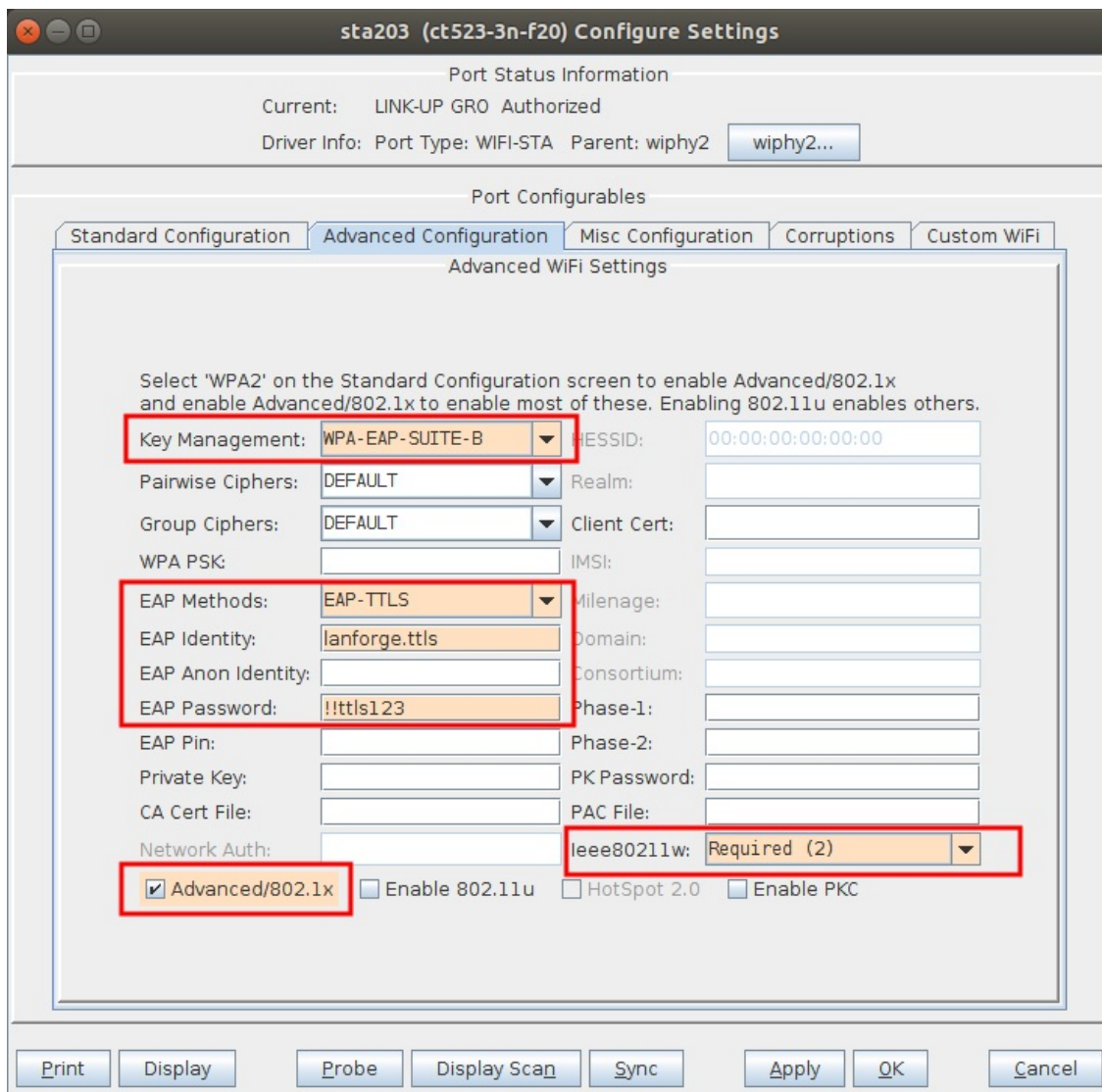
General Interface Settings:
Enable: Set MAC, Set TX Q Len, Set MTU, Set Offload, Set PROMISC
Services: HTTP, FTP, RADIUS, IPSEC-Client, IPsec-Upstream
Low Level: PROMISC, TSO Enabled, UFO Enabled, GSO Enabled, LRO Enabled, GRO Enabled

General Interface Settings (Main):
 Down Aux-Mgt
 DHCP-IPv6 DHCP Release DHCP Vendor ID: None
 DHCP-IPv4 Secondary-IPs DHCP Client ID: None
DNS Servers: BLANK 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: 00:03:7f:ce:63:00 TX Q Len: 1000
Rpt Timer: medium (8 s) WiFi Bridge: NONE
IPSec GW: 0.0.0.0 IPSec Password:
IPSec Local ID.: IPSec Remote ID.:

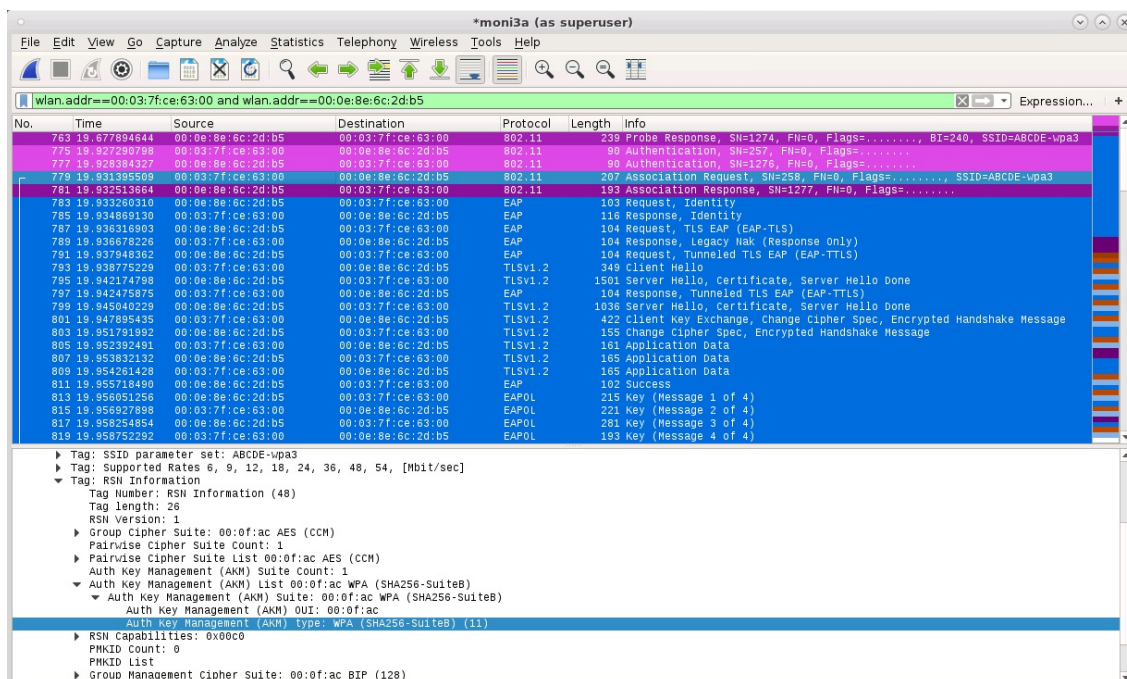
WiFi Settings:
SSID: ABCDE-wpa3 AP: DEFAULT
Key/Phrase: Mode: 802.11abgn-AC
Freq/Channel: 5745/149 Rate: 0S Default
 WPA WPA2 WPA3 OSEN WEP
 Disable HT40 Enable VHT160 Disable SGI

Buttons: Print, Display, Probe, Display Scan, Sync, Apply, OK, Cancel

- 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.

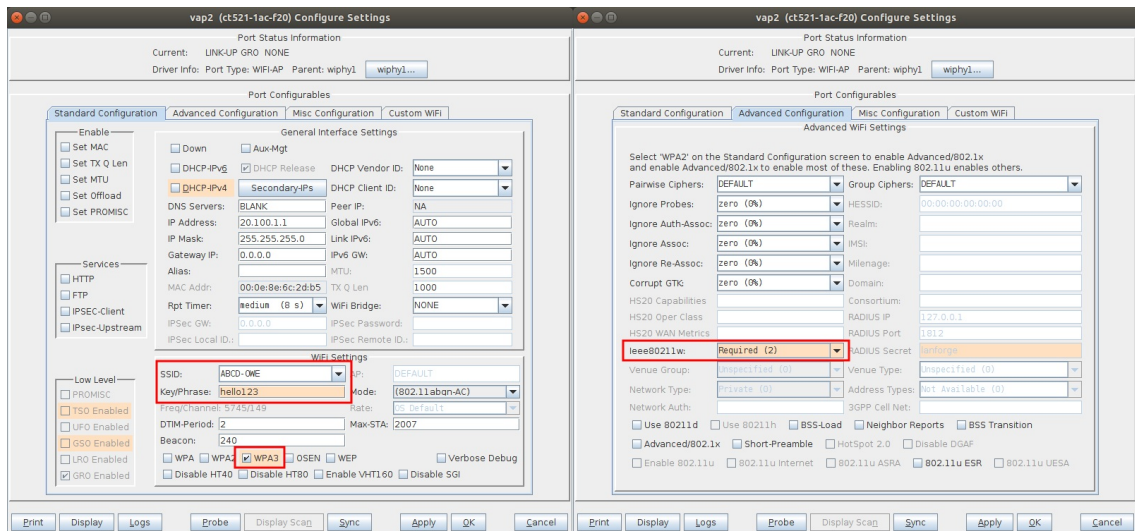


- G. A capture of the association.



3. WPA3 OWE - Opportunistic Wireless Encryption.

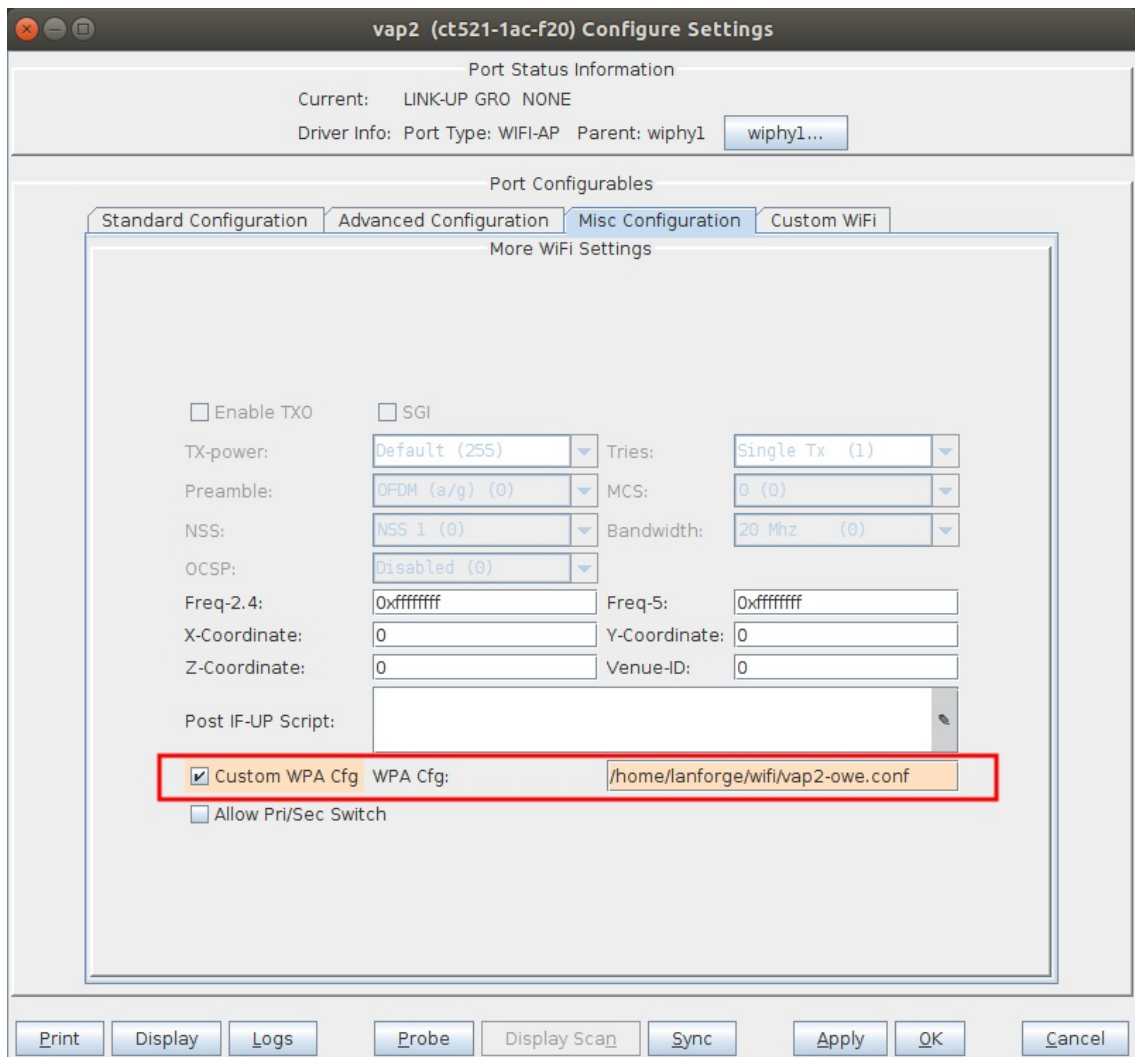
- A. Setup the VAP with WPA3 security and a PSK on the standard configuration, then select option 11w PMF option Required on the advanced configuration, then admin up the VAP.



- 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.



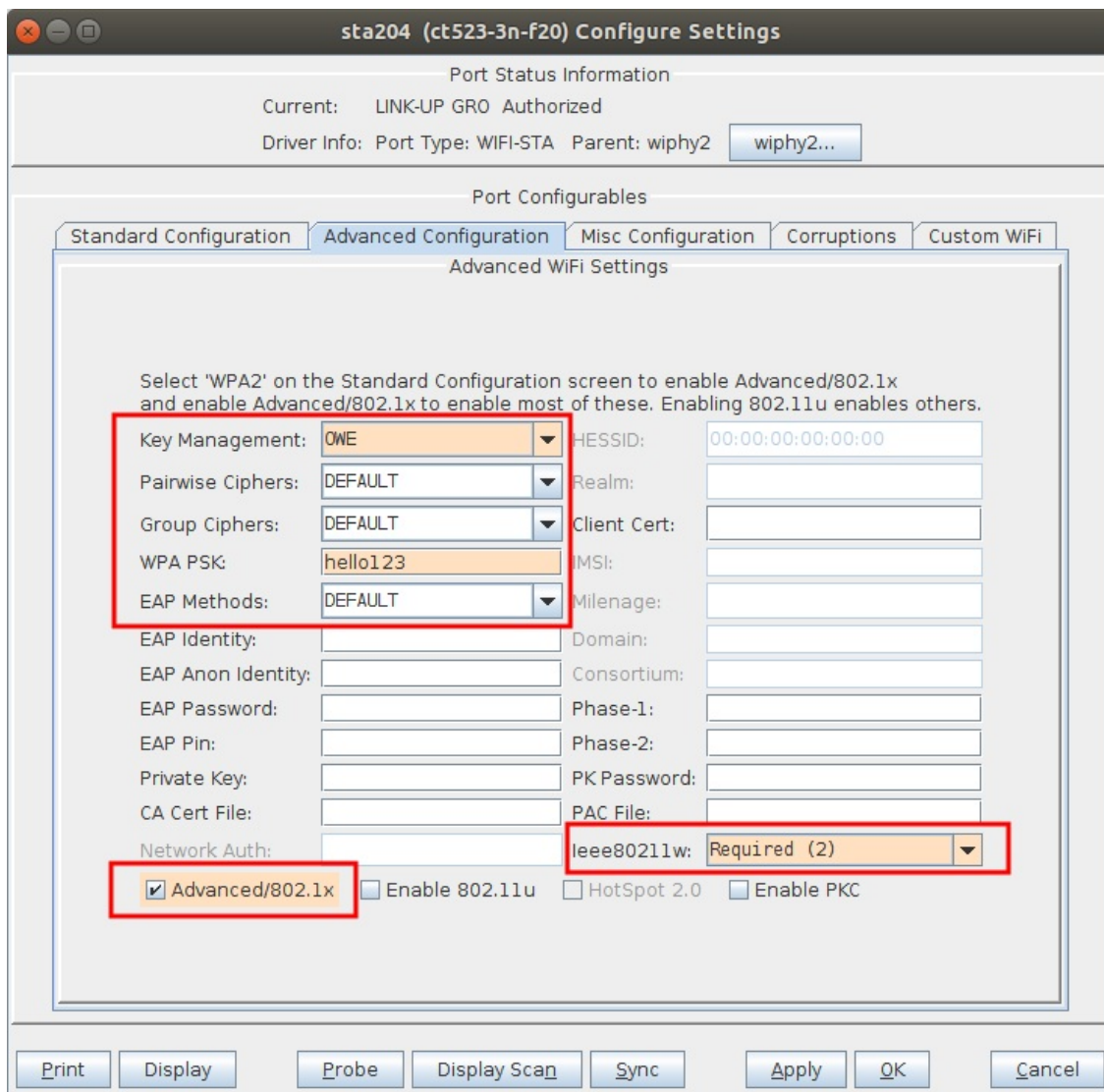
D. Setup the STA with WPA3 security and no PSK on the standard configuration screen.

The screenshot shows the 'Configure Settings' window for a device named 'sta204 (ct523-3n-f20)'. The window is divided into several sections:

- Port Status Information:** Shows 'Current: LINK-UP GRO Authorized' and 'Driver Info: Port Type: WIFI-STA Parent: wiphy2'. There is a 'wiphy2...' button.
- Port Configurables:** Contains tabs for 'Standard Configuration', 'Advanced Configuration', 'Misc Configuration', 'Corruptions', and 'Custom WiFi'. The 'Standard Configuration' tab is active.
- General Interface Settings:** Includes options for 'Down', 'Aux-Mgt', 'DHCP-IPv6', 'DHCP Release', 'DHCP Vendor ID', 'DHCP Client ID', 'DNS Servers', 'IP Address', 'IP Mask', 'Gateway IP', 'Alias', 'MAC Addr', 'Rpt Timer', 'IPSec GW', 'IPSec Local ID.', 'Peer IP', 'Global IPv6', 'Link IPv6', 'IPv6 GW', 'MTU', 'TX Q Len', 'WiFi Bridge', 'IPSec Password', and 'IPSec Remote ID.'.
- WiFi Settings:** This section is highlighted with a red box. It includes:
 - SSID: ABCD-OWE
 - Key/Phrase: (empty)
 - AP: DEFAULT
 - Mode: 802.11abgn-AC
 - Rate: OS Default
 - Security options: WPA, WPA2, **WPA3** (checked), OSEN, WEP.
 - Other options: Disable HT40, Enable VHT160, Disable SGI.
- Enable:** Includes 'Set MAC', 'Set TX Q Len', 'Set MTU', 'Set Offload', and 'Set PROMISC'.
- Services:** Includes 'HTTP', 'FTP', 'RADIUS', 'IPSEC-Client', and 'IPsec-Upstream'.
- Low Level:** Includes 'PROMISC', 'TSO Enabled', 'UFO Enabled', 'GSO Enabled', 'LRO Enabled', and 'GRO Enabled'.

At the bottom of the window, there are buttons for 'Print', 'Display', 'Probe', 'Display Scan', 'Sync', 'Apply', 'OK', and 'Cancel'.

- 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.

