

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.

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

General Interface Settings

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

☐ 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: ABCD-wpa3 AP: DEFAULT
Key/Phrase: hello123 Mode: (802.11abgn-AC)
Freq/Channel: 5745/149 Rate: 0S 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

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

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

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
ieee80211w:	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.

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

☐ 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: OS Default

☐ WPA ☐ WPA2 ☒ WPA3 ☐ OSEN ☐ WEP

☐ Disable HT40 ☐ Enable VHT160 ☐ Disable SGI

[Print](#) [Display](#) [Probe](#) [Display Scan](#) [Sync](#) [Apply](#) [OK](#) [Cancel](#)

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

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

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: DEFAULT HESSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: IMSI:

EAP Methods: DEFAULT Milenage:

EAP Identity: Domain:

EAP Anon Identity: Consortium:

EAP Password: Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

CA Cert File: PAC File:

Network Auth: IEEE80211w: Required (2)

☐ Advanced/802.1x ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

E. A capture of the association.

wpa3-personal.pcapng (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.addr==00:03:7f:30:e0:00 and wlan.addr==00:0e:8e:6c:2d:b5

No.	Time	Source	Destination	Protocol	Length	Info
3452	74.324876814	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	234	Probe Response, SN=2371, FN=0, Flags=....., BI=240, SSID=ABC0-wpa3
3468	74.58202045	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	802.11	188	Authentication, SN=257, FN=0, Flags=.....
3470	74.588879153	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	188	Authentication, SN=2373, FN=0, Flags=.....
3472	74.592861789	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	802.11	124	Authentication, SN=258, FN=0, Flags=.....
3474	74.593815258	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	124	Authentication, SN=2374, FN=0, Flags=.....
3476	74.595497098	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	802.11	206	Association Request, SN=259, FN=0, Flags=....., SSID=ABC0-wpa3
3478	74.59646000	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	189	Association Response, SN=2375, FN=0, Flags=.....
3480	74.597443407	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	EAPOL	215	Key (Message 1 of 4)
3482	74.599223124	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	EAPOL	221	Key (Message 2 of 4)
3484	74.600030607	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	EAPOL	281	Key (Message 3 of 4)
3486	74.600476768	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	EAPOL	193	Key (Message 4 of 4)
3488	74.601401320	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	87	Action, SN=2376, FN=0, Flags=.....
3490	74.605347767	00:03:7f:30:e0:00	00:0e:8e:6c:2d:b5	802.11	189	Action, SN=0, FN=0, Flags=p.....
3492	74.606650038	00:0e:8e:6c:2d:b5	00:03:7f:30:e0:00	802.11	189	Action, SN=2377, FN=0, Flags=p.....

Frame 3468: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits) on interface 0

Radiotap Header v0, Length 60

802.11 radio information

IEEE 802.11 Authentication, Flags:

IEEE 802.11 wireless LAN

Fixed parameters (144 bytes)

Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)

Authentication Seq: 0x0001

Status code: Successful (0x0000)

SAE Message Type: Commit (1)

Group ID: 256-bit random ECP group (19)

Scalar: 505b7d9e3ccb0b548b2f9cdf5a03dcfb944cb543cf9ffefac..

Finite Field Element: 252e82dc16c2ec38947a70a70de3e389a9e200f591a96c7..

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.

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

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
 HS20 WAN Metrics
IEEE80211w: Required (2) **RADIUS IP: 127.0.0.1**
RADIUS Port: 1812
RADIUS Secret: lanforge
 Venue Group: Unspecified (0) Venue Type: Unspecified (0)
 Network Type: Private (0) Address Types: Not Available (0)
 Network Auth:
☐ 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

- 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.

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

☐ 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:

IPSec GW: IPSec Password:

IPSec Local ID.: IPSec Remote ID.:

WiFi Settings

SSID: AP:

Key/Phrase: Mode:

Freq/Channel: Rate:

☐ WPA ☐ WPA2 ☒ WPA3 ☐ OSEN ☐ WEP

☐ Disable HT40 ☐ Enable VHT160 ☐ Disable SGI

[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.

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

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: WPA-EAP-SUITE-B BSSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: IMSI:

EAP Methods: EAP-TTLS Millenage:

EAP Identity: lanforge.ttls Domain:

EAP Anon Identity: Consortium:

EAP Password: !!ttls123 Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

CA Cert File: PAC File:

Network Auth: IEEE80211w: Required (2)

☒ Advanced/802.1X ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

- G. A capture of the association.

No.	Time	Source	Destination	Protocol	Length	Info
763	19.677894644	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	802.11	238	Probe Response, SN=1274, FN=0, Flags=..., BI=240, SSID=ABCDE-wpa3
775	19.927290798	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	802.11	98	Authentication, SN=257, FN=0, Flags=...
777	19.928384327	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	802.11	98	Authentication, SN=1276, FN=0, Flags=...
779	19.931395509	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	802.11	207	Association Request, SN=258, FN=0, Flags=..., SSID=ABCDE-wpa3
781	19.932513664	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	802.11	193	Association Response, SN=1277, FN=0, Flags=...
783	19.933260310	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	103	Request, Identity
785	19.934869130	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAP	119	Response, Identity
787	19.936316903	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	104	Request, TLS EAP (EAP-TLS)
789	19.936678226	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAP	104	Response, Legacy Nak (Response Only)
791	19.937948362	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	104	Request, Tunnelled TLS EAP (EAP-TTLS)
793	19.938775229	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TLSv1.2	349	Client Hello
795	19.942174798	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	TLSv1.2	1501	Server Hello, Certificate, Server Hello Done
797	19.942475875	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAP	104	Response, Tunnelled TLS EAP (EAP-TTLS)
799	19.945040229	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	TLSv1.2	1038	Server Hello, Certificate, Server Hello Done
801	19.947895435	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TLSv1.2	422	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
803	19.953781902	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	TLSv1.2	155	Change Cipher Spec, Change Cipher Spec, Encrypted Handshake Message
805	19.95392491	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TLSv1.2	161	Application Data
807	19.953832132	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	TLSv1.2	165	Application Data
809	19.954261428	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	TLSv1.2	165	Application Data
811	19.955718490	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAP	102	Success
813	19.956051355	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAPOL	215	Key (Message 1 of 4)
815	19.956927898	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAPOL	221	Key (Message 2 of 4)
817	19.958254854	00:0e:8e:6c:2d:b5	00:03:7f:ce:63:00	EAPOL	281	Key (Message 3 of 4)
819	19.958752292	00:03:7f:ce:63:00	00:0e:8e:6c:2d:b5	EAPOL	193	Key (Message 4 of 4)

Tag: SSID parameter set: ABCDE-wpa3

Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]

Tag: RSN Information

Tag Number: RSN Information (48)

Tag length: 28

RSN version: 1

Group Cipher Suite: 00:0f:ac AES (CCM)

Pairwise Cipher Suite Count: 1

Pairwise Cipher Suite List 00:0f:ac AES (CCM)

Auth Key Management (AKM) Suite Count: 1

Auth Key Management (AKM) List 00:0f:ac WPA (SHA256-SuiteB)

Auth Key Management (AKM) Suite: 00:0f:ac WPA (SHA256-SuiteB)

Auth Key Management (AKM) OUI: 00:0f:ac

Auth Key Management (AKM) type: WPA (SHA256-SuiteB) (11)

RSN capabilities: 0x0000

PMKID Count: 0

PMKID List

Group Management Cipher Suite: 00:0f:ac BIP (128)

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.

The left screenshot shows the 'Standard Configuration' tab. Under 'WIFI Settings', 'WPA3' is selected. The 'KeyPhrase' is 'hello123'. The right screenshot shows the 'Advanced Configuration' tab. Under 'Advanced WIFI Settings', 'IEEE80211w' is set to 'Required (2)'.

- 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.

The screenshot shows the 'Misc Configuration' tab. The 'Custom WPA Cfg' checkbox is checked, and the path '/home/lanforge/wifi/vap2-owe.conf' is entered in the adjacent text field.

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

**sta204 (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

☐ 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:a3:cc: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-OWE AP: DEFAULT

Key/Phrase: Mode: 802.11abgn-AC

Freq/Channel: 5745/149 Rate: OS Default

☐ WPA ☐ WPA2 ☒ WPA3 ☐ OSEN ☐ WEP

☐ Disable HT40 ☐ Enable VHT160 ☐ Disable SGI

Print Display Probe Display Scan Sync Apply OK 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.

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

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: OWE HESSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: hello123 IMSI:

EAP Methods: DEFAULT Milenage:

EAP Identity: Domain:

EAP Anon Identity: Consortium:

EAP Password: Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

CA Cert File: PAC File:

Network Auth: IEEE80211w: Required (2)

☒ Advanced/802.1x ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print Display Probe Display Scan Sync Apply OK Cancel

- F. A capture of the association.

| No.  | Time         | Source            | Destination       | Protocol | Length | Info                                                            |
|------|--------------|-------------------|-------------------|----------|--------|-----------------------------------------------------------------|
| 1298 | 14.469614504 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | 802.11   | 233    | Probe Response, SN=2274, FN=0, Flags=..., BI=240, SSID=ABCD-OWE |
| 1325 | 14.721099536 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | 802.11   | 80     | Authentication, SN=257, FN=0, Flags=...                         |
| 1327 | 14.722087175 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 80     | Authentication, SN=2276, FN=0, Flags=...                        |
| 1330 | 14.727092179 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | 802.11   | 242    | Association Request, SN=258, FN=0, Flags=..., SSID=ABCD-OWE     |
| 1332 | 14.728191312 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 104    | Action, SN=2277, FN=0, Flags=...                                |
| 1334 | 14.728593653 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 200    | Association Response, SN=2278, FN=0, Flags=...                  |
| 1347 | 14.934144512 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 104    | Action, SN=2280, FN=0, Flags=...                                |
| 1394 | 15.149207519 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 104    | Action, SN=2282, FN=0, Flags=...                                |
| 1410 | 15.348202045 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 104    | Action, SN=2284, FN=0, Flags=...                                |
| 1429 | 15.552245876 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 104    | Action, SN=2285, FN=0, Flags=...                                |
| 1479 | 15.762205591 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | 802.11   | 242    | Association Request, SN=259, FN=0, Flags=..., SSID=ABCD-OWE     |
| 1481 | 15.766736183 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 252    | Association Response, SN=2287, FN=0, Flags=...                  |
| 1483 | 15.767188734 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 87     | Action, SN=2288, FN=0, Flags=...                                |
| 1485 | 15.767185458 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | 802.11   | 87     | Action, SN=2289, FN=0, Flags=...                                |
| 1487 | 15.767566571 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | EAPOL    | 193    | Key (Message 1 of 4)                                            |
| 1489 | 15.771300015 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | EAPOL    | 221    | Key (Message 2 of 4)                                            |
| 1491 | 15.772482847 | 00:0e:8e:6c:2d:b5 | 00:03:7f:a3:cc:00 | EAPOL    | 281    | Key (Message 3 of 4)                                            |
| 1493 | 15.773088516 | 00:03:7f:a3:cc:00 | 00:0e:8e:6c:2d:b5 | EAPOL    | 193    | Key (Message 4 of 4)                                            |

Tag Length: 0  
Supported Rates: 6 (0x0c)  
Supported Rates: 9 (0x12)  
Supported Rates: 12 (0x18)  
Supported Rates: 18 (0x24)  
Supported Rates: 24 (0x30)  
Supported Rates: 36 (0x48)  
Supported Rates: 48 (0x60)  
Supported Rates: 54 (0x6c)

Tag: RSN Information  
Tag Number: RSN Information (48)  
Tag Length: 26  
RSN Version: 1  
Group Cipher Suite: 00:0f:ac AES (CCM)  
Pairwise Cipher Suite Count: 1  
Pairwise Cipher Suite List 00:0f:ac AES (CCM)  
Auth Key Management (AKM) Suite Count: 1  
Auth Key Management (AKM) List 00:0f:ac Opportunistic Wireless Encryption  
Auth Key Management (AKM) Suite: 00:0f:ac Opportunistic Wireless Encryption  
Auth Key Management (AKM) OUI: 00:0f:ac  
Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)  
RSN capabilities: 0x0000  
PMKID Count: 0  
PMKID List