Configure and Verify Wi-Fi 6E WLAN Layer 2 Security

Contents

Introduction

This document describes how to configure Wi-Fi 6E WLAN Layer 2 security and what to expect on different clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Wireless Lan Controllers (WLC) 9800
- Cisco Access Points (APs) that support Wi-Fi 6E.
- IEEE Standard 802.11ax.
- Tools: Wireshark v4.0.6

Components Used

The information in this document is based on these software and hardware versions:

- WLC 9800-CL with IOS® XE 17.9.3.
- APs C9136, CW9162, CW9164 and CW9166.
- Wi-Fi 6E Clients:
  - Lenovo X1 Carbon Gen11 with Intel AX211 Wi-Fi 6 and 6E Adapter with driver version 22.200.2(1).
  - Netgear A8000 Wi-Fi 6 and 6E Adapter with driver v1(0.0.108);
  - Mobile Phone Pixel 6a with Android 13;
  - Mobile Phone Samsung S23 with Android 13.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The key thing to know is that Wi-Fi 6E is not an entirely new standard, but an extension. At its base, Wi-Fi 6E is an extension of the Wi-Fi 6 (802.11ax) wireless standard into the 6-GHz radio-frequency band.

Wi-Fi 6E builds on Wi-Fi 6, which is the latest generation of the Wi-Fi standard, but only Wi-Fi 6E devices and applications can operate in the 6-GHz band.

Wi-Fi 6E Security

Wi-Fi 6E uplevels security with Wi-Fi Protected Access 3 (WPA3) and Opportunistic Wireless Encryption (OWE) and there is no backward compatibility with Open and WPA2 security.

WPA3 and Enhanced Open Security are now mandatory for Wi-Fi 6E certification and Wi-Fi 6E also requires Protected Management Frame (PMF) in both AP and Clients.

When configuring a 6GHz SSID there are certain security requirements that must be met:

- WPA3 L2 security with OWE, SAE or 802.1x-SHA256
- Protected Management Frame Enabled;
- Any other L2 security method is not allowed, that is, no mixed mode possible.

WPA3

WPA3 is designed to improve Wi-Fi security by enabling better authentication over WPA2, providing expanded cryptographic strength and increasing the resiliency of critical networks.

Key features of WPA3 include:

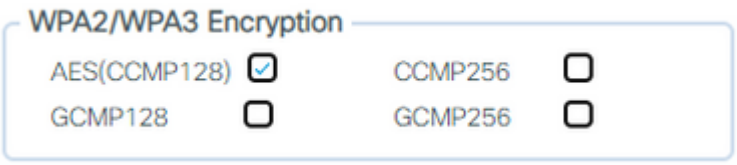
- **Protected Management Frame (PMF)**protects unicast and broadcast management frames and encrypts unicast management frames. This means wireless intrusion detection and wireless intrusion prevention systemsnow have fewer brute-force ways to enforce client policies.
- **Simultaneous Authentication of Equals (SAE)**enables password-based authentication and a key agreement mechanism. This protects against brute-force attacks.
- **Transition mode**is a mixed mode that enables the use of WPA2 to connect clients that do not support WPA3.

WPA3 is about continuous security development and conformance as well as interoperability.
There is no Information Element that designates WPA3 (same as WPA2). WPA3 is defined by AKM/Cipher

Suite/PMF combinations.

On the 9800 WLAN configuration, you have 4 different WPA3 encryption algorithms you can use.

They are based on Galois/Counter Mode Protocol (GCMP) and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 and GCMP256:

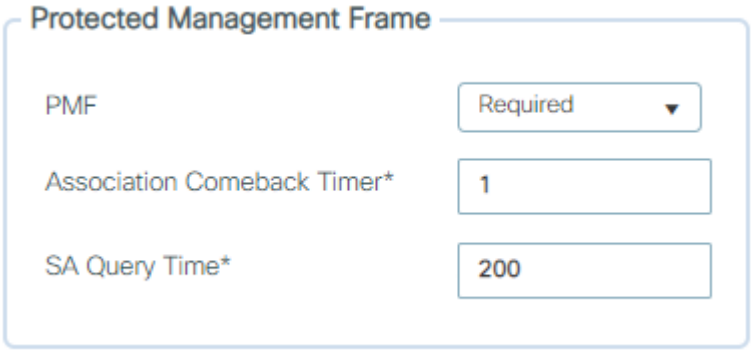


WPA2/3 Encryption options

PMF

PMF is activated on a WLAN when you enable PMF.

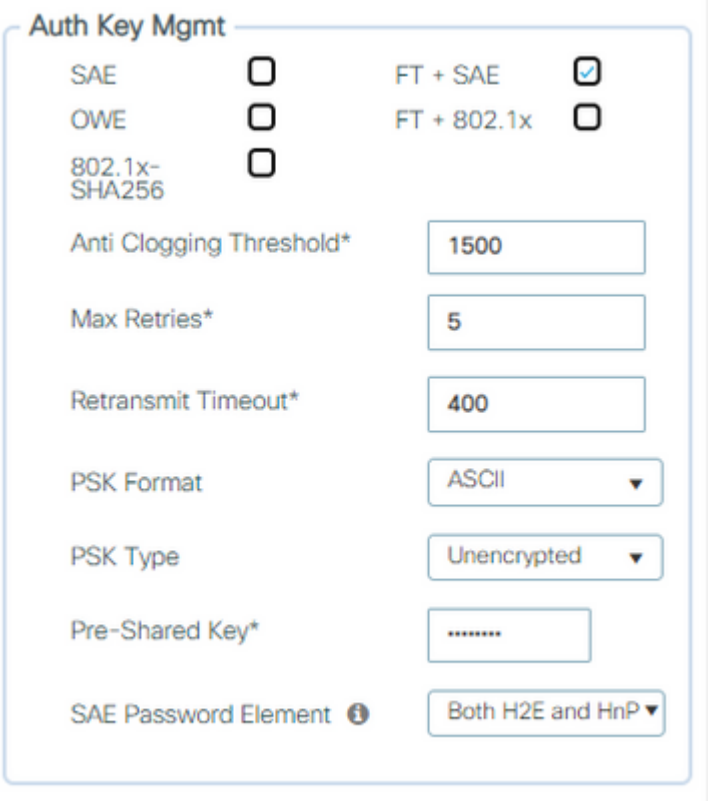
By default, 802.11 management frames are unauthenticated and hence not protected against spoofing. Infrastructure Management Protection Frame (MFP) and 802.11w protected management frames (PMF) provide protection against such attacks.



PMF Options

Authentication Key Management

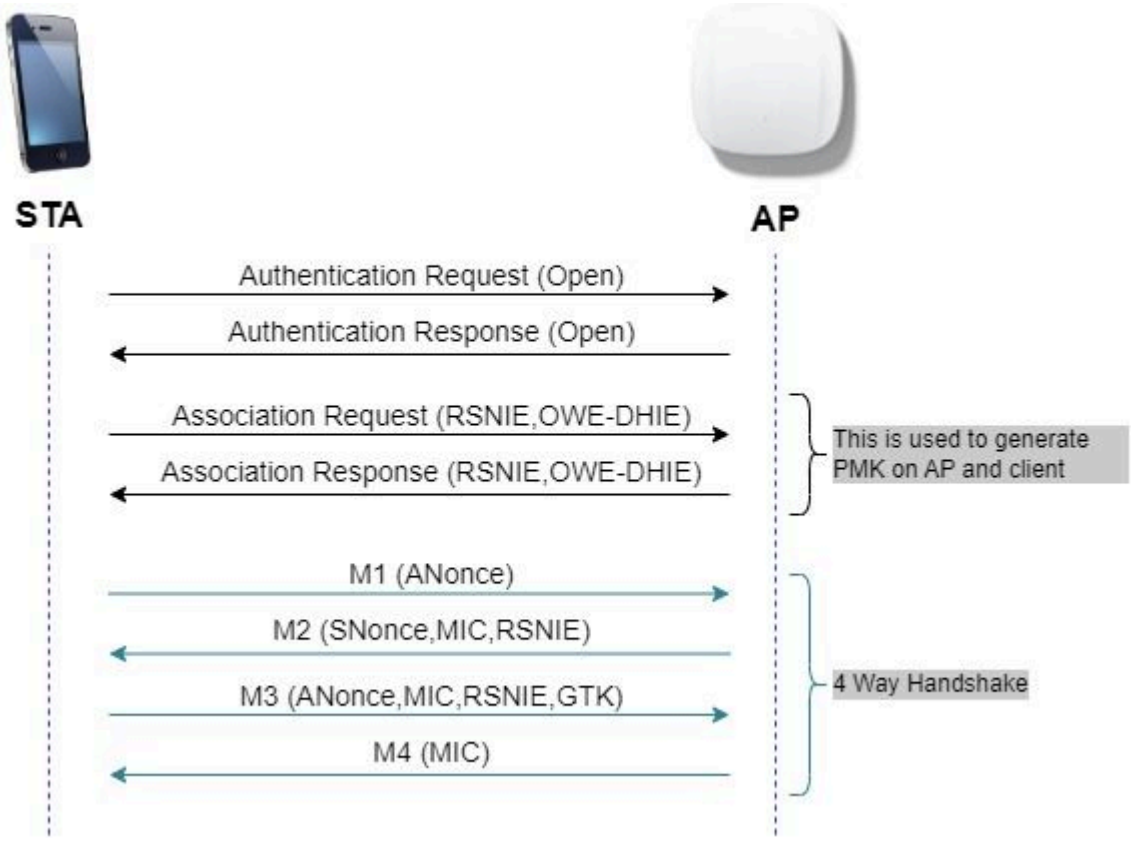
These are the AKM options available in the 17.9.x version:



AKM Options

OWE

Opportunistic Wireless Encryption (OWE) is an extension to IEEE 802.11 that provides encryption of the wireless medium (IETF RFC 8110). The purpose of OWE based authentication is avoid open unsecured wireless connectivity between the APâ€™s and clients. The OWE uses the Diffie-Hellman algorithms based Cryptography to setup the wireless encryption. With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise master key (PMK) secret with the 4-way handshake. The use of OWE enhances wireless network security for deployments where Open or shared PSK based networks are deployed.



OWE frame exchange

SAE

WPA3 use a new authentication and key management mechanism called Simultaneous Authentication of Equals. This mechanism is further enhanced through the use of SAE Hash-to-Element (H2E).

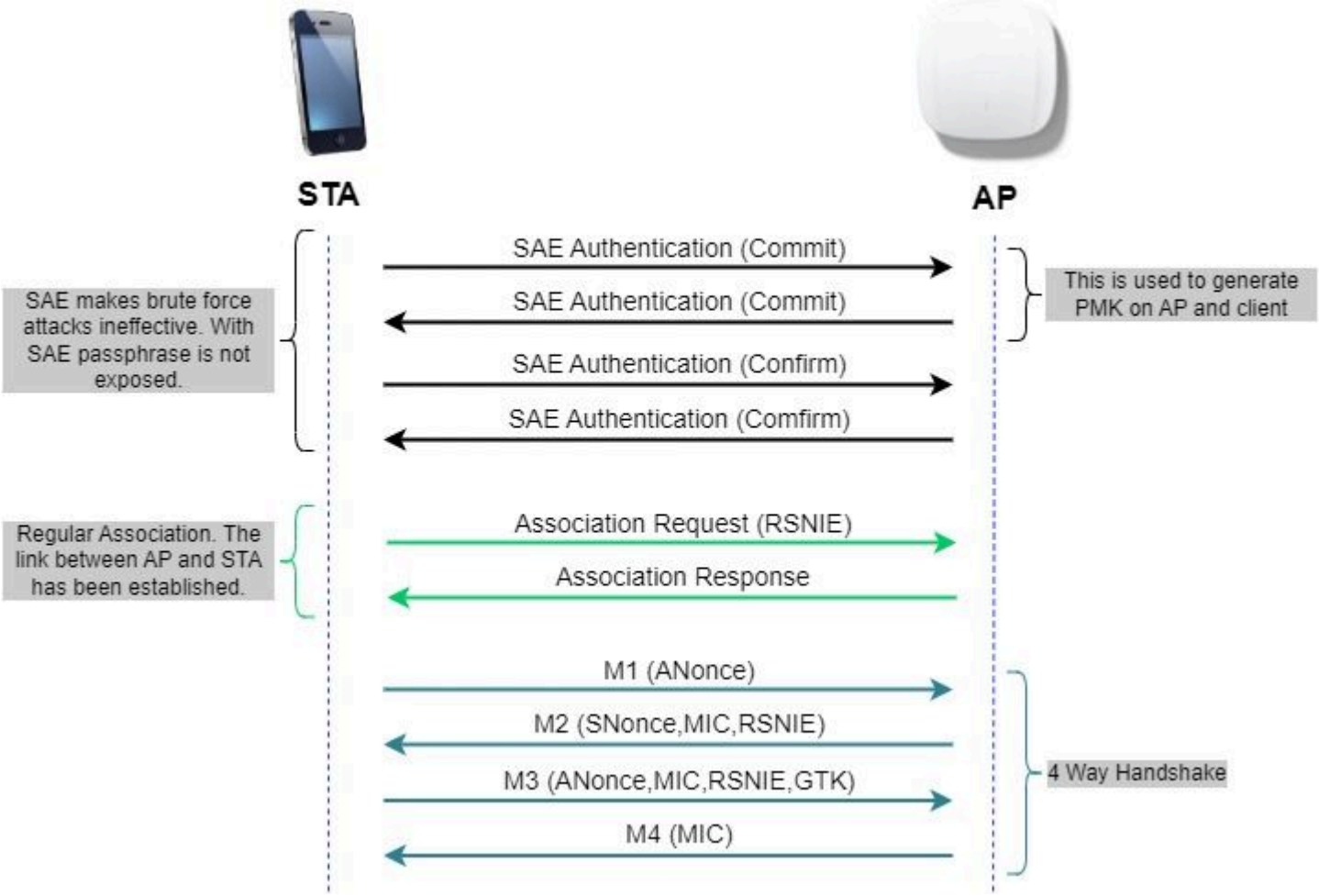
SAE with H2E is mandatory for WPA3 and Wi-Fi 6E.

SAE employs a discrete logarithm cryptography to perform an efficient exchange in a way that performs mutual authentication using a password that is probably resistant to an offline dictionary attack.

An offline dictionary attack is where an adversary attempts to determine a network password by trying possible passwords without further network interaction.

When the client connects to the access point, they perform an SAE exchange. If successful, they create each a cryptographically strong key, from which the session key is derived. Basically a client and access point goes into phases of commit and then confirm.

Once there is a commitment, the client and access point can then go into the confirm states each time there is a session key to be generated. The method uses forward secrecy, where an intruder could crack a single key, but not all of the other keys.



SAE frame exchange

Hash-to-Element (H2E)

Hash-to-Element (H2E) is a new SAE Password Element (PWE) method. In this method, the secret PWE used in the SAE protocol is generated from a password.

When a station (STA) that supports H2E initiates SAE with an AP, it checks whether AP supports H2E. If yes, the AP uses the H2E to derive the PWE by using a newly defined Status Code value in the SAE Commit message.

If STA uses Hunting-and-Pecking (HnP), the entire SAE exchange remains unchanged.

While using the H2E, the PWE derivation is divided into these components:

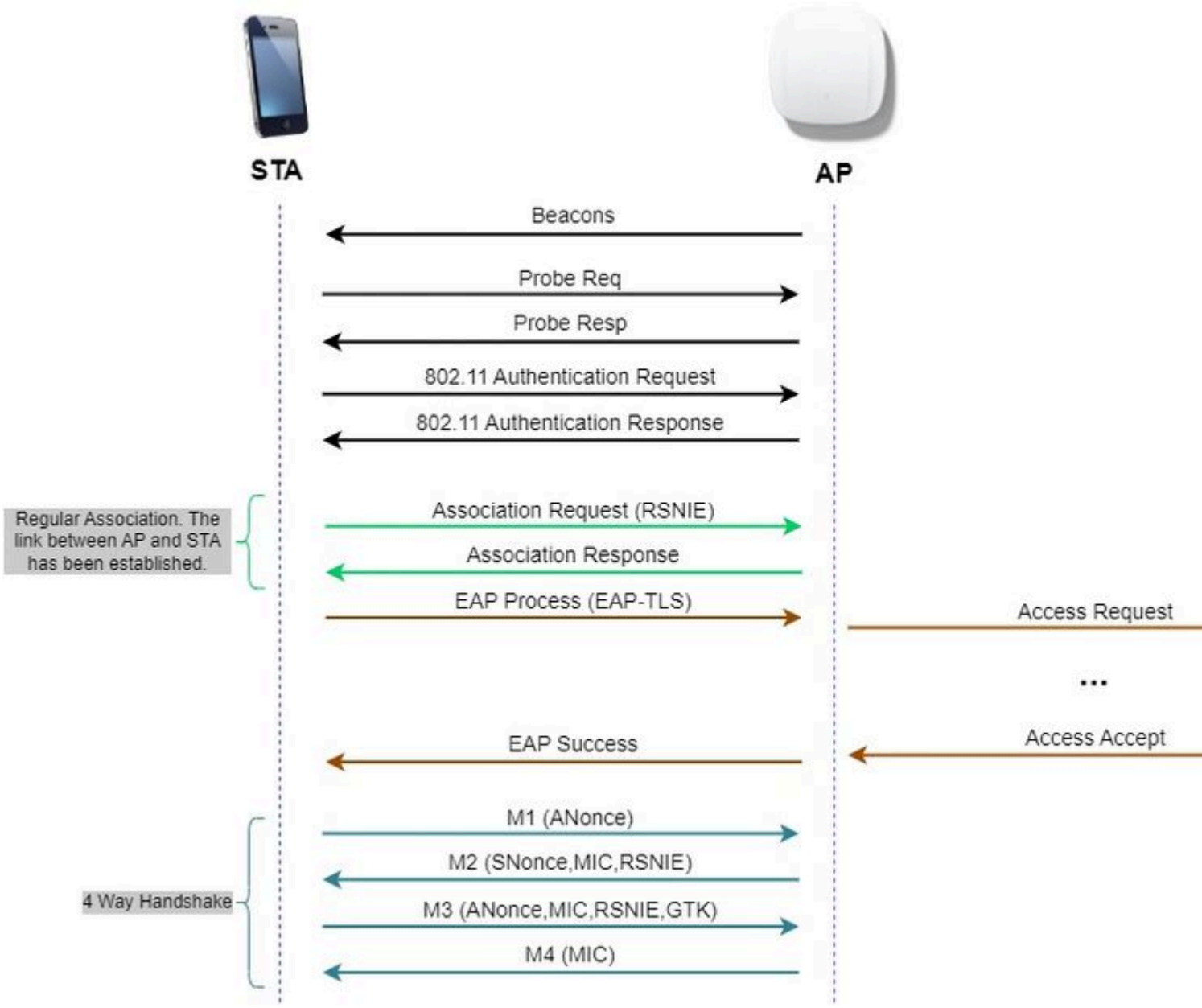
- Derivation of a secret intermediary element (PT) from the password. This can be performed offline when the password is initially configured on the device for each supported group.
- Derivation of the PWE from the stored PT. This depends on the negotiated group and MAC addresses of peers. This is performed in real-time during the SAE exchange.

Note: 6-GHz supports only Hash-to-Element SAE PWE method.

WPA-Enterprise aka 802.1x

WPA3-Enterprise is the most secure version of WPA3 and uses a username plus password combination with

802.1X for user authentication with a RADIUS server. By default, WPA3 uses 128-bit encryption, but it also introduces an optionally configurable 192-bit cryptographic strength encryption, which gives additional protection to any network transmitting sensitive data.



WPA3 Enterprise diagram flow

Level Set: WPA3 Modes

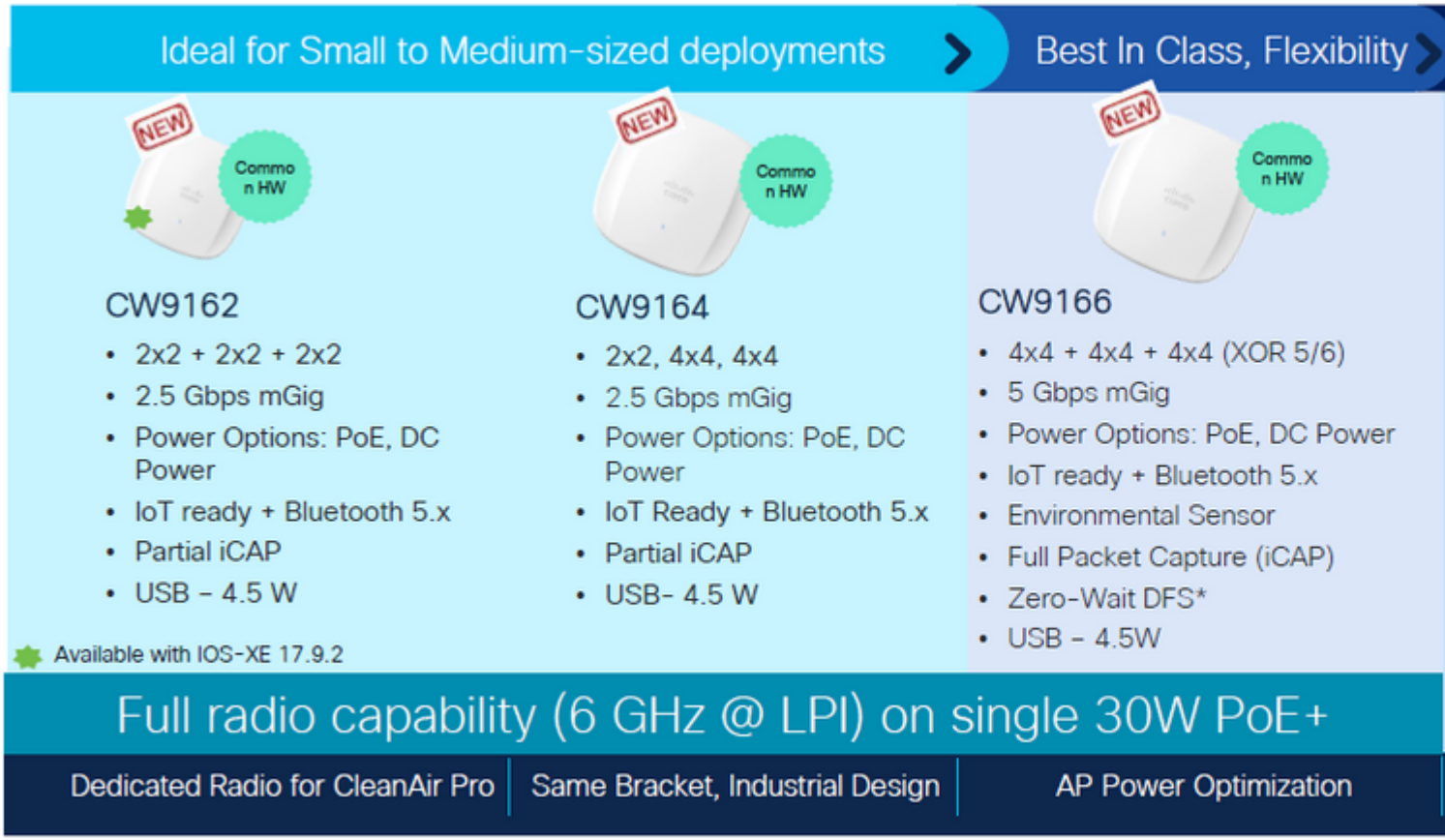
- WPA3-Personal
  - WPA3-Personal only mode
    - PMF Required
  - WPA3-Personal Transition mode
    - Configuration rules: On an AP, whenever WPA2-Personal is enabled, the WPA3-Personal Transition mode must also be enabled by default, unless explicitly overridden by the administrator to operate in WPA2-Personal only mode

- WPA3-Enterprise
  - WPA3-Enterprise only mode
    - PMF shall be negotiated for all WPA3 connections
  - WPA3-Enterprise Transition mode
    - PMF shall be negotiated for a WPA3 connection
    - PMF optional for a WPA2 connection
  - WPA3-Enterprise suite-B â€œ192-bitâ€ mode aligned with Commercial National Security Algorithm (CNSA)
    - More than just for the federal government

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

To know more about detailed information about WPA3 implementation in Cisco WLANs, including client security compatibility matrix, please feel free to check the WPA3 Deployment Guide.

Cisco Catalyst Wi-Fi 6E APs



Wi-Fi 6E Access Points

Clients Supported Security Settings

You can find which product support WPA3-Enterprise using WiFi Alliance webpage [product finder](#).

On windows devices you can verify what are the security settings supported by the adapter using the command "netsh wlan show drivers".

Here you can see the output of Intel AX211:

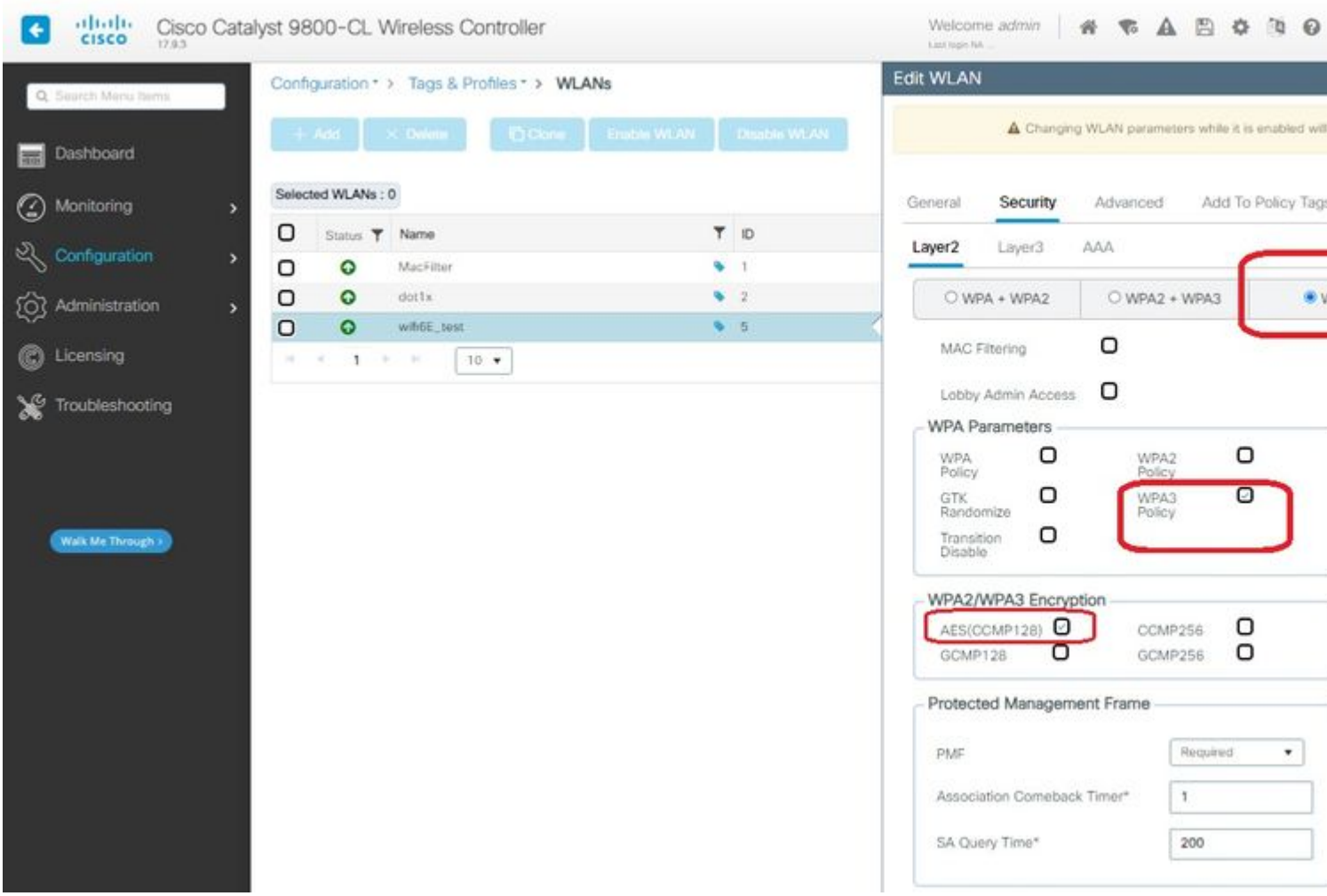
```
C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                  : Intel(R) Wi-Fi 6E AX211 160MHz
    Vendor                  : Intel Corporation
    Provider                : Intel
    Date                    : 3/9/2023
    Version                 : 22.200.2.1
    INF file                : oem151.inf
    Type                    : Native Wi-Fi Driver
    Radio types supported   : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                            Open            None
                            Open            WEP-40bit
                            Open            WEP-104bit
                            Open            WEP
                            WPA-Enterprise  TKIP
                            WPA-Enterprise  CCMP
                            WPA-Personal    TKIP
                            WPA-Personal    CCMP
                            WPA2-Enterprise TKIP
                            WPA2-Enterprise CCMP
                            WPA2-Personal   TKIP
```

: Even though there are no clients supporting GCMP128 cipher + SUITEB-1X as of writting this document, it was tested to observe it being broadcasted and check the RSN info in the beacons.

â€ƒ

WPA3 - AES(CCPM128) + OWE

This is the WLAN Security configuration:



OWE Security Settings

View on WLC GUI of the WLAN Security settings:

WLAN Security settings on WLC GUI

Here we can observe Wi-Fi 6E clients connection process:

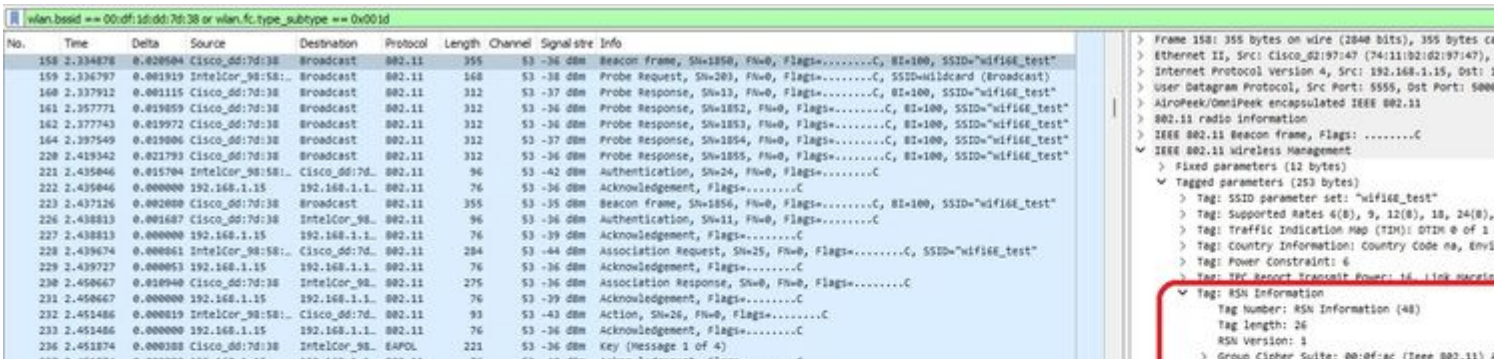
Intel AX211

Here we show the complete connection process of client Intel AX211.

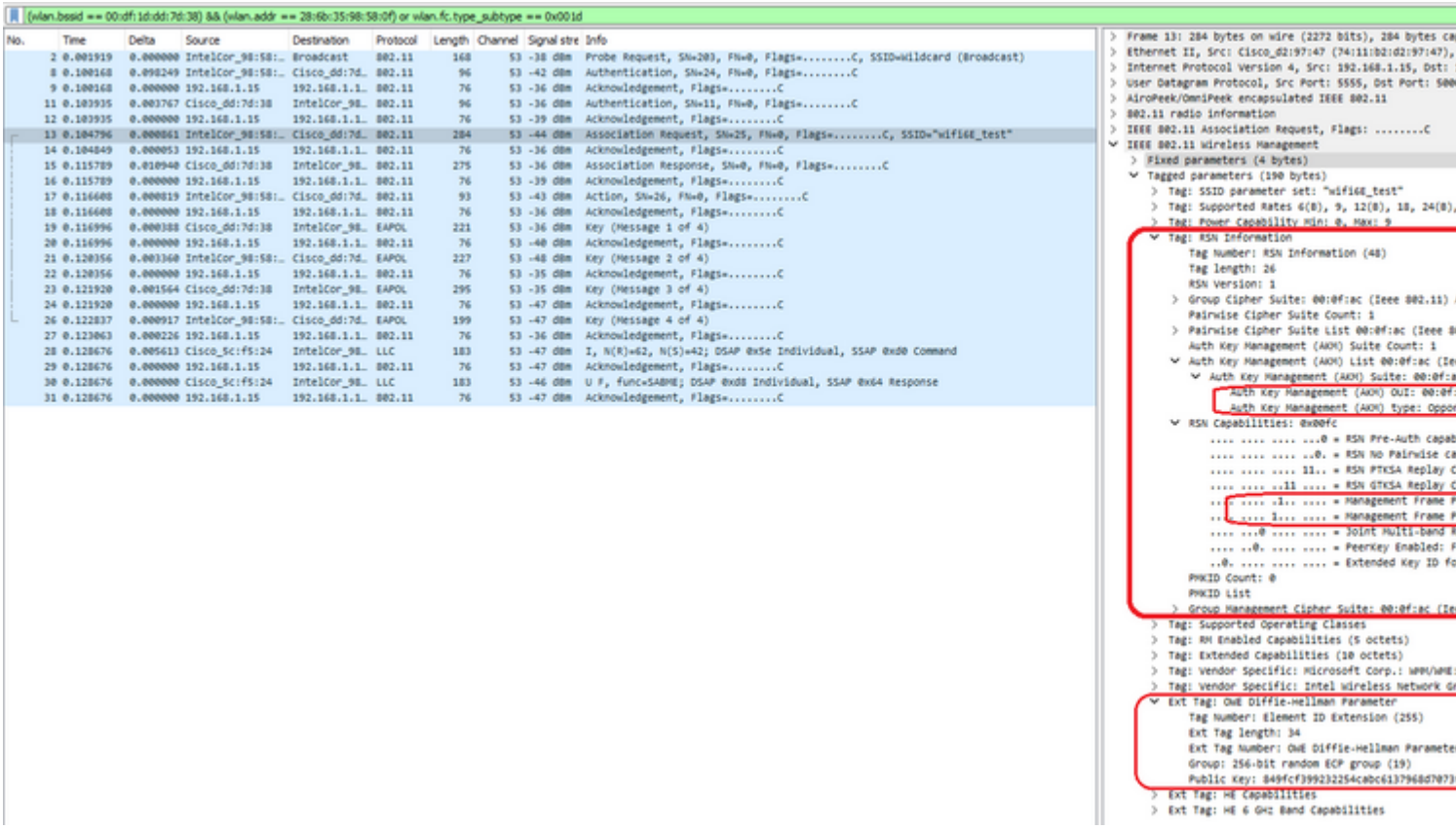
OWE Discovery

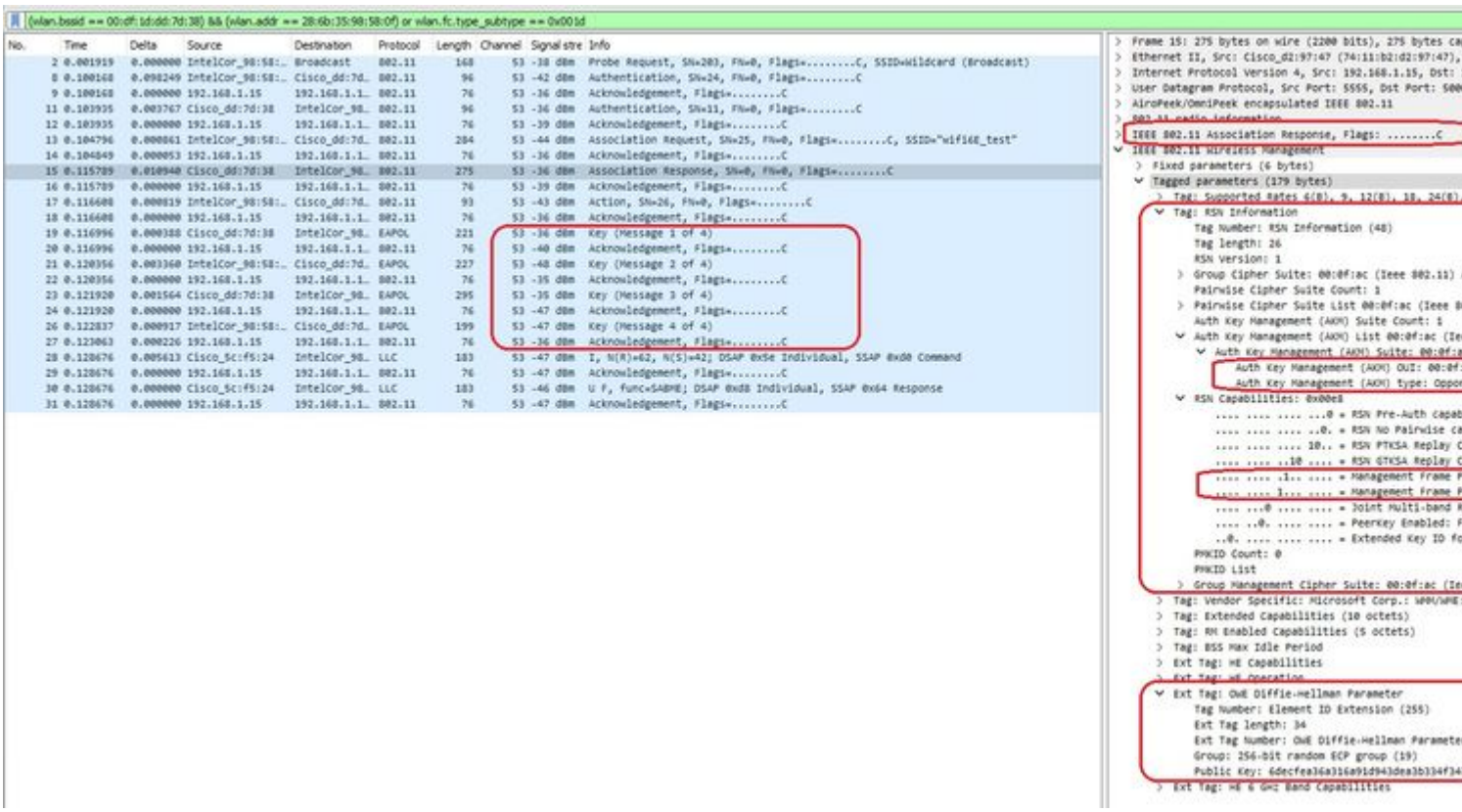
Here you can see the beacons OTA. The AP advertises support for OWE using AKM suite selector for OWE under RSN information element.

You can see AKM suite type value 18 (**00-0F-AC:18**) that indicates OWE support.



client that wants to do OWE must indicate OWE AKM in the RSN IE of Association Request frame and include Diffie Helman (DH) parameter element:

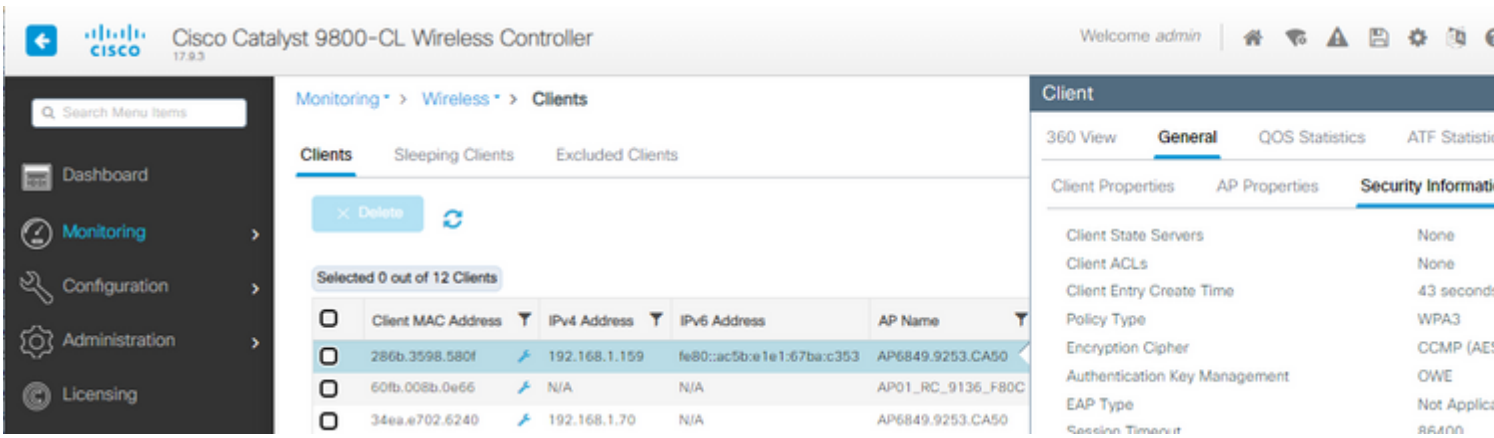




OWE Association response

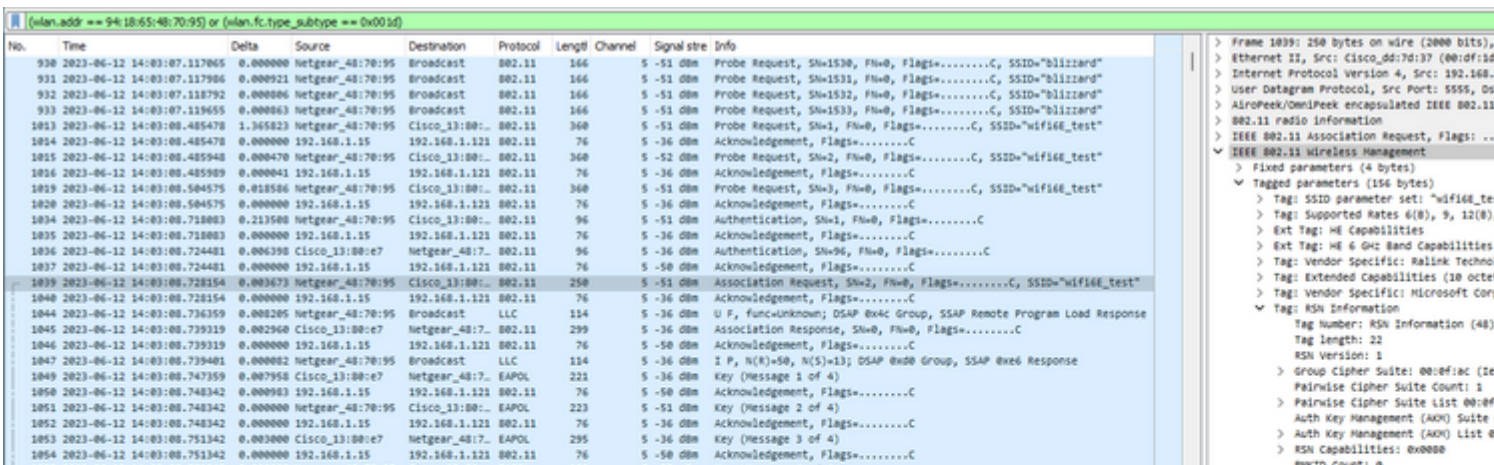
After the association response we can see the 4-way handshake and client moves to connected state.

Here you can see the client details on the WLC GUI:



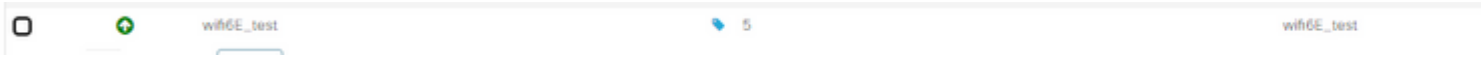
NetGear A8000

Connection OTA with focus on the RSN information from client:

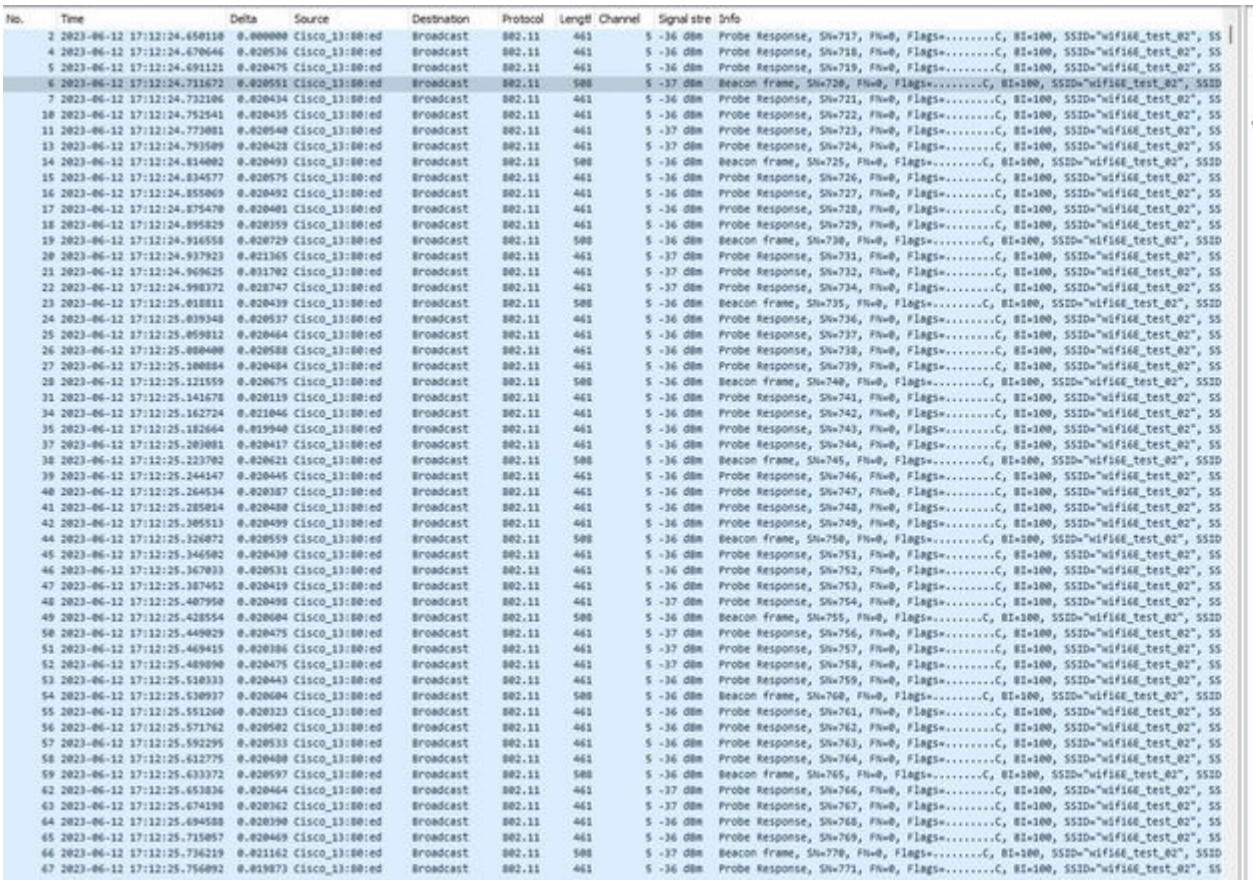


: Keep in mind that Hunting and Pecking is not allowed with 6 GHz radio policy. When you configure a 6GHz only WLAN, you must select H2E SAE Password Element.

View on WLC GUI of the WLAN Security settings:



Verification of beacons OTA:

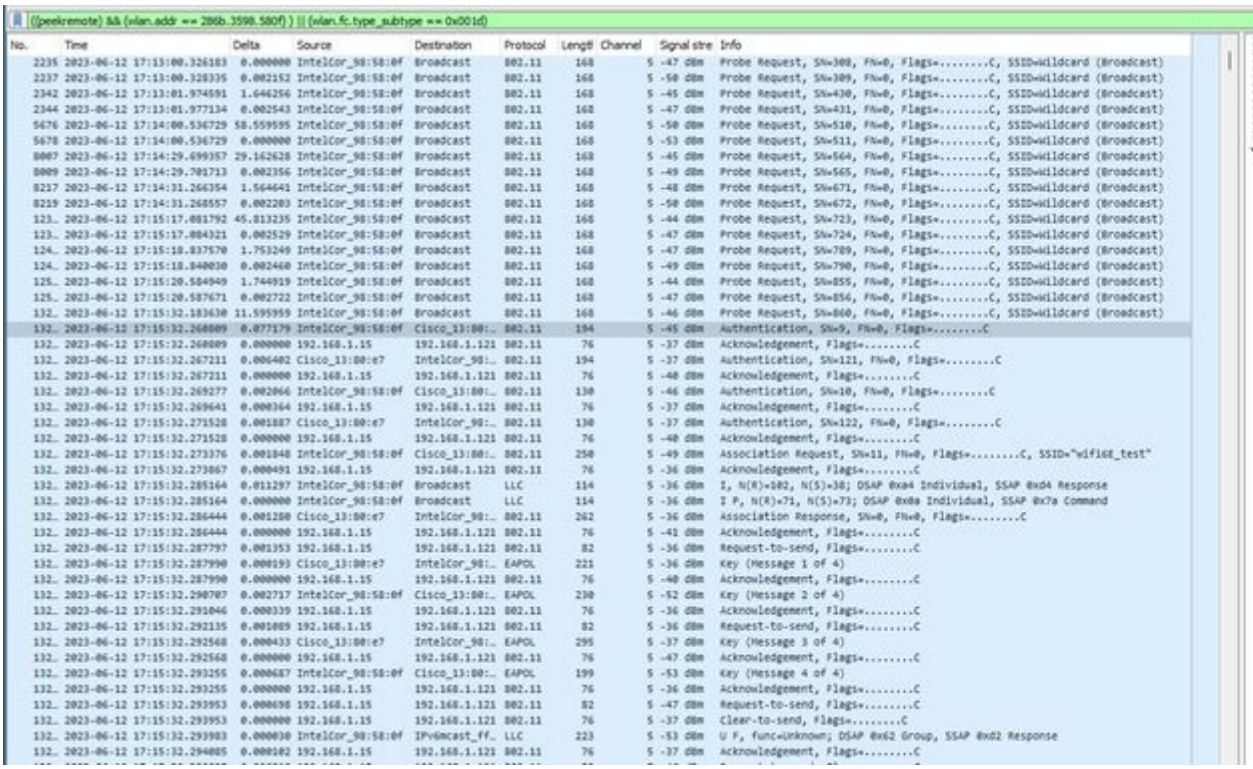


WPA3 SAE Beacons

Here we can observe Wi-Fi 6E clients associating:

Intel AX211

Connection OTA with focus on the RSN information from client:



Client details in WLC:

: In the Authentication Key Management, the WLC allows to select FT+SAE without SAE enabled, however it was observed the clients were not able to connect. Always enable both check boxes SAE and FT+SAE if you want to use SAE with Fast Transition.

View on WLC GUI of the WLAN Security settings:

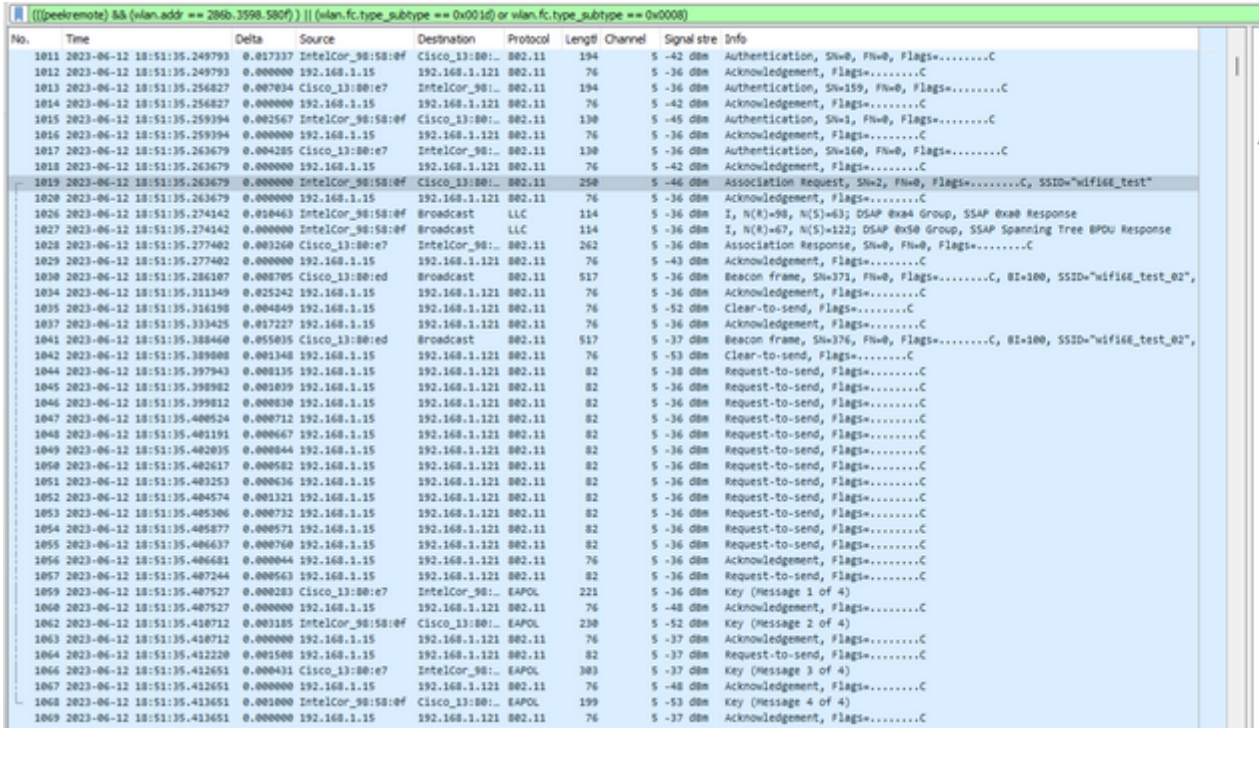
Verification of beacons OTA:

WPA3 SAE + FT Beacons

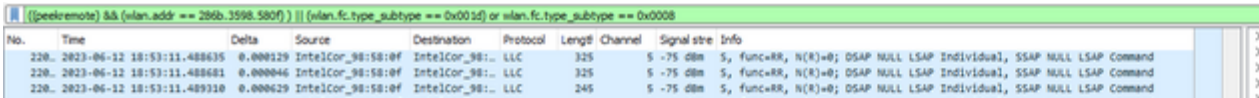
Here we can observe Wi-Fi 6E clients associating:

Intel AX211

Connection OTA with focus on the RSN information from client:



Roaming event where you can see the PMKID:



OWE	AES-CCMP128	OWE	NA.	NA.	NA	NA	Supported	Supported	Sup
SAE	AES-CCMP128	SAE (H2E Only)	SHA256	NA.	Supported	Supported	Supported: H2E Only and FT-oTA	Supported: H2E Only. FT Failed. FT-oDS Failed.	Sup H2E and oTA FT-Fail
Enterprise	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	Supported	Supported	Supported: SHA256 and FT-oTA/oDS Not-Supported: EAP-FAST	Supported: SHA256 and FT-oTA, FT-oDS (S23) Not-Supported: EAP-FAST, FT-oDS (Pixel6a)	Sup SHA and oTA Not Sup EAP FAS FT-
Enterprise	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	Not Supported	Not Supported	Not Supported	Not Supported	Not Sup
Enterprise	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	Not Supported	Not Supported	NA/TBD	NA/TBD	Not Sup

Troubleshoot

The troubleshooting used in this document was based on the online document:

Troubleshoot COS APs

The general guideline for troubleshooting is to collect RA trace in debug mode from the WLC using the client mac address making sure that the client is connecting using the device mac and not a randomized mac address.

For Over the Air troubleshooting, the recommendation is to use AP in sniffer mode capturing the traffic on the channel of the client serving AP.

Note: Refer to Important Information on Debug Commandsbefore you use **debug** commands.

Related Information

What is Wi-Fi 6E?

What Is Wi-Fi 6 vs. Wi-Fi 6E?

Wi-Fi 6E At-a-Glance

Wi-Fi 6E: The Next Great Chapter in Wi-Fi White Paper

Cisco Live - Architecting Next Generation Wireless Network with Catalyst Wi-Fi 6E Access Points

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide 17.9.x

WPA3 Deployment Guide